Citrix Virtual Apps and Desktops™ 7 2507 LTSR

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

Contents

What's new 22

Cumulative Update 2 (CU2) 22

What's new 25

Fixed issues 26

Cumulative Update 1 (CU1) 31

What's new 35

Fixed issues 37

Citrix Virtual Apps and Desktops™ 7 2507 LTSR (Initial release) 41

What's new 44

Fixed issues 50

Known issues 55

Deprecations and removals 63

System requirements 78

Technical overview 90

Databases 100

Delivery methods 107

Network ports 112

HDX™ 112

Citrix ICA® virtual channels 122

Double hop in Citrix Virtual Apps and Desktops™ 132

Install and configure 135

Machine identities 137

Active Directory joined 139

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

Microsoft Entra hybrid joined 143

Non-domain-joined 147

Prepare to install 148

AWS cloud environments 160

Azure Local environments 167

XenServer® virtualization environments 168

Google Cloud environments 168

HPE Moonshot virtualization environments 180

Microsoft Azure Resource Manager cloud environments 182

Microsoft System Center Configuration Manager environments 183

Microsoft System Center Virtual Machine Manager virtualization environments 185

Nutanix virtualization environments 186

Nutanix cloud and partner solutions 189

Red Hat OpenShift virtualization environments 194

VMware virtualization environments 197

VMware cloud and partner solutions 198

Install core components 225

Install using the command line 238

Install Web Studio 256

Install VDAs 265

Configure Windows Defender Access Control related to VDA Installation 287

Precheck for VDA install and upgrade 289

Install VDAs using scripts 293

Third-party VDA deployment methods 296

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

Install VDAs using SCCM 296

Install VDAs using Microsoft Intune 314

Create a site 329

Create and manage connections and resources 333

Connection to AWS 350

Connection to Azure Local 367

Connection to XenServer® 368

Connection to Google cloud environments 372

Connection to HPE Moonshot 387

Connection to Microsoft Azure 390

Connection to Microsoft System Center Virtual Machine Manager 418

Connection to Nutanix 419

Connection to Nutanix cloud and partner solutions 430

Connection to Red Hat OpenShift 432

Connection to VMware 436

Connection to VMware cloud and partner solutions 446

Service accounts for machine identity management 446

On-premises Active Directory service accounts 447

Manage service accounts 449

Image management 451

Create prepared image machine catalogs 457

Create a prepared image machine catalog in Azure 458

Create a prepared image machine catalog in Red Hat OpenShift 468

Create a prepared image machine catalog in VMware 473

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

Manage prepared image machine catalogs **481**

Create machine catalogs **488**

Create an AWS catalog **518**

Create an Azure Local catalog **535**

Create a XenServer® catalog **536**

Create a Google Cloud Platform catalog **539**

Create an HPE Moonshot machine catalog **565**

Create a Microsoft Azure catalog **567**

Create a Microsoft System Center Virtual Machine Manager catalog **646**

Create a Nutanix catalog **651**

Create a Red Hat OpenShift catalog **659**

Create a VMware catalog **664**

Identity pools of different machine identity join types **670**

Identity pool of on-premises Active Directory joined machine identity **670**

Identity pool of Microsoft Entra hybrid joined machine identity **671**

Identity pool of non-domain-joined machine identity **676**

Manage machine catalogs **678**

Manage an AWS catalog **713**

Manage a XenServer® catalog **717**

Manage a Google Cloud Platform catalog **718**

Manage an HPE Moonshot catalog **724**

Manage a Microsoft Azure catalog **725**

Manage a Microsoft System Center Virtual Machine Manager catalog **745**

Manage a Nutanix catalog **746**

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

Manage a VMware catalog **751**

Power Management **753**

Power manage AWS VMs **753**

Power manage Azure Local VMs **756**

Power manage Azure VMs **757**

Power manage Red Hat OpenShift VMs **772**

Power manage Nutanix AHV VMs **772**

Security policies **773**

Security groups **773**

Secure Boot and vTPM **775**

Encryption capabilities **777**

Load balance machines **779**

Create delivery groups **781**

Manage delivery groups **794**

Create application groups **830**

Manage application groups **838**

Remote PC Access **845**

Cloud Connector Standalone Citrix Secure Ticketing Authority (STA) service **862**

Publish content **863**

Server VDI **868**

User personalization layer **870**

Remove components **886**

Upgrade and migrate **888**

Upgrade a deployment **892**

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

Proxy Support for VDA Upgrade Agent **917**

Secure **919**

FIDO2 and WebAuthn authentication **920**

Integrate Citrix Virtual Apps and Desktops™ with Citrix Gateway **926**

Security considerations and best practices **927**

Manage certificates **938**

Smart cards **959**

Smart card deployments **966**

Pass-through authentication and single sign-on with smart cards **973**

Enable TLS on Delivery Controllers **974**

Enable TLS on Web Studio and Director **979**

Enable TLS / DTLS on VDAs **985**

Enable TLS on Universal Print Server **1003**

Virtual channel allow list **1013**

WebSocket communication between VDA and Delivery Controller™ **1017**

HDX™ connectivity **1019**

Adaptive transport **1020**

Enlightened Data Transport **1024**

Troubleshooting **1025**

HDX™ Direct **1029**

Certificate management **1034**

NAT Compatibility **1038**

Troubleshooting **1041**

Secure HDX™ **1044**

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

Network telemetry **1047**

Virtual channel allow list **1050**

Troubleshooting **1054**

Known third-party virtual channels **1057**

Virtual Channel Allow List for DVC **1058**

Devices **1060**

Scanning **1061**

TWAIN Redirection **1061**

WIA devices **1064**

Scanning on non-windows client platforms - SANE Redirection **1065**

USB devices **1068**

Configuration **1070**

Composite Devices and Device Splitting **1076**

Troubleshooting **1080**

USB Diagnostics Tool **1085**

Legacy USB Redirection Configuration **1090**

Generic USB redirection and client drive considerations **1095**

Client Drive Mapping (CDM) **1098**

Support for mobile and touch screen client devices **1099**

Serial ports **1104**

Specialty keyboards **1109**

Support key event sequence processing in Windows VDA for double hop **1111**

Windows - Keyboard & IME Supportability Tool **1112**

Webcams **1113**

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

Graphics **1114**

An introduction to Thinwire **1116**

HDX™ 3D Pro **1116**

GPU Acceleration **1120**

10-Bit High Dynamic Range (HDR) **1122**

Adaptive Refresh Rate **1124**

Loss tolerant mode for graphics **1126**

HDX™ Screen sharing **1127**

Virtual display layout **1131**

Text-based watermark **1134**

Thinwire **1136**

Thinwire Analysis **1137**

Thinwire Configuration **1138**

Thinwire Full Screen Encoder **1140**

When to Use the Full Screen Encoder? **1140**

Configuration **1141**

Monitoring **1141**

Deprecated Policy - Optimize for 3D Graphics Workload **1143**

Additional Notes **1143**

Overview **1144**

When to use Thinwire Selective Encoding **1144**

Configuration **1145**

Build to Lossless **1147**

When to Use the Regular Build to Lossless? **1148**

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

Intelligent Build to Lossless **1149**

Comparing Graphics Modes - Intelligent BTL vs. BTL vs. Always Lossless **1149**

Prerequisites **1150**

When to Use the Intelligent Build to Lossless? **1151**

How it works? **1152**

Configuration **1153**

Monitoring Intelligent Build to Lossless **1154**

Troubleshooting **1158**

Overview **1159**

When to use do not use a video codec **1160**

Configuration **1160**

Always Lossless mode **1161**

Color space **1164**

Configuration **1165**

Requirements **1166**

High resolution displays **1167**

DPI scaling **1168**

GPU **1169**

Performance and scalability considerations **1170**

Known issues **1170**

Loss tolerant mode for graphics **1171**

When to use loss tolerant mode for graphics **1171**

System Requirements **1172**

Configuration **1172**

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

HDX™ Graphics Superresolution Upscaling (Preview) **1173**

How it works? **1174**

System Requirements **1175**

Configuration **1176**

Monitoring and Troubleshooting **1177**

Seamless **1179**

Applications **1181**

Create application groups **1203**

Publish content **1211**

App packages **1216**

Universal Windows Platform Apps **1230**

Publish applications **1233**

Windows Accessibility Settings **1235**

Prerequisites **1237**

How to enable **1237**

Window Dragging **1238**

Troubleshooting **1238**

System Tray Icon Redirection **1250**

Multimedia **1251**

Audio features **1255**

Browser content redirection **1266**

Single sign-on support **1280**

HDX™ video conferencing and webcam video compression **1289**

HTML5 multimedia redirection **1292**

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

Optimization for Microsoft Teams (New) **1295**

Citrix HDX™ Optimization **1297**

New VDI solution for Teams **1303**

Optimization for Microsoft Teams (Classic) **1310**

Monitor, troubleshoot, and support Microsoft Teams **1352**

Windows Media redirection **1359**

Virtual Channel Plugin Manager **1360**

Virtual Channel Plugin Manager **1361**

Virtual Channel Plugin Manager **1362**

Unified Communications SDK Optimization **1365**

General content redirection **1373**

Client folder redirection **1373**

Client location redirection **1374**

Bidirectional content redirection **1376**

Host to client redirection **1379**

Local App Access and URL redirection **1383**

Overview **1391**

Citrix Universal™ Print Driver (UPD) **1391**

Configuration **1393**

Client printer redirection **1393**

Citrix Universal™ Print Server (UPS) **1395**

Network Printers (on the VDA) **1397**

Troubleshooting **1398**

Best practices **1403**

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

Policies 1404

Work with policies 1406

Policy templates 1410

Create policies 1413

Policy sets 1422

Compare, prioritize, and troubleshoot policies 1426

Default policy settings 1431

Policy settings reference 1461

ICA® policy settings 1465

Auto client reconnect policy settings 1475

Audio policy settings 1477

Bandwidth policy settings 1479

Bidirectional content redirection policy settings 1485

Browser content redirection policy settings 1493

Client sensors policy settings 1497

Desktop UI policy settings 1498

End user monitoring policy settings 1500

Enhanced desktop experience policy setting 1501

File Redirection policy settings 1502

Overview 1507

Configuration 1508

Clipboard Format control 1510

Standard clipboard data formats 1512

Data Exchange formats 1514

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

Special & System Formats **1515**

Citrix Virtual Apps and Desktops™ clipboard formats **1516**

Custom Clipboard Format **1516**

Convertible clipboard formats **1517**

Clipboard transfer size limits **1519**

Cross session Clipboard Exchange (Preview) **1521**

Configuration **1522**

Policy and registry priority **1525**

Scenarios and use case examples **1527**

Graphics policy settings **1528**

Caching policy settings **1536**

Keep alive policy settings **1536**

Local App Access policy settings **1537**

Mobile experience policy settings **1538**

Multimedia policy settings **1539**

Multi-stream connections policy settings **1548**

Port redirection policy settings **1551**

FIDO2 redirection **1552**

Printing policy settings **1552**

Client printers policy settings **1556**

Drivers policy settings **1560**

Universal Print Server policy settings **1562**

Universal printing policy settings **1568**

Security policy settings **1571**

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

Server limits policy settings 1572

Session limits policy settings 1573

Session reliability policy settings 1575

Session watermark policy settings 1577

Time zone control policy settings 1581

TWAIN devices policy settings 1582

USB devices policy settings 1583

Virtual channel allow list policy settings 1592

Visual display policy settings 1594

Moving images policy settings 1596

Still images policy settings 1598

WebSockets policy settings 1600

WIA devices policy settings 1600

HDX™ features managed through the registry 1601

Load management policy settings 1615

Profile Management policy settings 1617

Advanced policy settings 1617

Basic policy settings 1627

Cross-platform policy settings 1631

File system policy settings 1633

Exclusions policy settings 1633

Synchronization policy settings 1635

Folder redirection policy settings 1637

AppData(Roaming) policy settings 1638

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

Contacts policy settings 1639

Desktop policy settings 1639

Documents policy settings 1640

Downloads policy settings 1641

Favorites policy settings 1641

Links policy settings 1642

Music policy settings 1642

Pictures policy settings 1643

Saved Games policy settings 1644

Start menu policy settings 1645

Searches policy settings 1645

Video policy settings 1646

Log policy settings 1647

Profile handling policy settings 1651

Registry policy settings 1655

Streamed user profiles policy settings 1656

User personalization layer policy settings 1659

Virtual Delivery Agent policy settings 1659

HDX™ 3D Pro policy settings 1661

Monitoring policy settings 1662

Virtual IP policy settings 1667

Workspace Environment Management™ policy settings 1668

Configure COM Port and LPT Port Redirection settings using the registry 1668

Policy changes 1669

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

Manage 1670

Applications 1672

App packages 1695

Universal Windows Platform Apps 1710

Backup or Migrate your configuration 1712

Backup and Restore configuration 1714

Backup and Restore using Web Studio 1716

Backup and Restore using the Automated Configuration tool 1722

Best practices for backup and restore 1726

Migrate configuration to Citrix Cloud™ 1727

Merging multiple sites into a single site 1741

Migrating from cloud to cloud 1749

Migrate Cloud configurations to on-premises 1753

Migrate on-premises configurations to on-premises site 1755

Automated configuration tool cmdlets for migration 1757

Automated configuration tool cmdlets for backup and restore 1785

Troubleshoot Automated configuration and additional information 1803

Autoscale™ 1811

Get started with Autoscale™ 1813

Schedule-based and load-based settings 1826

Dynamic session timeouts 1849

Autoscaling tagged machines (cloud burst) 1852

User logoff notifications (formerly force user logoff) 1861

Analyze the effectiveness of Autoscale™ settings 1864

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

Broker PowerShell SDK commands **1867**

Citrix Insight Services **1870**

Citrix Scout **1881**

Collect a Citrix Diagnostic Facility (CDF) trace at system startup **1909**

Delegated administration **1912**

Delivery Controllers **1922**

Home page for Web Studio **1927**

IPv4/IPv6 support **1929**

Licensing for Citrix Virtual Apps and Desktops™ using Web Studio **1931**

Multi-type licensing **1935**

License Activation Service **1943**

Citrix Virtual Apps and Desktops™ telemetry data elements **1957**

FAQ for licensing **1976**

Local Host Cache **1991**

Monitor and manage machines and sessions using Search **2005**

Machine actions and columns **2012**

Session actions and columns **2024**

Manage security keys **2028**

Session resilience settings **2042**

Settings **2049**

Tags **2055**

User profiles **2066**

VDA registration **2072**

Virtual IP and virtual loopback **2083**

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

Zones **2087**

Remove broker user from the cache **2099**

Citrix Assistant application (Preview) **2100**

Monitor **2111**

Configuration logging **2113**

Event logs **2120**

Director **2120**

Install and configure **2126**

Advanced configuration **2130**

Configure PIV smart card authentication **2133**

Configure network analysis **2140**

Delegated administration and Director **2141**

Secure Director deployment **2144**

Configuring on-premises sites with Citrix Analytics for Performance™ **2147**

Independent release of Director for LTSR deployments **2156**

Site Analytics **2159**

Alerts and notifications **2170**

Application usage monitoring **2203**

Filter data to troubleshoot failures **2208**

Monitor historical trends across a site **2210**

Monitor Autoscale-managed machines **2216**

Troubleshoot deployments **2218**

Troubleshoot applications **2219**

Troubleshoot machines **2222**

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

Troubleshoot user issues **2231**

Diagnose session startup issues **2236**

Diagnose user logon issues **2241**

Diagnose Session Performance issues **2249**

Diagnose ended user sessions **2277**

Shadow users **2279**

Send messages to users **2281**

Resolve application failures **2281**

Restore desktop connections **2282**

Restore sessions **2283**

Run HDX™ channel system reports **2284**

Reset a user profile **2284**

Record sessions **2288**

Unified search for Hybrid multi-cloud deployments **2291**

Infrastructure monitoring **2297**

Getting started with Infrastructure Monitoring **2299**

Manage connections **2300**

Infrastructure dashboard **2302**

Application and Desktop Probing **2314**

Cost optimization **2322**

Cost savings **2328**

Workload rightsizing **2335**

Cost summary **2341**

Feature compatibility matrix **2345**

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

Data granularity and retention **2354**

Citrix Director failure reasons and troubleshooting **2365**

Secure Private Access integration with Director (Preview) **2386**

Citrix VDA Upgrade Service (VUS) - Tech Preview **2399**

Pre-requisites for Upgrading VDAs Using VUS **2400**

Monitoring and Troubleshooting **2403**

Introduction **2410**

Core Concepts **2411**

Centralized AOT Log Server **2414**

Log Server Recommendation **2415**

Minimum supported versions for Always on Tracing (AOT) **2419**

Installing and Configuring Log Server **2420**

Upgrade Log Server **2440**

Uninstall Log Server **2441**

Uploading the AOT logs from CVAD Core Components **2442**

Viewing and Using AOT Logs **2452**

AOT Logs availability across deployment scenarios **2458**

General Response Code for Log Server API **2460**

Troubleshoot Common Issues with Always On Tracing **2461**

FAQ **2472**

Known Issues and Limitations **2476**

Third party notice **2478**

Introduction **2478**

Architecture Overview **2479**

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

Centralized AOT Log Server **2482**

Installing and Configuring Log Server **2485**

Uninstall Log Server **2489**

Uploading the AOT logs from CVAD Core Components **2490**

General Response Code for Log Server API **2494**

Troubleshooting with AOT and Log Server **2496**

Best Practices for Using AOT **2496**

FAQ **2497**

Known Issues and Limitations **2497**

Third party notice **2498**

Third party notices **2498**

SDKs and APIs **2498**

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

What's new

July 7, 2026

About this release

Cumulative Update 2 (CU2) is the most recent update to the 2507 LTSR.

About Cumulative Update 2 (CU2)

About Cumulative Update 1 (CU1)

About 2507 LTSR (initial release)

Cumulative Update 2 (CU2)

August 26, 2026

Release date: Aug 18, 2026

About this release

Citrix Virtual Apps and Desktops™ 7 2507 LTSR Cumulative Update 2 (CU2) fixes more than 20 issues reported since the release of the 2507 LTSR.

2507 LTSR (general information)

2507 LTSR (features and upgrade information)

What's new in this release

Issues fixed in Citrix Virtual Apps and Desktops 7 2507 LTSR CU1

Known issues in this release

Deprecations and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 2507 LTSR CU2

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

New deployments

How do I deploy CU2 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU2 - using the CU2 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 2507 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU2 provides updates to 15 baseline components of the 2507 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU2. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU2. If Citrix Provisioning isn't part of your deployment, you do not need to install or update it.

2507 LTSR CU2 baseline components

2507 CU2 baseline component	Version as shown in Programs and Features	Documentation
Single-session VDA	2507.0.2100.2123	Single-session VDA
Multi-session VDA	2507.0.2100.2123	Multi-session VDA
Delivery Controller	2507.0.2100.2123	Delivery Controller
Citrix Studio	7.45.2100.30	Citrix Studio
Citrix Director	7.45.2100.27	Citrix Director
Citrix Group Policy Management	7.45.2100.25	Citrix Group Policy Management
Citrix Group Policy Client-Side Extension	7.45.2100.25	
Citrix StoreFront	2507.0.2100.9	Citrix StoreFront
Universal Print Server	7.45.2100.62	Universal Print Server
Session Recording	25.7.2100	Session Recording

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

2507 CU2 baseline component	Version as shown in Programs and Features	Documentation
Linux VDA	24.02.1100.21	Linux Virtual Delivery Agent
Profile Management	25.7.2100.46	Profile Management
Citrix Federated Authentication Service	10.21.2100.15	Citrix Federated Authentication Service (FAS)
Browser Content Redirection	15.59.2100.66	Browser Content Redirection
Citrix Probe Agent	7.45.2100.15	Download

2507 LTSR CU2 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They aren't eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 2507 environments.

Compatible components and features	Version as shown in Programs and Features	Documentation
App Layering	2206.0.0	Citrix App Layering
HDX RealTime Optimization Pack	2.9.400.2702	HDX RealTime Optimization Pack
License Server	11.17.2.0_BUILD_56200	License Server
User personalization layer	26.3.3	User personalization layer
Session Recording web player	25.7.2100.16	Session recording web player
Microsoft Teams optimization	15.32.1000.9	Microsoft Teams optimization
Workspace Environment Management	2507.1.110.1	Workspace Environment Management
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only	Documentation
VDA 2411 or higher installed on Windows Server 2025 with a CVAD 2507 CUx Delivery Controller	2411.x.x.x	Documentation
Secure Private Access	25.11.200.4	Documentation
uberAgent	7.4.2.6688	Documentation

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

Compatible components and features	Version as shown in Programs and Features	Documentation
deviceTRUST	26.3.100.36	Documentation

2507 LTSR CU2 notable exclusions

The following features, components, and platforms aren't eligible for 2507 lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

What's new

August 26, 2026

There are no new features and enhancements in Citrix Virtual Apps and Desktops™ 7 2507 LTSR Cumulative Update 2 (CU2).

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

Fixed issues

September 3, 2026

The following issues have been fixed since Citrix Virtual Apps and Desktops™ 7 2507 LTSR CU1.

Citrix Director

- When the Citrix Director Shadowing invitation file path is hardcoded to `C:\\Users\\Public\\Documents` and GPO restrictions block access to this folder on the VDA, Citrix Director Shadowing might fail.
  To set the custom path, create a `REG_SZ` value named `ShadowSessionFilePath` under `HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\Director` and set it to the desired folder path (for example, `C:\\ShadowSessions`) on the VDA. [CVADHELP-32927]
- When network latency exceeds the actual ICA RTT, Citrix Director might display inflated ICA RTT values, causing a discrepancy between the Director UI dashboard and the Monitoring OData database values. [CVADHELP-28599]
- When the DDC FQDN contains mixed-case characters, Citrix Director might fail to collect infrastructure monitoring metrics from that DDC and display it as disconnected. [CVADHELP-27454]
- After you apply recent Microsoft OS security patches, you might not be able to use Citrix shadowing. [CVADHELP-31111]

Citrix Policy

- After each policy refresh or VDA registration, the Group Policy Client-Side Extension (CseEngine) might add duplicate App-V application entries to the `ApplicationStartDetails` registry value, causing the list to grow indefinitely. [CVADHELP-32805]
- When the VDA FQDN query fails during the Group Policy Client-Side Extension (CseEngine) initialization, VDAs might intermittently stop reporting CPU, Memory, and Disk load indexes, causing all sessions to be brokered to a single server. [CVADHELP-28688]
- When you configure session printers using MMC Citrix Studio, Web Studio might display only one session printer instead of all configured printers. [CVADHELP-32281]

Citrix Studio

- When you import Active Directory user or machine mappings from a CSV file, the import might fail with a "Usernames not found"error. [CVADHELP-30186]

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

- You might not be able to perform actions in Web Studio, such as managing tags, when your Desktop Delivery Controller has SSL binding configured to a specific IP address and the Citrix Orchestration service incorrectly uses the localhost IP address. [CVADHELP-31097]
- In certain Active Directory environments, you might receive an "invalid token"error when signing in to on-premises Web Studio and cannot access the console. [CVADHELP-31403]
- Web Studio might not correctly discover or display forests and domains that are reachable through external or one-way forest trusts.

Delivery Controller

- When you assign app packages containing updated namespaces (such as uap3) to a delivery group in Web Studio, app discovery might fail, preventing the applications from appearing in Web Studio for assignment to delivery groups. [CVADHELP-30250]
- When a configuration synchronization occurs without significant licensing changes, the High Availability Service might unnecessarily trigger License Activation Service (LAS) requests. [CVADHELP-31584]
- After you upgrade through VUS, sessions might fail to launch due to a policy evaluation error in CVAD. [CVADHELP-32389]
- When you install a VDA through the command line using a WebSocket enrollment token, the VDA installation might fail with "Invalid token"errors. [CVADHELP-31168]
- You might experience a `TokenNotFoundException` that prevents an application from launching when your device starts the application launch but does not support session sharing. [CVADHELP-31578]
- The weekly Broker usage telemetry payload might not include the "VDAs.RebootScheduleEnabled" datapoint. [CVADHELP-29635]
- When you upgrade a Delivery Controller to version 2507, Web Studio might display "Your software maintenance has expired,"and VDA sessions might display "Your corporate Citrix environment is currently unsupported,"even with valid licenses. [CVADHELP-29639]
- When launching an App-V application for the first time, a timing conflict during package synchronization might prevent the application from launching. [CVADHELP-31381]
- When users have only dbo permissions, the upgrade might fail. [BRK-25326]
- When the stored license service connection key becomes invalid, the Configuration Service might silently stop reporting telemetry data. [CVADHELP-33949]
- In SCCM and MCS environments, a leftover configuration file might not be cleaned up during image preparation, which can lead to machine identity conflicts in provisioned VMs. [CVADHELP-31444]
- When updating an MCS machine catalog on VMware, the vmx-21 hardware version might cause the PCI slot layout to shift between the MCS master image and the provisioned VDA, resulting in loss of network connectivity on the VDA. [CVADHELP-32936]

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

Machine Creation Service

- On Nutanix Prism Central, adding machines to an existing MCS catalog might fail when the environment has more than 500 subnets. [CVADHELP-31937]
- MCS might incorrectly change the Windows time synchronization type from NT5DS to NTP on domain-joined VMs. [CVADHELP-30209]
- On Nutanix, MCS-provisioned VMs might not retain the hardware virtualization setting from the master image, preventing Docker from running inside VDIs. [CVADHELP-33531]
- When an existing VM has a PCI bus-type disk attached, MCS catalog creation on Nutanix might fail to display provisioned VMs. [CVADHELP-33058]
- Nutanix MCS VDAs might show power status as "Unknown"in Citrix Studio due to an exception in the AHV PC plugin. [CVADHELP-33840]

Graphics

- With a single monitor, you might see incorrect HDX 3D Pro full-screen warnings when HDX 3D Pro is disabled. [CVADHELP-30880]
- After you reconnect to a session, your saved virtual display layout might not be applied. [CVADHELP-30818]
- After you reconnect with multiple monitors, Windows 11 app windows might become hidden. [CVADHELP-30815]
- When you set **Use local time of client** to **Use client time zone**, the watermark time zone might not sync. You might need to disconnect and reconnect the session for the watermark to update. [CVADHELP-29921]
- Published applications might disappear after disconnecting a secondary monitor during a multi-monitor session. [CVADHELP-32299]

Universal Print Server

Printing

- When you print PDF documents with Enhanced Metafile (EMF) using Citrix UPD in XenApp or XenDesktop sessions, icons might display incorrect or swapped colors. [CVADHELP-30837]

VDA for single-session OS

Session/Connection

- Browser Content Redirection might stop working unexpectedly due to an internal service crash. [CVADHELP-31963]

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

- When Drag and Drop is enabled on Published Desktops, mouse clicks on a small rectangular area on the left side of the screen might not register correctly. [CVADHELP-31919]
- When a seamless application takes time to start, its icon might not appear correctly in the taskbar. [CVADHELP-31687]
- When using UDP audio, you might experience outbound audio drops or hear beeping sounds. [CVADHELP-30820]
- When you launch Outlook Classic as a seamless application on VDA 2507 LTSR, Outlook toast notifications might not appear upon receiving an email. [CVADHELP-30789]
- When you launch an application from Citrix StoreFront, the launch might fail and display the following error message: "Cannot Start App: {app name}". [CVADHELP-30614]
- When Enhanced Single Sign-On with domain passthrough is enabled in a double-hop environment, published applications might fail to launch. [CVADHELP-30596]
- When checking a device's remaining power from within a session, the battery status indicator might not be visible. [CVADHELP-29230]
- When starting a new session, machines might intermittently hang at the welcome screen. [CVADHELP-28986]
- Copy and paste functionality between client and VDA might stop working intermittently during a HDX session, requiring a session reconnect to restore. [CVADHELP-29653]
- A Citrix VDA background service might prevent Windows update from completing its restart, causing Intune-initiated reboots to remain in a pending state. [CVADHELP-32191]
- When you use multiple parallel HDX sessions, clipboard operations between sessions might intermittently fail. [CVADHELP-31591]
- Clipboard operations might fail with a memory error when working across multiple concurrent Citrix sessions. [CVADHELP-32418]

System Exceptions

- After uninstalling VDA 2507 CU1 and rebooting the machine, RDP logon might fail, making the machine inaccessible. [CVADHELP-31644]
- When using VDA 2203 CU5 on AMD Turin-based hosts, a blue screen might occur during client disconnections. [CVADHELP-29628]
- Published Internet Explorer might close immediately at launch. [CVADHELP-30680]
- When a timing conflict occurs between the VDA Upgrade Agent (VUA) and the installer while deleting XenDesktopVDASetup.exe, the VUA might resume an upgrade on a VDA that has already completed its upgrade. [CVADHELP-31718]
- The Broker service might incorrectly report non-CVAD expired licenses, affecting license reporting accuracy. [CVADHELP-32258]
- When the Broker service enumerates applications or desktops, it might crash, affecting service availability. [CVADHELP-32259]

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

VDA for multi-session OS

Session/Connection

- When Drag and Drop is enabled on Published Desktops, mouse clicks on a small rectangular area on the left side of the screen might not register correctly. [CVADHELP-31919]
- When a seamless application takes time to start, its icon might not appear correctly in the taskbar. [CVADHELP-31687]
- The Citrix Audio Redirection Service might stop responding, causing session-level service disruptions until you restart the service. [CVADHELP-31363]
- After upgrading to the Citrix Workspace app for Windows 2309 and later, virtual apps and desktops might not launch as expected. [CVADHELP-30656]
- Citrix Audio Redirection might stop working intermittently, requiring a service restart to restore audio functionality. [CVADHELP-30160]
- In a dual-hop ICA setup with Windows Defender Credential Guard enabled, attempts to launch published applications or desktops might fail. [CVADHELP-30596]
- When you reconnect to an active session using VDA 2507 or 2603, copy and paste from the VDA to the client might stop working. [CVADHELP-30717]
- After upgrading the VDA to 2507, a black screen might appear during session startup when connecting via an HDX session. [CVADHELP-29373]
- If user logon takes longer than expected, HDX Direct might fail to activate for the session in VDA 2402 LTSR and VDA 2507 LTSR CU2 and later. [CVADHELP-31372]
- When checking a device's remaining power from within a session, the battery status indicator might not be visible. [CVADHELP-29230]
- On certain versions of Citrix Workspace app, a black screen might appear when you launch a virtual app or desktop. [CVADHELP-29087]
- You might experience intermittent Desktop Service re-registrations and reconnect failures. [CVADHELP-28137]
- When you launch Outlook Classic as a seamless application on VDA 2507 LTSR, Outlook toast notifications might not appear upon receiving an email. [CVADHELP-30789]
- You might be unable to sign in, and processes might stall, due to issues with the Citrix Audio Redirection service. [CVADHELP-28046]
- When Local App Access is enabled on Windows Server 2025, an unexpected folder integration prompt might appear at logon after installing Windows security update. [KB5075899], [CVADHELP-31880]
- In multi-session VDAs, inconsistent microphone audio performance might delay audio capture. [CVADHELP-32611]
- When the number of MSIX applications on a VDA reaches approximately 250, the Broker's PrepareSession request might exceed VDA communication limits, causing VDAs to deregister during session launch. [CVADHELP-33466]

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

- After you apply a recent Microsoft update, audio might not work on VDA for multi-session OS. [KB5094126], [HDX-107318]

System Exceptions

- The Profile Management service might fail to process logoff operations correctly on multi-session VDAs, leading to profile corruption or settings not being saved. [CVADHELP-30680]
- After uninstalling VDA 2507 CU1 and rebooting the machine, RDP logon might fail, making the machine inaccessible. [CVADHELP-31644]
- When using VDA 2203 CU5 on AMD Turin-based hosts, a blue screen might occur during client disconnections. [CVADHELP-29628]
- The Broker service might incorrectly report non-CVAD expired licenses, affecting license reporting accuracy. [CVADHELP-32258]

Linux VDA

For information about the fixed issues, see the Fixed issues article in its own document.

Profile Management

For information about the fixed issues, see the Fixed issues article in its own document.

Session Recording

For information about the fixed issues, see the Fixed issues article in its own document.

StoreFront

For information about the fixed issues, see the Fixed issues article in its own document.

Cumulative Update 1 (CU1)

August 26, 2026

Release date: December 16, 2025

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

About this release

Citrix Virtual Apps and Desktops™ 7 2507 LTSR Cumulative Update 1 (CU1) fixes more than 20 issues reported since the initial release of the 2507 LTSR.

2507 LTSR (general information)

2507 LTSR (features and upgrade information)

What's new in this release

Issues fixed in Citrix Virtual Apps and Desktops 7 2507 LTSR (initial release)

Known issues in this release

Deprecations and removals

Citrix Product Subscription Advantage Eligibility Dates

Downloads

Citrix Virtual Apps and Desktops 7 2507 LTSR CU1

New deployments

How do I deploy CU1 from scratch?

You can set up a brand-new Citrix Virtual Apps and Desktops environment based on CU1 - using the CU1 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the Citrix Virtual Apps and Desktops 7 2507 LTSR (initial release) section and pay close attention to the Technical Overview, Install and Configure, and Security sections before you start planning your deployment. Ensure your setup meets the system requirements for all components.

Existing deployments

What do I update?

CU1 provides updates to 15 baseline components of the 2507 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU1. For example: If Citrix Provisioning is part of your LTSR deployment, update the Citrix Provisioning components to CU1. If Citrix Provisioning isn't part of your deployment, you do not need to install or update it.

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

2507 LTSR CU1 baseline components

2507 CU1 baseline component	Version as shown in Programs and Features	Documentation
Single-session VDA	2507.0.1100.167	Single-session VDA
Multi-session VDA	2507.0.1100.167	Multi-session VDA
Delivery Controller	2507.0.1100.167	Delivery Controller
Citrix Studio	7.45.1100.55	Citrix Studio
Citrix Director	7.45.1100.50	Citrix Director
Citrix Group Policy Management	7.45.1100.59	Citrix Group Policy Management
Citrix Group Policy Client-Side Extension	7.45.1100.59	
Citrix StoreFront	2507.0.1100.61	Citrix StoreFront
Universal Print Server	7.45.1100.81	Universal Print Server
Session Recording	25.7.1100	Session Recording
Linux VDA	24.02.1100.21	Linux Virtual Delivery Agent
Profile Management	25.7.1100.35	Profile Management
Citrix Federated Authentication Service	10.17.1100.16	Citrix Federated Authentication Service (FAS)
Workspace Environment Management	2507.1.110.1	Workspace Environment Management
Browser Content Redirection	15.59.1100.77	Browser Content Redirection
Citrix Probe Agent 2206	7.45.1100.29	Download

2507 LTSR CU1 compatible components

The following components - at the versions given below - are compatible with LTSR environments. They aren't eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 2507 environments.

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

Compatible components and features	Version as shown in Programs and Features	Documentation
App Layering	2206.0.0	Citrix App Layering
HDX RealTime Optimization Pack	2.9.400.2702	HDX RealTime Optimization Pack
License Server	11.17.2.0_BUILD_48000	License Server
User personalization layer	25.7.0	User personalization layer
Session Recording web player	25.7.1100.20	Session recording web player
Microsoft Teams optimization	15.32.1000.9	Microsoft Teams optimization
XenApp & XenDesktop 7.15 LTSR VDA (latest release)*	Latest Cumulative Update only	Documentation
VDA 2411 or higher installed on Windows Server 2025 with a CVAD 2507 CUx Delivery Controller	2411.x.x.x	Documentation
Secure Private Access	24.12.100.20	Documentation
uberAgent	7.4.2.6688	Documentation
deviceTRUST	25.7.200.0	Documentation

2507 LTSR CU1 notable exclusions

The following features, components, and platforms aren't eligible for 2507 lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

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

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

What's new

August 26, 2026

The following new features and enhancements are available in Citrix Virtual Apps and Desktops™ 7 2507 LTSR Cumulative Update 1 (CU1):

Integration with Nutanix Prism Central on AHV

You can now connect Citrix Virtual Apps and Desktops 2507 CU1 and later 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

Automated LocalDB installation for Delivery Controller upgrades

When you upgrade Delivery Controllers, the metainstaller automatically installs the latest supported SQL Server Express LocalDB version. This enhancement streamlines your upgrade process. It ensures

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

compatibility for the Local Host Cache database without manual LocalDB installation. For more information, see Automatic update.

WIA Redirection enhancements

Admins can now enable and configure WIA redirection inside HDX sessions through a single Studio policy—no additional registry key configuration on the VDA required.

Virtual Delivery Agents (VDAs)

New Meta Installer for Single Session Core Service Virtual Delivery Agent

A new lightweight Single-Session VDA Meta Installer is now available for Windows 365 Cloud PC and Remote PC deployments. This installer is built on the existing Remote PC installer and serves as a streamlined version of the full Single-Session VDA, delivering essential VDA components along with Profile Management, deviceTRUST, uberAgent, WEM, Backup and Restore, and the VDA Upgrade Agent. It significantly reduces package size and improves installation reliability for cloud-based workloads. Designed for modern Remote PC scenarios, this installer provides a simplified and high-performance option for deploying Citrix workloads on Windows 365 and Remote PC.

Citrix Always on Tracing

Citrix AOT for all CVAD components

The latest update introduces a major expansion of Always-On Tracing (AOT), making it easier to collect, centralize, and analyze logs across the entire Citrix environment. A new configuration experience in Web Studio lets admins define the log server, control the logging scope, and enable Director access from one place, with all settings automatically propagated through the Site database. Director now includes a dedicated Logs view, giving admins real-time visibility into AOT events with search, time filters, categories, severity filters, and machine-level filtering. AOT coverage has been extended to more Citrix components, including all core components with Mac VDAs, Linux VDAs, FAS, and Session Recording Server and more, enabling true end-to-end tracing across control and data plane workflows.

The AOT Log Server has been enhanced with improved ingestion performance and more efficient storage using **LZ4 compression**. The architecture supports a **single Log Server per environment**, capable of handling **up to 128,000 active component connections** and **10,000 log events per second**, which is sufficient for most deployments. Updated sizing guidance and performance baselines help administrators plan capacity and tune storage and IOPS based on their environment. Standalone

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

components can now send logs to the Log Server using simple PowerShell commands, aligning them with the centralized logging model. Learn more and start your deployment here.

Exclude draining machines from autoscale calculations

You can now exclude machines undergoing draining due to reboot schedules from Autoscale capacity calculations. This prevents over-provisioning, helping you optimize resource usage. To activate this behavior, set the `ExcludeNaturalRebootDrainingFromAutoscale` property to `True` on your multi-session delivery groups.

This feature applies only to:

- Multi-session OS delivery groups.
- Reboot schedules configured with **Graceful restart** for Cloud or "**Re-start all machines after draining session**"for On-premises deployments.

For example, consider a delivery group with 10 active sessions. Two machines are draining for a scheduled reboot. Previously, Autoscale might count these two draining machines as available, potentially leading to over-provisioning of new machines. With this feature, Autoscale recognizes and ignores the draining machines. It only counts the truly available capacity. This ensures your Autoscale policy accurately provisions resources, preventing unnecessary infrastructure costs.

Fixed issues

August 20, 2026

The following issues have been fixed since Citrix Virtual Apps and Desktops™ 7 2507 LTSR (initial release).

Citrix Director

- The target VDA CPU usage might increase significantly when you keep in Director Session Performance Tap page. [CVADHELP-29162]
- When you groom the `SessionMetricsV2` and `EndpointMetricsV2` tables in an on-premises environment, the task fails due to insufficient ALTER permissions. [CVADHELP-29318]
- During session logon testing on a Windows 11 VDI running Citrix 2507 LTSR, the Appx package load metrics failed to populate due to an event conversion error. [CVADHELP-29332]
- You might face issues with the Appx package load metrics during session logon testing on a Windows 11 VDI running in Citrix 2507 LTSR, due to an event conversion error. [CVADHELP-29332]

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

Citrix Policy

- The Citrix group policy might fail to apply to Windows 365 (W365) VDA machines. [CVADHELP-27655]

Citrix Studio

- When you add a Delivery Group (DG) to the log server in version 2511.0.10.23, the DG selection resets after navigating between nodes, requiring administrators to manually re-select it. [CVADHELP-29696]
- You might encounter a "Requested value 'MaxCapacityVerticalLoadBalancing'was not found" error. The filter for "MaxCapacityVerticalLoadBalancing"does not work when DDC versions are older than R125. [CVADHELP-29445]
- When you create an Azure catalog in Citrix Studio and select "Azure ephemeral OS disk"as the storage type, the machine size list incorrectly shows "No results."[CVADHELP-29564]
- When you attempt to log in to WebStudio, you might see an error caused by invalid tokens when domain names contain special characters. [CVADHELP-28119]
- Upgrade scripts for packaged applications might not automatically populate all necessary details, requiring manual input to ensure complete configurations.[APPV-834]

Delivery Controller

- When you add a host in MMC Studio with a custom SDK port, you might encounter an error due to the non-default port configuration. [CVADHELP-29385]
- When you upgrade a site from versions 2203 CU6 or 2402 CU2 to 2507 CU1, the upgrade might fail with an authorization error because the Delegated Admin Service is not registered. [CVADHELP-29816]
- After you upgrade to version 2507, the Configuration Service might time out when connecting to the Telemetry Service, preventing you from accessing Director and other site management consoles. [CVADHELP-29849]
- When you create or update a catalog for AD-joined machines in Web Studio, you may see an error if the identity pool domain differs from the admin domain. [CVADHELP-29374]
- When you publish apps to multiple delivery groups simultaneously, an SQL exception might occur, preventing the app from being published. [CVADHELP-33069]
- When you upgrade to version 2507, the Configuration Service might time out when connecting to the Telemetry Service, preventing access to Director and other site management consoles. [CVADHELP-29849]

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

Machine Creation Service

- Citrix Host Service may fail to start automatically after a reboot in case the DDC can't contact Active Directory(AD) at that time (e.g. both DDC and AD are rebooted), requiring manual intervention to start the service. [CVADHELP-29495]
- When you change CPU cores using the Set-ProvScheme command or Web Studio in a Nutanix Acropolis environment, the changes do not apply to new machines. [CVADHELP-28714]
- When upgrading DDC from 2402 CU1 to 2507, the installer may fail due to Azure Arc plugin timeout. [CVADHELP-29787]

Universal Print Server

Printing

- Printing large files to pdf might fail. [CVADHELP-28116]

VDA for single-session OS

Session/Connection

- When you use the EDT protocol with HDX Direct connections, ICA sessions may disconnect and reconnect due to a cipher mismatch error. Switching to TCP temporarily resolves the issue. [CVADHELP-29336]
- When you turn a monitor off and on during a session, the playback device name may switch to "Citrix HDX Audio,"causing identification issues. [CVADHELP-28903]
- Communication with the VDA might fail, when you use the Nexthink client. [HDX-93834]
- You might see delay with cloud hosted VDAs while using SANE redirection. [HDX-92652]

System Exceptions

- During the uninstallation of the Virtual Delivery Agent (VDA) in Citrix Virtual Apps and Desktops (CVAD) 2507 LTSR, uberAgent is always removed, even if the `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\uberAgent\InstalledBy` flag is not set to CVAD. [CVADHELP-29182]
- When you publish App-V applications, you cannot move them afterward due to technical limitations in the underlying mechanism. [CVADHELP-29136]
- You might experience BSOD with error on icausbb.sys on rebooting PVS Provisioned VDAs. [CVADHELP-27597]

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

- When you use a dual-monitor setup and share a popped-out browser window, the audience can see the parent browser in the background. [CVADHELP-27809]
- Client time redirection is not working in Windows 11 single sessions VDA. [CVADHELP-28742]
- FIDO2 does now work for edgewebview2 by default. [CVADHELP-29040]
- When VDA uses IPV6, loopback IP is seen in studio for the "Connected through"field instead of NetScaler snip. [CVADHELP-29084]
- You might experience random BSOD crashes with `PAGE_FAULT_IN_NONPAGED_AREA SYSTEM_SERVICE_EXCEPTION`. [CVADHELP-29044]

VDA for multi-session OS

Session/Connection

- When you use the EDT protocol with HDX Direct connections, ICA sessions may disconnect and reconnect due to a cipher mismatch error. Switching to TCP temporarily resolves the issue. [CVADHELP-29336]
- When you disconnect and reconnect to your Citrix session on a Windows 11 multisession VDA, the time zone might reset regardless of your time zone settings. [CVADHELP-28781]
- When reconnecting to 2016/2022 RDS Double Hop published application from Dell-Wyse Thin OS 9.x, a 20 second delay is seen with Linux Citrix client 23.7. [CVADHELP-28831]
- Communication with the VDA might fail, when you use the Nexthink client. [HDX-93834]
- You might see delay with cloud hosted VDAs while using SANE redirection. [HDX-92652]

System Exceptions

- During the uninstallation of the Virtual Delivery Agent (VDA) in Citrix Virtual Apps and Desktops (CVAD) 2507 LTSR, uberAgent is always removed, even if the `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\uberAgent\InstalledBy` flag is not set to CVAD. [CVADHELP-29182]
- When you publish App-V applications, you cannot move them afterward due to technical limitations in the underlying mechanism. [CVADHELP-29136]
- You might experience BSOD with error on icausbb.sys on rebooting PVS Provisioned VDAs. [CVADHELP-27597]
- The VDA might become unresponsive due to the Winlogon process crash by TWI3.dll. [CVADHELP-27630]
- When you use a dual-monitor setup and share a popped-out browser window, the audience can see the parent browser in the background. [CVADHELP-27809]
- The TdIca.sys driver may intermittently cause BSOD crashes on Windows Server 2019 [CVADHELP-27893]

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

- FIDO2 does now work for edgewebview2 by default. [CVADHELP-29040]
- You might experience random BSOD crashes with `PAGE_FAULT_IN_NONPAGED_AREA SYSTEM_SERVICE_EXCEPTION`. [CVADHELP-29044]
- With 2507 LTSR, clipboard on multi-user desktops might stop working after a while. [CVADHELP-29644]
- With 2507 LTSR, you might see delay in session launch when network telemetry is enabled. [CVADHELP-30352]

Linux VDA

For information about the fixed issues, see the Fixed issues article in its own document.

Profile Management

For information about the fixed issues, see the Fixed issues article in its own document.

Session Recording

For information about the fixed issues, see the Fixed issues article in its own document.

StoreFront

For information about the fixed issues, see the Fixed issues article in its own document.

Citrix Virtual Apps and Desktops™ 7 2507 LTSR (Initial release)

August 26, 2026

The Long Term Service Release (LTSR) program for Citrix Virtual Apps and Desktops provides stability and long-term support for Citrix Virtual Apps and Desktops releases.

LTSRs are also available for Citrix Virtual Apps and Desktops 2402 and 2203.

This Citrix Virtual Apps and Desktops release includes new versions of the Windows Virtual Delivery Agents (VDAs) and new versions of several core components. You can:

- **Install or upgrade a site**: Use the ISO for this release to install or upgrade core components and VDAs. Installing or upgrading to the latest version allows you to use the latest features.

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

- **Install or upgrade VDAs in an existing site**: If you already have a deployment and aren't ready to upgrade your core components, you can still use several of the latest HDX features by installing (or upgrading to) a new VDA. Upgrading only the VDAs can be helpful when you want to test enhancements in a non-production environment.

  After upgrading your VDAs to this version, you do not need to update the machine catalog's functional level. For more information, see VDA versions and functional levels.

For installation and upgrade instructions:

- If you are building a new site, follow the sequence in Install and configure.
- If you are upgrading a site, see Upgrade a deployment.

Documentation for supported and legacy versions

Documentations for supported versions are in Citrix Virtual Apps and Desktops.

The End of Life (EOL) version documentation PDFs are archived in Legacy Documentation.

2507 LTSR initial release baseline components

2507 baseline component	Version as shown in Programs and Features	Documentation
Single-session VDA	2507.0.100.418	Single-session VDA
Multi-session VDA	2507.0.100.418	Multi-session VDA
Delivery Controller	7.45.100.130	Delivery Controller
Citrix Studio	7.45.100.143	
Web Studio	7.45.100.193	Web Studio
Citrix Director	7.45.100.130	Citrix Director
Citrix Group Policy Management	7.45.100.137	Citrix Group Policy Management
Citrix Group Policy Client-Side Extension	7.45.100.137	
Citrix StoreFront	2507.0.100.0	Citrix StoreFront
Citrix Provisioning	7.45.100.51	Citrix Provisioning
Universal Print Server	7.45.100.256	Universal Print Server
Session Recording	25.7.100.30	Session Recording

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

2507 baseline component	Version as shown in Programs and Features	Documentation
Session Recording Agent for Endpoint Devices 2507	27.7.0.7	Session recording for endpoint devices
Linux VDA	25.07.0.91	Linux Virtual Delivery Agent
Citrix Federated Authentication Service	10.21.100.45	Citrix Federated Authentication Service (FAS)
Citrix Probe Agent 2507		Download

2507 LTSR initial release compatible components

The following components - at the versions given below - are compatible with LTSR environments. They aren't eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 2507 environments.

Compatible components and features	Version as shown in Programs and Features	Documentation
HDX RealTime Optimization Pack	2.9.700	HDX RealTime Optimization Pack
License Server	v11.17.2 Build 53100	License Server
User personalization layer	25.3.3.4	User personalization layer
Session Recording web player	25.7.100.30	Session recording web player
Microsoft Teams optimization	15.59.100.245	Microsoft Teams optimization
Browser Content Redirection	15.59.100.244	Browser Content Redirection
Workspace Environment Management	2507.1.100.1	Workspace Environment Management
Profile Management	25.7.100.95	Profile Management
uberAgent	7.4.1.6602	uberAgent
deviceTRUST	25.7.100.2	deviceTRUST

2507 LTSR initial release notable exclusions

The following features, components, and platforms aren't eligible for 2507 lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to

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

excluded features and components are available through regular current releases.

Excluded components and features
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
StoreFront Citrix Online Integration

Excluded Windows platforms *
Windows 2008 32-bit (for Universal Print Server)

* Citrix reserves the right to update platform support based on third-party vendors' lifecycle milestones.

What's new

August 26, 2026

This article lists new and enhanced features for Citrix Virtual Apps and Desktops™ 7 2507 LTSR. Updates are organized by component.

Delivery Controller

License Server version compatibility with Citrix Virtual Apps and Desktops site

For Citrix Virtual Apps and Desktops site creation and upgrades, ensure that the License Server is running a minimum of version 11.17.2 build 53100.

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

Multimedia

Audio Quality Enhancer for EDT loss tolerant mode

Starting with the 2507 version, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio.

Single sign-on support for Browser Content Redirection Browser Content Redirection now offers a streamlined user experience with single sign-on support, enabling VDA-side authentication and cookie sharing. This enhancement eliminates redundant logins, boosting productivity by maintaining authentication and cookie persistence across BCR sessions, even after the BCR window is closed. This seamless experience further enhances security by ensuring authentication originates from the VDA, not the client.

For more information, see Browser Content Redirection documentation.

Server-side certificate validation for Browser Content Redirection Browser Content Redirection is further enhanced with certificate validation support. When accessing a redirected website from the client, the client overlay browser may not trust the certificate from the server or the MitM proxy. In such cases, BCR can now validate the Host or Proxy certificates against the VDA's certificate store.

For more information, see Server-side certificate validation documentation.

Virtual Delivery Agents (VDAs)

Passkey support for in-session applications

This enhancement allows users to register and use passkeys for authentication to applications within HDX sessions, eliminating the need for physical security keys.

Web Studio

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 using Web Studio. Alternatively, you can use PowerShell commands. For more information, see:

- Red Hat OpenShift virtualization environments
- Connection to Red Hat OpenShift

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

- Create a Red Hat OpenShift catalog

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 Web 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.

New login page settings

The **Settings** node in Web Studio now includes two options to enhance the Web Studio login experience:

- **Login page notice**: Display a custom message to share important information with administrators.
- **Show connected Delivery Controller**: Display the FQDN of the connected Delivery Controller for added visibility and transparency.

For more information, see Settings.

Citrix Director

Microsoft call quality dashboard for monitoring and troubleshooting

This feature enhances Citrix Director by providing administrators a unified view of Microsoft Teams call performance using Microsoft Graph API integration. It enables aggregate monitoring and troubleshooting, improving user experience by streamlining IT operations for Microsoft Teams in Citrix.

The dashboard shows call details and quality metrics for each participant session. You can distinguish between regular calls, video conferences, and other collaboration sessions.

For more information, see the Microsoft Teams documentation.

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

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 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.

Change in default policy behavior of the endpoint data collection used in Session topology

The default settings for the "Endpoint location data collection"and "Endpoint network latency measurement interval"policies are now disabled. These policies involve interactions with external cloud services. You can enable them in Studio to give administrators the details they need to troubleshoot Citrix performance issues reported by users.

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

Enhanced definitions of ICA RTT and Network latency measurements in Director

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.

For more information, see the HDX metrics documentation.

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

Enhanced visibility of plug-in manager and optimization state for real-time communication applications

Plug-in manager details for troubleshooting third-party optimization are now available for Zoom and Webex applications. Microsoft Teams Slimcore, Zoom, and Webex now show plug-in information and optimization state on the endpoint. This information helps administrators quickly identify causes of user experience issues.

The feature provides a plug-in manager and relevant Virtual Delivery Agent (VDA) details for troubleshooting. These details are available on supported client platforms in both on-premises and cloud deployments.

For more information, see Real-time communications optimization visibility documentation.

Machine Creation Services (MCS)

Power management of Azure Local VMs with Azure Arc plug-in

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 power management of VMs created on Azure Local.

For more information, see:

- Azure Local environments
- Connection to Azure Local
- Create an Azure Local catalog
- Power manage Azure Local VMs

Azure Local for Citrix Virtual Apps and Desktops 2507 LTSR is only available for customers with Hybrid Rights/Universal License.

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.

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

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.

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.

Autoscale

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.

Scout

Enhanced Scout functionality for StoreFront machines

Scout now supports displaying the **Add machine** button on the **Collect** page when running on StoreFront type machines starting from Citrix Virtual Apps and Desktops LTSR 2507. This enhancement enables you to manually add multiple StoreFront Server machines in the same cluster and trigger collection simultaneously, improving the efficiency of data collection across StoreFront deployments.

> **Note:**
>
> Older versions of TelemetryService do not support this feature.

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

Unicode keyboard layout mapping

- The feature "Unicode keyboard layout mapping"is prohibited by default in CVAD 2507, you can enable it through Group Policy. For more details, see Keyboard and Input Method Editor (IME)

Preview features

HDX graphics superresolution upscaling

Starting with the Citrix Workspace app for Windows 2507 version, the HDX graphics superresolution upscaling feature enhances session performance and significantly reduces bandwidth consumption.

HDX Graphics Superresolution upscaling seamlessly downscales video regions on the Virtual Desktop Agent (VDA) and utilizes a compatible endpoint Graphics Processing Unit (GPU) to upscale them back to their original resolution without noticeable quality degradation or performance impact.

For more information, see HDX Graphics Superresolution Upscaling.

Citrix Assistant application

The Citrix Assistant is an intuitive GUI tool that provides a simple, convenient experience, often requiring just a single click to significantly improve session performance or facilitate troubleshooting. You can now optimize system resources, perform network status checks with personalized recommendations, identify and terminate unresponsive applications, and manage storage by cleaning temporary files or deleting large items directly from the interface. It also includes hardware diagnostics for audio and camera devices. For information, see Citrix Assistant application (Preview).

Fixed issues

August 26, 2026

Citrix Virtual Apps and Desktops™ 7 2507 LTSR includes the following fixed issues.

> **Note:**
>
> Fixes to issues in previous versions of Citrix Virtual Apps and Desktops are included in this and subsequent releases.

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

General

- During the initial site setup, the Broker Service temporarily starts with License Activation Service setting set to `false` due to a delay in configuration sync from the Citrix Config Synchronizer Service (CSS). This results in a one-time error, resolved automatically after the sync completes. [BRK-22410]
- Delivery Controller™ fails to upgrade from Citrix Virtual Apps and Desktops 2402 CU1 to 2503. [BRK-22408]
- A memory leak in the Broker Service might happen because of the WCF connection to the FMA trust service. [BRK-22441]
- Machines on GoCloud can sometimes hibernate or shut down while in use. [BRK-21894]
- Previously, sessions could not be launched on machines with incorrect or missing hypervisor HostedMachineID values (resulting in their PowerState or FaultState being `VirtualMachineNotFound`). Sessions can now be launched on these machines provided they are powered-on and registered. [BRK-22391]
- Installing VDA 2507 LTSR EAR2 fails if an existing version of uberAgent® was installed independently of the VDA MetaInstaller. As a workaround, you can uninstall the existing uberAgent before installing VDA 2507 LTSR EAR2. The installer will then deploy the required uberAgent version.[HDX-88963]
- When you use the Citrix Workspace™ app to access the VDA with Unicode input mode enabled, and either the "Unicode keyboard layout mapping"or "Automatic keyboard display"group policy is turned on, you might notice reduced performance in Microsoft Excel when scrolling through large pages. This issue occurs because UIAutomation APIs are incompatible with Excel.[HDX-91618]
- A new option **A restart before installation is recommended** is added to the meta installer when uninstalling the VDA agent. However, the checkbox does not function correctly, and you are advised not to use it.[HDX-82545]
- With Citrix Virtual Apps and Desktops 2411, the Connection Strength Indicator (CSI) on the Desktop Viewer toolbar does not display the correct protocol information. Instead, the protocol is shown as N/A in the CSI details. [XASUP-6810]
- The **Back** button action might not work when used in a window that is redirected with Browser Content Redirection. [HDX-88099]
- When Google Chrome is configured as a published application, Browser Content Redirection (BCR) may fail for the first navigation attempt after the application is launched.[HDX-88636]
- When using Google Chrome on a page that is actively being redirected by Browser Content Redirection (BCR), the address bar's autocomplete suggestion list is rendered incorrectly. As you

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

type into the address bar, the drop-down list of suggestions (such as search history or bookmarks) appears behind the BCR content overlay, making it invisible and unusable.[HDX-85041]

- When Browser Content Redirection (BCR) is used for Google Meet in conjunction with the Browser Profile Sharing feature, users might be unexpectedly disconnected from the meeting after a period of time. [HDX-88267]
- When accessing a signed-in website using Browser Content Redirection with profile sharing, disconnecting and then reconnecting a Citrix session can sometimes prompt the user to sign in again after the page is reloaded. This issue can also occasionally occur upon a page refresh within the same session. [HDX-85493]
- The thumbnail preview will not display in the foreground when you hover over an app's thumbnail preview (for example, from the task bar) if Browser Content Redirection page, MTOP, UC SDK or RAVE window is overlapping it.[HDX-91095]
- The BCR page may flicker if you click outside the browser window (for example, on the taskbar or Start menu) and then click back into it. [HDX-90521]

Citrix Director

- You might be unable to reset a user profile in Citrix Director. You can manually rename the user profile folder in the profile store path. [CVADHELP-28082]

Citrix Policy

- After hibernation, you might notice that the VDA doesn't apply domain-configured GPOs, leading to policy misalignment upon reinitialization. [CVADHELP-27660]

Delivery Controller

- CitrixUpgradeAgent service is not able to start in non English OS locale. [CVADHELP-28819]

Graphics

- After installing July 2025 Windows updates on session hosts, you might experience issues with mouse cursor placement in your sessions. [CVADHELP-28943]

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

Secure Private Access with Web Studio

- Under the **Settings > Integrations** tab, the error messages appear behind the dialog box instead of in front of it. No workaround for this issue and it does not affect any features or user experiences. [SPAOP-4856]

  > **Note:**
  >
  > The issue occurs only when you access the Secure Private Access from Web Studio. It is not applicable if you access the standalone Secure Private Access.

Universal Print Server

Printing

After upgrading from Universal Print Server (UPS) to 2203 LTSR CU5, you might experience long delays when selecting a printer. The printer might stay in the "Connecting to printer"state and take over a minute to become available. [CVADHELP-27306]

VDA for single-session OS

System Exceptions

- A blue screen error with code PAGE_FAULT_IN_NONPAGED_AREA (0x50) might occur intermittently due to an issue in the picadm.sys module. [CVADHELP-27854]

VDA for multi-session OS

Session/Connection

- A multi-session VDA might become unregistered and completely unresponsive. You cannot reconnect to the affected virtual machine until you manually restart it. [CVADHELP-27863]
- A blue screen error with code PAGE_FAULT_IN_NONPAGED_AREA (0x50) might occur intermittently due to an issue in the picadm.sys module. [CVADHELP-27540]

Smart Cards

- The Certificate Propagation Service might crash intermittently, causing smart card authentication to fail. [CVADHELP-27733]

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

System Exceptions

- You are unable to expand seamless application Windows horizontally on a laptop screen when a secondary monitor is unplugged. [CVADHELP-27710]
- When using Citrix Workspace app for HTML5, the Citrix Shell (wfshell.exe) process might crash when copying large amounts of data. [CVADHELP-27496]

Profile Management

For information about the fixed issues, see the Fixed issues article in its own document.

Linux VDA

For information about the fixed issues, see the Fixed issues article in its own document.

Session Recording

For information about the fixed issues, see the Fixed issues article in its own document.

Citrix Provisioning™

For information about the fixed issues, see the Fixed issues article in its own document.

Citrix Virtual Delivery Agent for macOS

For information about the fixed issues, see the Fixed issues article in its own document.

Workspace Environment Management

For information about the fixed issues, see the Fixed issues article in its own document.

Federated Authentication Service

For information about the fixed issues, see the Fixed issues article in its own document.

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

Known issues

August 21, 2026

Citrix Virtual Apps and Desktops™ 7 2507 LTSR includes the following known issues:

Notes

- If a known issue has a workaround, it is provided after the description of the issue.
- The following warning applies to any workaround that suggests changing a registry entry:

> **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 the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Known issues in 2507 CU2

> **Important —Data retention limitation for uberAgent lite**
>
> The uberAgent lite feature, introduced in 2507 CU2, stores new performance metrics —resource-utilization, session metrics, and Session Score history —in the Monitor database. The data collected for these metrics is not preserved during upgrades for following scenarios -
>
> - When you upgrade from 2507 CU2 to a future version of 2507 CU within CVAD 2507
> - When you upgrade from 2507 CU (CU2 and above) to CR 2603 or later releases.
> - When you upgrade from 2507 CU (CU2 and above) to CR 2511. Since CR 2511 does not have this feature, the feature itself will be removed during the site monitor database upgrade.
>
> Once you are on CR 2603 or higher release, the feature is part of the base release itself and therefore, later upgrades would preserve the data. Note that the feature itself is not impacted during such upgrades (except for the upgrade to 2511 as mentioned above). Data collection resumes automatically after the upgrade; only the history collected before the upgrade is affected.
>
> If you want to retain this data across the upgrade, follow the steps documented in [CTX696889] before starting the upgrade

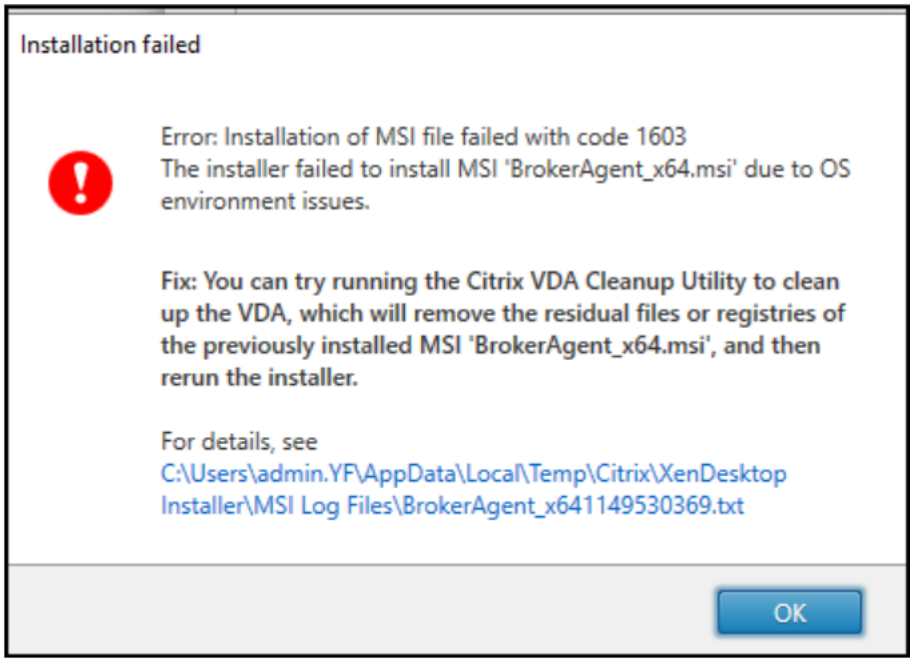
- When you refresh licenses in the MMC-based Studio, with the DDC configured for Licensing Activation Service (LAS), V6 license file details are briefly displayed incorrectly. This temporarily affects the accurate presentation of license information within the MMC Studio. To mitigate, close and re-open MMC Studio. [STUD-37809]

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

Known issues in 2507 initial release

General

- You might encounter the following error during Citrix VDA installation on Windows 10 (22H2) and Windows Server 2022 platforms.



  Also, in the broker agent msi logs, you might see the following error message:

```
MSI (s) (04:D8) [09:46:08:426]: Note: 1: 1722 2: CA_RunInstallAgent 3: C:\Program Files\Citrix\Virtual Desktop Agent\BrokerAgent.exe 4: -install
CustomAction CA_RunInstallAgent returned actual error code 1701 ( note this may not be 100% accurate if translation happened inside sandbox)
MSI (s) (04:D8) [09:46:08:427]: Product: Citrix Virtual Desktop Agent - x64 -- Error 1722. There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor. Action CA_RunInstallAgent, location: C:\Program Files\Citrix\Virtual Desktop Agent\BrokerAgent.exe, command: -install
```

  To resolve this issue, close the installer, rebuild Windows Performance Counters, restart the machine, and do the installation again. See the Microsoft document Manually rebuild performance counters for Windows Server 2008 64 bit or Windows Server 2008 R2 systems for information.

  [LCM-23228]

- If you launch the app bar and then open the Connection Center menu in Citrix Workspace™ app

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

for Windows, the app bar doesn't appear under the server that hosts it. [HDX-27504]

- The **Session limits** settings for multi-session VDAs are declined in session hosts running Windows Server 2022, Windows 10 Enterprise multi-session, and Windows 11 Enterprise multi-session.[HDX-47001]
- Microsoft confirms there is an issue retaining print settings between print jobs when using the Modern Print Dialog, which they are working to address. Their current projection is the first half of 2025. The Modern Print Dialog is enabled by default in newer OS versions such as Windows 11 and Windows Server 2025. The OS can be configured to use the legacy print dialog by taking the following action:

  1. Open the Registry Editor.
  2. Go to `HKEY_CURRENT_USER\Software\Microsoft\Print\UnifiedPrintDialog`
  3. Right-click and select **New > DWORD (32-bit) Value**
  4. Rename the value as **PreferLegacyPrintDialog**.
  5. Right-click **PreferLegacyPrintDialog** and select **Modify**.
  6. Set the value data to 1 and click **OK**.

  [HDX-66953] [HDX-66904]

- **[3rd Party] Printing might fail after an in place Windows upgrade on machines with the Citrix VDA already installed**
  After an in place Windows upgrade, Citrix print providers might no longer be invoked, which can result in printing failures. This issue occurs because the Windows upgrade process resets the print provider execution order and does not preserve Citrix registered providers. Microsoft has confirmed this is a Windows behavior and does not currently preserve provider registrations in the execution order during upgrades. [HDX-85359]

The workaround is to add the print providers back into the appropriate registry location.

```
1. Open the Registry Editor.
1. Go to `HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Print\Providers`
1. Right-click **order** and select **Modify**.
1. Add the values `Universal Printer` and `Client Printer` above any other providers.
1. Reboot the VDA.
```

- If the uberAgent® service is installed independently from the VDA (not through the VDA MetaInstaller), the uberAgent service must not be uninstalled when the VDA is uninstalled. [HDX-92242]
- When publishing an application packaged with App-V, users may be unable to move or resize the application. As a workaround, set the following registry value: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\SeamlessSwclFlags(`

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

`DWORD`) = 2. This key must only be used to work around this specific issue and might cause reduced user experience with resizing and moving windows. [HDX-91796]

- During a Citrix Virtual Apps and Desktops session, if a client monitor supporting audio playback is power cycled (turned off and then on), the name of the monitor's audio playback device within the VDA's Sound Control Panel (mmsys.cpl) changes from its correct, specific name to "Citrix HDX Audio". This is an intermittent issue. As a workaround, close the VDA's Sound Control Panel (mmsys.cpl) window and then re-launch it. [HDX-87080]
- When a new profile is created in NAPS2 version 8.x and a feeder-based scan is immediately initiated, the application might crash. The issue is specifically observed with NAPS2 version 8.1.4. [HDX-86985]
- When attempting to add a new printer from within certain applications published on a Windows Server 2019 Virtual Delivery Agent (VDA), an error occurs preventing the printer from being listed or added. Specifically, an error message indicating that `rundll32.exe` cannot be accessed appears.

  As a workaround, use a printer that is already visible in the application or add the printer so that it is available in the current session.

  [HDX-86440]
- If the device name is changed on the client machine while a session is active, the new name is not immediately reflected inside the session settings. This behavior affects both playback and recording devices.

  As a workaround, to view the updated device name, you must disconnect from the session and then reconnect. Alternatively, logging out of the session and logging back in also resolves the issue.

  [HDX-86327]
- When multiple Chrome browser tabs, including those configured for Browser Content Redirection (BCR), are dragged and dropped simultaneously from one Chrome window to another, the redirected content might exhibit unexpected behavior. [HDX-81501]
- If you move a tab with video content to a new window, playback might stop or the video might not appear. [HDX-92343]
- When using Browser Content redirection with Browser Profile Sharing, SSO persistence with multiple profiles is not supported. [HDX-85325]
- Windows 11 has a new UI feature to snap the windows on the desktop. A special toolbar appears on top of the desktop while the user drags the window. So multimedia overlay clipping logic is cutting the top/center area out, probably because of the new invisible/transparent window for this functionality.

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

As a workaround,

- For more info, see Snap your windows section.
- Refer How to disable "Snap your windows"feature. [HDX-91532]

- When you use the Citrix Workspace app to access the VDA with Unicode input mode enabled, and either the "Unicode keyboard layout mapping"or "Automatic keyboard display"group policy is turned on, you might notice reduced performance in Microsoft Excel when scrolling through large pages. This issue occurs because UIAutomation APIs are incompatible with Excel.[HDX-91618]
- When using Enhanced domain pass-through for single sign-on (SSO), SSO into applications inside the session works as expected when a user first connects. However, if the user disconnects and later reconnects to the same session, SSO within the session may stop working. This is due to a regression introduced with Windows updates released in March and April 2025. Customers experiencing this issue are advised to open a support case with Microsoft and reference tracking ID 2410230030007977. [HDX-66643]
- When you launch an application on a device that does not support session sharing, a `TokenNotFoundException` might occur. This prevents the application from launching. [CVADHELP-31578]
- When you update the Virtual Delivery Agent (VDA), the installation process might not resume as expected. This issue occurs due to a failure in checking the `CitrixVirtualDesktopAgent.xml` file and affects VDA updates on Cumulative Updates such as CU2 and CU4. [CVADHELP-31718]
- When you perform a WIA scan in `mspaint.exe` on a VDA running 2507 CU2 (build B755 or later) with WIA redirection enabled, `mspaint.exe` crashes. This prevents successful image scanning operations.
  - **Workaround:** Replace the `WIARedirection.dll` file in `C:\Program Files\Citrix\HDX\bin` with the version from the 2507 CU1 VDA. [LCM-25586]
- When launching Citrix RDP sessions through StoreFront™ with VDA 2507 CU2 B1 or later, authentication fails. An "Incorrect username or password"error appears, preventing user access to remote RDP sessions.
  - **Workaround:** Set `HKLM\Software\Citrix\UsePasswordFromClientData` to `DWORD` 1 on the VDA. [LCM-25730]
- When you upgrade a Delivery Controller™ (DDC) to version 2507, Web Studio incorrectly reports "Your software maintenance has expired."VDA sessions display "Your corporate Citrix environment is currently unsupported,"even with valid licenses. [CVADHELP-29639]

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

- When you assign newer app packages containing updated namespaces (such as uap3) to a delivery group in Web Studio, app discovery fails. This prevents the applications from appearing in Web Studio for assignment to delivery groups. [CVADHELP-30250]
- When you launch an App-V application for the first time, a timing conflict during package synchronization prevents the application from launching successfully.
  - **Workaround:** Try re-launching the application. [CVADHELP-31381]
- Due to new App-V related features added in CVAD 2311, App-V functionality is now fully supported only in Web Studio. Using MMC Studio for App-V may lead to issues.

  1. Existing App-V Applications might stop working

     After upgrading the Delivery Controller (DDC) to: 2402 LTSR CU3 or earlier 2402 LTSR versions, or 2507 RTM,
     App-V applications previously created using MMC Studio may no longer function as expected. As a workaround:
     For 2507 RTM, run sql in siteDB :

```
-- Convert Broker Apps which are Packaged Apps to be explicitly labeled as such.
-- this is detected by the presence of ctxAppVLauncher.exe on the command line
-- The application record in the Applibrary and the related Package and Library denote which packaging technology was used.

 update chb_Config.Applications
 set ApplicationType = 4, --$ATPackagedApplication
     --NB: The AppLibrary's LibaryUid and the Broker's PackagedApplicationType have the same value
     PackagedApplicationType = case
                                 when TRY_CONVERT(uniqueidentifier, A.CommandLineArguments) is null then 2 --Dual Admin
                                 else 1 -- Single Admin.
                                         -- This is a bug with legacy MMC Studio not understanding the new Broker App format. But only App-V apps can be affected
                               end,
     PackagedApplicationId = case
```

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

```
                                        when TRY_CONVERT(
                                            uniqueidentifier, A.
                                            CommandLineArguments)
                                            is null then REPLACE(A.
                                            CommandLineArguments, N
                                            '"','')
                                        else CONVERT(char(36),
                                            CONVERT(
                                            uniqueIdentifier,  A.
                                            CommandLineArguments))
                                    end,
        PackagedApplicationVisibility = 3 --
            WorkspaceAndDesktop
    from chb_Config.Applications A
        inner join chb_Config.ApplicationsMetadata AMD on A.
            Uid = AMD.ApplicationUid
    where A.CommandLineExecutable like N'%ctxAppVLauncher.exe'
        and A.ApplicationType = 0 --$ATHostedOnDesktop
        and AMD.Name = 'Citrix_DesktopStudio_SequenceLocation'
        and right(AMD.Value, 5) = '.appv'
```

2. Creating New App-V Applications in MMC Studio

In 2402 LTSR and 2507 LTSR, creating new App-V applications via MMC Studio may not function correctly.It is recommended to use Web Studio to create new App-V applications. [LCM-23481]

- When you upgrade a Single session VDA from any older version to 2507 LTSR CU1, the upgrade operation fails.

  As a workaround, see the **Important** note in Time zone control policy settings.

  This issue is resolved in Citrix Virtual Apps and Desktops 2507 CU1 Update 4 [CVADHELP-31839]

Audio

- When an audio device, such as a headset, is generically redirected using USB redirection to a Windows Server Virtual Delivery Agent (VDA) (for example, Windows Server 2019 or 2022), and multiple user sessions are simultaneously active on the same VDA, clicking the volume icon in the lower-right corner of the taskbar to adjust the settings can cause an unexpected crash of the Windows `ShellExperienceHost.exe` process. This issue primarily occurs in a session where the audio device is not actively redirected, but another session on the same VDA is utilizing generic USB audio redirection.

  As a workaround, restart the Windows Explorer process (explorer.exe) in the affected session through the Task Manager. This might allow the volume icon to function without crashing.

  [HDX-80937]

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

Machine Creation Services™

- 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. [PMCS-58254]
- The VMs created using `InstanceType` are not supported as a master image in Red Hat OpenShift environments. [PMCS-54272]
- 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. [PMCS-54009]
- In a Red Hat OpenShift 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 and later versions 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. [PMCS-53794]
- 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. [PMCS-38514]

Profile Management

- For information about the known issues, see the Known issues article in its own document.

Linux VDA

- For information about the known issues, see the Known issues article in its own document.

Session Recording

- For information about the known issues, see the Known issues article in its own document.

Workspace Environment Management™

- For information about the known issues, see the Known issues article in its own document.

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

Citrix Provisioning™

- For information about the known issues, see the Known issues article in its own document.

Federated Authentication Service

- For information about the known issues, see the Known issues article in its own document.

Deprecations and removals

August 20, 2026

The announcements in this article are intended to give you advanced notice of platforms, Citrix products, and features that are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they 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. For information about the Long Term Service Release (LTSR) servicing option, see https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549.

The following table shows the platforms, Citrix® products, and features that are deprecated or removed. Dates in **bold** face indicate changes at this release.

Deprecations

Deprecation means we intend to remove the feature or capability from a future release. The feature or capability will continue to work and is fully supported until it is officially removed. This deprecation notification can span a few months or years. After removal, the feature or capability will no longer work. This notice is to allow you sufficient time to plan and update your code before the feature or capability is removed. Alternatives for deprecated items are suggested where possible.

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

Item	Deprecation announced in version	Alternative
File based licensing	2507	License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. Customers using file based licensing are required to upgrade to a compatible release and perform this technology transition before April 15, 2026. LAS will be the only way to activate and license Citrix on-premises components after April 15, 2026.
Support for `Get-BrokerMachine`	2507	Use `Get-BrokerMachineV2`
Support for **Enable heavyweight compression** option under the Image compression section of **Universal printing optimization defaults** policy setting	2507	
Support for `Repair-AcctADAccount` PowerShell command	2503	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 example, `repair-userCertificate` attributes for Hybrid Azure AD 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, from tainted to available). This can
Optimize for 3D HDX Graphics policy	2411	Use Use a video codec for compression set to For the Entire Screen. See https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/2507-ltsr/policies/reference/ica-policy-settings/graphics-policy-settings.html#use-video-codec-for-compression

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

Item	Deprecation announced in version	Alternative
NVIDIA GPU hardware encoding (NVENC) with: vGPU 15 and older, and driver version 529.19 and older.	2411	Use currently supported NVIDIA drivers: vGPU 16 or newer, and driver version 536.22 or newer. See https://docs.nvidia.com/vgpu/index.html#driver-versions on NVIDIA supported vGPU and driver versions for more information.
Support for the following `-AcctADAccount` PowerShell commands New-AcctADAccount Add-AcctADAccount Update-AcctADAccount Remove-AcctADAccount Unlock-AcctADAccount Get-AcctADAccount	2411	Use the -AcctIdentity PowerShell commands New-AcctIdentity Add-AcctIdentity Update-AcctIdentity Remove-AcctIdentity Unlock-AcctIdentity Get-AcctIdentity
Support for `-ResetIdentityInfo` PowerShell command	2411	Use `-Recreate` to recreate the identity disk. For information, see Repair the identity information of active computer accounts.
MMC-based Studio	2411	Use Web Studio.
Multiple monitor hooks	2407	-
Domain pass-through authentication	2407	Use enhanced domain pass-through for single sign-on.
Rendezvous V1	2402	Use Rendezvous V2.
Secure ICA®	2402	Use Secure HDX.
VDA support on Windows Server 2016	2402	Upgrade to the latest Windows Server versions.

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

Item	Deprecation announced in version	Alternative
Support for Delivery Controller™, Web Studio, Citrix Director, Citrix License Server, Citrix StoreFront, Server VDI for single-session OS, VDA for multi-session OS, Active Directory forest and domain, and Universal Print Server on Windows Server 2016	2402	Upgrade to the latest version of Windows Server.
Support for Microsoft SQL Server versions 2016 and 2017 for the site configuration, configuration logging, and monitoring databases	2402	Upgrade to the latest version of Microsoft SQL Server.
Support for Azure catalogs created before on-demand provisioning feature (“legacy” catalogs)	2402	Recreate Azure legacy catalog VMs. The catalogs are provisioned as on-demand and thereby, save storage cost.
The **Target Minimum Frame Rate** policy	2311	Use **Graphics Status Indicator** to modify the target minimum frame rate.
Support for using a master image in a region different from the region where the catalog is created	2311	Use Azure Compute Gallery to replicate the master image to the desired region.
HDX™ Graphics Display Memory Limit setting	2311	The minimum amount of memory required is allocated to ensure the client’s display layout is fully accommodated.
Progressive mode support in HDX Graphics	2311	Use Thinwire. See Progressive mode.
Support for browser content redirection in Internet Explorer 11	2311	Use Google Chrome-based browser content redirection.
Support for SQL Server 2016 in Broker	2308	Use the latest versions. For more information, see System Requirements.

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

Item	Deprecation announced in version	Alternative
Support for XenApp 5.x in Director	2308	—
Support for XenApp 6.x in Director	2308	—
SCOM Pack for alerts in Director	2308	—
Support for plug-in in Director	2308	—
Support for WebRTC SDP format (Plan B)	2308	Upgrade the Citrix Workspace™ App to a supported version.
Support for Single Window mode in Microsoft Teams Optimization	2308	Upgrade the Citrix Workspace App to a version that supports MultiWindow mode. For more information, see Feature matrix and version support.
Support for `AwsCaptureInstanceProperties` used in AWS environments	2308	Use a machine profile. See Create a catalog using a machine profile.
`Schedule-ProvVMUpdate` PowerShell command	2305	Use `Set-ProvVMUpdateTimeWindow`.
`Request-ProvVMUpdate` PowerShell command	2305	Use `Set-ProvVMUpdateTimeWindow` with `-StartsNow` and `-DurationInMinutes -1` parameters.
`Cancel-ProvVMUpdate` PowerShell command	2305	Use `Clear-ProvVMUpdateTimeWindow`.
`DedicatedTenancy` parameter used in `New-ProvScheme` command	2303	Use `TenancyType` parameter.
License Server VPX	2206	—
Unmanaged disk to provision VMs in Azure environments.	2206	Use managed disks.
Host to Client (URL) redirection	2203	Bidirectional content redirection.

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

Item	Deprecation announced in version	Alternative
Support for four AWS specific commands: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress`, and `Grant-HypSecurityGroupIngress` used in Cloud and on-premises environment.	2203	—
Citrix Files for Windows and Citrix Files for Outlook from the VDA metainstaller.	2203	Use the standalone installers.
WEM Agent component from the VDA metainstaller.	2203	—
SCCM-integrated Wake on LAN option for Remote PC Access.	2012	Use the standalone Wake on LAN feature.
Citrix SCOM Management Packs for XenApp and XenDesktop, Provisioning Services, and StoreFront. For the product versions that can be monitored, see Citrix SCOM Management Packs documentation.	1912	Use Director for monitoring and managing your deployment. For more information on SCOM EOL and alternatives, see https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX266943.
Mobility SDK / Mobile SDK (from the former Citrix Labs)	7.16	Superseded by mobile experience policy settings, and native experiences for hosted desktops/apps.

Removals

Removed items are either removed, or are no longer supported, in Citrix Virtual Apps and Desktops.

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

Item	Deprecation announced in version	Removed in version	Alternative
Support for Citrix Connector 3.1 for System Center Configuration Manager	2311	2507	Do image or application update manually.
Removed the support for AWS volume worker	2311	2503	Use Direct disk upload and download. See Direct disk upload and download.
Support for SQL Server 2016 and 2017	2402 and 2308	2411	Use SQL Server 2019 and 2022
Support for configuring the MCS I/O write-back cache to include only a disk cache and no memory cache	2402	2411	When creating machines with write-back cache enabled, select the **Memory cache size (MB)** option and give it a non-zero size.
Support for PVS Import wizard in Citrix Studio	1912 LTSR	2311	Provision Citrix Provisioning™ machines using either of the following ways
Citrix Workspace app for Windows 1912	—	2402	Use the latest versions.
HDX Graphics FullScreen + Text optimization	2311	2311	Provision machines using Citrix Provisioning Console and export them to Citrix Virtual Apps and Desktops using Citrix Provisioning Devices Export Wizard. See Export Devices Wizard for more details.
Support for NVIDIA Frame Buffer Capture (NVFBC) with HDX 3D Pro	2308	2311	Use Desktop Duplication API (DDAPI).
VDA support for policy setting “Automatic installation of in-box printer drivers”.	7.16	2311	Use Policy setting Create Citrix Provisioning catalogs (Windows 7, Windows Server 2012 R2 and earlier).

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

Item	Deprecation announced in version	Removed in version	Alternative
NVIDIA GPU hardware encoding (NVENC) with: vGPU 11 and older, and driver version 466.77 and older.	2305	2305	Use currently supported NVIDIA drivers: vGPU 13 or newer, version 471.41 or newer.
Citrix Supportability Tools (Supportability-Tool_x64 .msi) from the VDA Meta-Installer.	—	2212	—
Citrix License Administration Console (last included in the Windows License Server 11.16.3 build 30000 and removed in the Windows License Server v11.16.6 build 31000).	2003	2006	Use the Citrix Licensing Manager.
Citrix Indirect Display Driver (IDD) graphics adapter support on Windows 10 version 1709 and earlier.	2003	2003	Use Citrix Virtual Apps and Desktops 7 1912 LTSR VDAs.
Hardware encoding with NVIDIA GPUs (NVENC) using GRID 9 or earlier display drivers.	2003	2003	Use GRID 10 display drivers with Citrix Virtual Apps and Desktops 7 2003 or later VDAs, or use Citrix Virtual Apps and Desktops 7 1912 LTSR VDAs.
Self-Service Password Reset (SSPR) feature.	2003	2006	—

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

Item	Deprecation announced in version	Removed in version	Alternative
Support for Microsoft .NET Framework versions prior to version 4.8 for VDAs and core server components. Includes Delivery Controller, Studio, Director.	1912	2003	Upgrade to .NET Framework version 4.8.
VDAs on Windows Server 2012 R2.	1912	2003	Install VDAs on a supported operating system.
AppDNA® application migration component of Citrix Virtual Apps and Desktops Premium edition.	1909	2003	—
Installing Studio on 32-bit (x86) machines.	1909	2003	Install on a supported x64 operating system.
Support for the Excel hook in seamless applications. This was used for creating separate taskbar icons for each Microsoft Excel 2010 workbook.	1909	1909	—
Core server components on Windows Server 2012 R2 (including Service Packs). Includes: Delivery Controller, Studio, and Director.	1906	2003	Install on a newer supported operating system.

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

Item	Deprecation announced in version	Removed in version	Alternative
Support for Site Configuration, Configuration Logging, and Monitoring databases on Microsoft SQL Server versions 2008 R2, 2012, and 2014 (including all Service Packs and editions).	1906	2003	Install databases on a supported Microsoft SQL Server version.
Support for VDAs on Windows 10 on x86 platforms.	1906	1909*	Install VDAs on a supported x64 operating system. *This feature is still supported in Citrix Virtual Apps and Desktops 7 1912 LTSR.
Removal of Citrix Smart Tools Agent from Citrix Virtual Apps and Desktops installation media.	1903	1906	—
Support for Linux VDA on Red Hat Enterprise Linux/CentOS 7.5.	1903	1903	Install Linux VDA on a later version of Red Hat Enterprise Linux.
StoreFront support for TLS 1.0, and TLS 1.1 protocols between Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) and Citrix Receiver, and Workspace Hub.	7.17	2203	Upgrade Citrix Receivers to a Citrix Workspace app that supports the TLS 1.2 protocol. For more information on Citrix Workspace app, see https://docs.citrix.com/en-us/citrix-workspace-app.

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

Item	Deprecation announced in version	Removed in version	Alternative
VDA support for policy setting "Automatic installation of in-box printer drivers".	7.16	2311	None. Policy setting supported with VDAs on earlier OSs only (Windows 7, Windows Server 2012 R2 and earlier).
Support for Framehawk display remoting technology	1811	1903	Use Thinwire with adaptive transport enabled.
Support for Citrix Smart Scale in all Citrix Virtual Apps and Desktops (and XenApp and XenDesktop) versions. This functionality will reach End of Life on 31 May 2019.	1808	1906	Consider using the Virtual Apps and Desktops Service on Citrix Cloud for improved power management functionality.
Support for Microsoft .NET Framework versions 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, and 4.7 by Citrix StoreFront, Citrix VDAs, Citrix Studio, Citrix Director, and Citrix Delivery Controller.	7.18	1808	Upgrade to .NET Framework version 4.7.1 or later. (The installer automatically installs .NET Framework 4.7.1 if it is not already installed.)
Support for Linux VDA on Red Hat Enterprise Linux 7.3.	7.18	1808	Install Linux VDA on a later version of Red Hat Enterprise Linux.
Support for the Linux VDA on SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Install Linux VDA on supported SUSE version.
Support for Citrix WDDM driver on VDAs	7.16	7.16	The Citrix WDDM driver is no longer installed with VDAs.

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

Item	Deprecation announced in version	Removed in version	Alternative
VDAs on Windows 10 version 1511 (Threshold 2) and earlier Windows Single-session OS releases, including Windows 8.x and Windows 7 (see https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/).	7.15 LTSR (and 7.12)	7.16	Install Single-session OS VDAs on Windows 10 minimum version 1607 (Redstone 1) or newer Semi-Annual Channels. If using 1607 LTSB, we recommend a 7.15 VDA. See CTX224843.
VDAs on Windows Server 2008 R2 and Windows Server 2012 (including Service Packs)	7.15 LTSR (and 7.12)	7.16	Install VDAs on a supported operating system.
Desktop Composition Redirection (previously known as DirectX Command Remoting) (DCR)	7.15 LTSR	7.16	Use Thinwire.
Core components on Windows Server 2012 and Windows Server 2008 R2 (including Service Packs). Includes: Delivery Controller, Studio, Director, StoreFront, License Server, and Universal Print Server.	7.15 LTSR	7.18	Install components on a supported operating system.

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

Item	Deprecation announced in version	Removed in version	Alternative
Self-Service Password Reset (SSPR) feature on Windows Server 2012 and Windows Server 2008 R2 (including Service Packs)	7.15 LTSR	7.18	Install on a newer supported operating system.
Studio on Windows 7, Windows 8, and Windows 8.1 (including Service Packs)	7.15 LTSR	7.18	Install Studio on a supported operating system.
Flash Redirection	7.15 LTSR	1912	Create video content as HTML5 Video. Use HTML5 Video Redirection for managed content, and Browser Content Redirection for public websites. For more information, see the Flash Redirection End of Life note.
Citrix Online Integration (Goto product) with StoreFront	7.14 (and StoreFront 3.11)	StoreFront 3.12	—

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

Item	Deprecation announced in version	Removed in version	Alternative
The user account, CtxAppVCOMAdmin, which was created during VDA installation and added to the Local Administrators Group on the VDA machine, is no longer created. The underlying "COM" mechanism is also removed.	7.14	7.14	The Windows service CtxAppVService performs the same function. It is automatically installed and configured and requires no user interaction.
Universal Print Server UpsServer component support on Windows Server 2008 32-bit	7.14	7.14	Install on a newer supported operating system.
StoreFront and Receiver for Web on Internet Explorer 8	7.13	7.13	—
VDA command line installation option /no_appv to prevent installation of the Citrix App-V components	7.13	7.13	Use the command line installation option /exclude "Citrix Personalization for App-V –VDA".
The full-product installer no longer installs the Citrix.Common.Commands snap-in on new installations and automatically removes it when upgrading existing installations.	7.13	7.13	Some PowerShell commands that were provided by the Citrix.Common.Commands snap-in are still available in the XenApp 6.5 SDK.
Partial functionality to manipulate icon data that was provided by *-CtxIcon cmdlets.	7.13	7.13	Now provided by *-BrokerIcon cmdlets in the Broker Service.

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

Item	Deprecation announced in version	Removed in version	Alternative
Legacy Thinwire mode	7.12	7.16	Use Thinwire. If you are using Legacy Thinwire mode on Windows Server 2008 R2, migrate to Windows Server 2012 R2 or Windows Server 2016, and use Thinwire.
In-place upgrades from StoreFront 2.0, 2.1, 2.5, and 2.5.2	7.13	7.16	Upgrade from one of these versions to a later supported version and then to XenApp and XenDesktop 7.16.
In-place upgrades from XenDesktop 5.6 or 5.6 FP1	7.12	7.16	Migrate your XenDesktop 5.6 or 5.6 FP1 deployment to the current XenDesktop version. To do this, first upgrade to XenDesktop 7.6 LTSR (with the latest CU), then upgrade to the latest Citrix Virtual Desktops (formerly XenDesktop) release or LTSR version.
Installing Delivery Controller, Director, StoreFront, or License Server on 32-bit (x86) machines.	7.12	7.16	Install on a supported x64 operating system.
Connection leasing	7.12	7.16	Use Local Host Cache.

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

Item	Deprecation announced in version	Removed in version	Alternative
XenDesktop 5.6 used on Windows XP. VDA installations on Windows XP are not supported.	7.12	7.16	Install VDAs on a supported operating system.
Support for CloudPlatform connections	7.12	2003	Use a different supported hypervisor or cloud service.
Support for Azure Classic (also known as Azure Service Management) connections	7.12	2003	Consider using the Virtual Apps and Desktops Service on Citrix Cloud.
AppDisks functionality (and the AppDNA integration into Studio, which supports it)	7.13	2003	Use Citrix App Layering.
Personal vDisk functionality	7.15	2006†	Use Citrix App Layering user layer or user personalization layer technology.

† At Citrix Virtual Apps and Desktops 7 2003, the Personal vDisk driver was removed from the VDA installer. At Citrix Virtual Apps and Desktops 7 2006, the Personal vDisk driver workflow was removed from Studio.

System requirements

January 6, 2026

Introduction

The system requirements in this document were valid when this product version was released. Updates are made periodically. System requirements for components not covered here (such as host

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

systems, Citrix Workspace™ app, and Citrix Provisioning™) are described in their respective documentation.

Review Prepare to install before beginning an installation.

Except where noted, the component installer deploys software prerequisites automatically (such as .NET and C++ packages) if the required versions are not detected on the machine. The Citrix® installation media also contains some of this prerequisite software.

The installation media contains several third-party components. Before using the Citrix software, check for security updates from the third party, and install them.

For globalization information, see Knowledge Center article CTX119253.

For components and features that can be installed on Windows Servers, Nano Server installations are not supported, unless noted. Server Core is supported only for Delivery Controllers and Director.

Hardware requirements

RAM and disk space values are in addition to requirements for the product image, operating system, and other software on the machine. Your performance varies, depending on your configuration. Your configuration includes the features that you use, plus the number of users, and other factors. Using only the minimum can result in slow performance.

The following table lists the minimum requirements for core components.

Component	Minimum
All core components and StoreFront™ on one server, for an evaluation only, not a production deployment	5 GB RAM
All core components and StoreFront on one server, for a test deployment or a small production environment	12 GB RAM
Delivery Controller™ (more disk space required for Local Host Cache)	5 GB RAM, 800 MB hard disk
Studio	1 GB RAM, 100 MB hard disk
Director	2 GB RAM, 200 MB hard disk
StoreFront	2 GB RAM, see the StoreFront documentation for disk recommendations
License Server	8 GB RAM; see the Licensing documentation for disk recommendatio

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

Sizing of VMs that deliver desktops and applications

Specific recommendations cannot be provided because of the complex and dynamic nature of hardware offerings, and every deployment has unique needs. Generally, sizing a Citrix Virtual Apps™ VM is based on the hardware and not the user workloads. The exception is RAM. You need more RAM for applications that consume more.

For more information:

- Citrix Tech Zone contains guidance on sizing.
- Citrix Virtual Apps and Desktops Single Server Scalability discusses how many users or VMs can be supported on a single physical host.

Microsoft Visual C++

When installing a Delivery Controller, Virtual Delivery Agent (VDA), or Universal Print Server, the Citrix installer automatically installs the Microsoft Visual C++ 2015–2022 Redistributable.

- If the machine contains an earlier version of that runtime (such as 2015-2019), the Citrix installer upgrades it.
- If the machine contains a version earlier than 2015, Citrix installs the newer version in parallel.

Delivery Controller

> **Note:**
>
> **License Server version compatibility:** Ensure that the License Server is running a minimum of version 11.17.2 build 53100. Failure to meet this prerequisite will block the Citrix Virtual Apps and Desktops (CVAD) site upgrades and site creation

Supported operating systems:

- Windows Server 2025
- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, Standard and Datacenter Editions, and with the Server Core option

Requirements:

- Microsoft .NET Framework 4.8 is installed automatically if it (or a later version) is not already installed.
- Windows PowerShell 3.0, 4.0, or 5.0.
- Microsoft Visual C++ 2015–2022 Redistributable.

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

- If you upgrade from Citrix Virtual Apps and Desktops version 2407 to 2411 or later, or perform a fresh installation of version 2411 or later, update the License Server to the latest version (version 11.2.17 build 53100 or later) as the first step. Then, upgrade the Delivery Controller. Failing to do so results in a warning message on the UI and failure of command-line installations.

> **Note:**
>
> Citrix Virtual Apps and Desktops™ Delivery Controllers do not support the read-only domain controller (RODC).

Databases

> **Note:**
>
> Starting with version 2411, you can use Azure SQL Managed Instance for databases.

Supported Microsoft SQL Server versions for the site configuration, configuration logging, and monitoring databases:

- SQL Server 2022, Express, Standard, and Enterprise Editions.
  - For new installations: By default, SQL Server Express 2022 with Cumulative Update 14 is installed when installing the Controller, if an existing supported SQL Server installation is not detected.
- SQL Server 2019, Express, Standard, and Enterprise Editions.

The following database high availability solutions are supported (except for SQL Server Express, which supports only standalone mode):

- SQL Server AlwaysOn Failover Cluster Instances
- SQL Server AlwaysOn Availability Groups (including Basic Availability Groups)
- SQL Server Database Mirroring

Windows authentication is required for connections between the Controller and the SQL Server site database.

Local Host Cache considerations: Microsoft SQL Server Express LocalDB is a feature of SQL Server Express that Local Host Cache uses on a standalone basis. Local Host Cache does not require any components of SQL Server Express other than SQL Server Express LocalDB.

- When installing a Controller, Microsoft SQL Server Express LocalDB 2022 with Cumulative Update 15 is installed for use with the Local Host Cache feature. (This installation is separate from the default SQL Server Express installation for the site database.)

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

- When upgrading a Controller, the existing Microsoft SQL Server Express LocalDB version is not automatically upgraded. For replacement requirements and procedures, see Replace SQL Server Express LocalDB.

More database information:

- Databases
- CTX114501 lists the most currently supported databases
- Database sizing guidance
- Local Host Cache

Web Studio

> **Note:**
>
> - You can manage your Citrix Virtual Apps and Desktops deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.
> - Web Studio is a web-based management console that lets you configure and manage your on-premises Citrix Virtual Apps and Desktops deployment. It's designed for an improved user experience and generally responds faster than Citrix Studio, the Windows-based management console. See Install Web Studio.

For information about supported operating systems, browsers, display settings, and hardware requirements for installing and using Web Studio, see System requirements in the Web Studio article.

Citrix Director

Supported operating systems:

- Windows Server 2025
- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, Standard and Datacenter Editions, and with the Server Core option

Requirements:

- Microsoft .NET Framework 4.8 is installed automatically if it (or a later version) is not already installed.
- Microsoft Internet Information Services (IIS) 7.0 and ASP.NET 2.0. Ensure that the IIS server role has the Static Content role service installed. If this software is not already installed, you are prompted for the Windows Server installation media. Then, that software is installed for you.

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

- To view the event logs on machines where Citrix Director is installed, you must install Microsoft .NET Framework 2.0.

Citrix Profile Management:

- Ensure that the Citrix Profile Management and Citrix Profile Management WMI Plug-in are installed on the VDA (**Additional Components** page in the installation wizard) and that the Citrix Profile Management Service is running to view the user profile details in Director.

System Center Operations Manager (SCOM) integration requirements:

- System Center 2012 R2 Operations Manager

Supported browsers for viewing Director:

- Microsoft Edge.
- Firefox ESR (Extended Support Release).
- Chrome.

The recommended optimal screen resolution for viewing Director is 1440 x 1024.

Virtual Delivery Agent (VDA) for single-session OS

Supported operating systems:

- Windows 11
- Windows 10 (x64 only), any version that is currently in mainstream support.
    - For edition support, see Knowledge Center article CTX224843.

Requirements:

- Microsoft .NET Framework 4.8 is installed automatically if it (or a later version) is not already installed.
- Microsoft Visual C++ 2015–2022 Redistributable.

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 on Windows 11 and Windows 10.

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 single-session

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

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. For more information, see Prepare to install.

For Linux VDA information, see the Linux Virtual Delivery Agent articles.

To use the Server VDI feature, you can use the command-line interface to install a VDA for Windows single-session OS on a supported Windows Server machine. See Server VDI for guidance.

For information about installing a VDA on a Windows 7 machine, see Earlier operating systems.

Virtual Delivery Agent (VDA) for multi-session OS

Supported operating systems:

- Windows Server 2025
- Windows 11 (supported only with Citrix DaaS™)
- Windows 10 (x64 only; supported only with Citrix DaaS), any version that is currently in mainstream support.
- Windows Server 2022
- Windows Server 2019, Standard, and Datacenter Editions

The installer automatically deploys the following requirements, which are also available on the Citrix installation media in the **Support** folders:

- Microsoft .NET Framework 4.8 is installed automatically if it (or a later version) is not already installed.
- Microsoft Visual C++ 2015–2022 Redistributable.

The installer automatically installs and enables Remote Desktop Services role services, if they are not already installed and enabled.

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 will not be able to log on to the machine. On most Windows Server versions, the Media Foundation feature is installed through the Server Manager. For more information, see Prepare to install.

If the Media Foundation is not present on the VDA, these multimedia features do not work:

- Windows Media Redirection
- HTML5 Video Redirection
- HDX™ RealTime Webcam Redirection

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

For Linux VDA information, see the Linux Virtual Delivery Agent articles.

For information about installing a VDA on a Windows Server 2008 R2 machine, see Earlier operating systems.

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. Knowledge Center article CTX131239 contains current version information, plus links to known issues.

Some features might not be supported on all host platforms or all platform versions. See the feature documentation for details.

The Remote PC Access Wake on LAN feature requires Microsoft System Center Configuration Manager minimum 2012.

Supported hypervisors:

- **Azure Local**

  For more information, see Azure Local environments.

- **XenServer (formerly Citrix Hypervisor™)**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see XenServer virtualization 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 Acropolis**

  CTX131239 contains current version information, plus links to known issues.

  For more information, see Nutanix virtualization environments.

- **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.

Supported public cloud hosts:

- **Amazon Web Services (AWS)**

  For information about using AWS to provision virtual machines, see Amazon Web Services virtualization environments.

- **Google Cloud Platform**
  For more information, see Google Cloud Platform virtualization environments and Getting Started with Citrix DaaS on Google Cloud.

- **Microsoft Azure Resource Manager**

  For information about using Microsoft Azure Resource Manager to provision virtual machines, see Microsoft Azure Resource Manager virtualization environments.

- **Red Hat OpenShift**

  For information about using Red Hat OpenShift to provision virtual machines, see Red Hat OpenShift virtualization environments.

- **Nutanix cloud and partner solutions**

  For information about using Nutanix cloud and partner solutions, see Nutanix cloud and partner solutions.

- **VMware cloud and partner solutions**

  For information about using VMware cloud and partner solutions, see VMware cloud and partner solutions.

When adding public cloud host connections to your deployment, consider the following:

- You need a Hybrid Rights License. For information about Hybrid Rights License, see Transition and Trade-Up (TTU) with Hybrid Rights. For information about adding a license, see Create a site.
- The information sources direct you to the Citrix DaaS documentation. If you are familiar with the public cloud hosts in the Citrix DaaS product, the on-premises version has several differences.
  - In Citrix DaaS, the management interface is known as Full Configuration. In on-premises Citrix Virtual Apps and Desktops, the management interface is known as Web Studio.
  - Updates are rolled out to Citrix DaaS approximately every four weeks. So, you might find that certain features available with Citrix DaaS are not available with the on-premises version.

Active Directory functional levels

The following functional levels for the Active Directory forest and domain are supported:

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

- Windows Server 2025
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

> **Note:**
>
> Before upgrading the Citrix Virtual Apps and Desktops site, review the requirements for individual features, as newer features and VDAs might need specific minimum Active Directory functional levels.

HDX

Audio

UDP audio for Multi-Stream ICA® is supported on Citrix Workspace app for Windows and Citrix Workspace app for Linux 13.

Echo cancellation is supported on Citrix Workspace app for Windows.

See the specific HDX feature support and requirements. For more information on HDX features and Citrix Workspace apps, see the Feature matrix.

HDX Windows Media delivery

The following clients are supported for Windows Media client-side content fetching, Windows Media redirection, and real-time Windows Media multimedia transcoding: Citrix Workspace app for Windows, Citrix Workspace app for iOS, and Citrix Workspace app for Linux.

To use Windows Media client-side content fetching on Windows 8 devices, set the Citrix Multimedia Redirector as a default program: in **Control Panel > Programs > Default Programs > Set your default programs**, select **Citrix Multimedia Redirector** and click either **Set this program as default** or **Choose defaults for this program**. GPU transcoding requires an NVIDIA CUDA-enabled GPU with Compute Capability 1.1 or higher; see https://developer.nvidia.com/cuda/cuda-gpus.

HDX 3D Pro

The VDA for Windows single-session OS detects the presence of GPU hardware at runtime.

The physical or virtual machine hosting the application can use GPU Passthrough or Virtual GPU (vGPU):

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

- GPU Passthrough is available with:
  - XenServer®
  - Nutanix AHV
  - VMware vSphere and VMware ESX, where it is referred to as virtual Direct Graphics Acceleration (vDGA)
- vGPU is available with:
  - XenServer
  - Nutanix AHV
  - VMware vSphere

See https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/2507-ltsr/graphics/hdx-3d-pro.

Citrix recommends that the host computer has at least 4 GB of RAM and four virtual CPUs with a clock speed of 2.3 GHz or higher.

Graphical Processing Unit (GPU):

- For virtualized graphics acceleration using the NVIDIA GRID API, you can use HDX 3D Pro with all the NVIDIA GRID GPUs supported by the NVIDIA Virtual GPU (vGPU) software version 13 and up, see https://docs.nvidia.com/grid/index.html.
  For a detailed list of supported Hypervisors and supported hardware, see the NVIDIA vGPU software documentation.
- Virtualized graphics acceleration is supported on the Intel Xeon Processor E3 Family of data center graphics platforms and the Intel data center GPU Flex series. For more information, see GPU Flex series.
- AMD GPUs are supported with AMD's mxGPU virtualization. For more information on supported hardware, see AMD documentation.

User device:

- Citrix supports up to 8 4k monitors, depending on the hardware resources. Depending on the GPU used, there can be other hardware restrictions on this maximum.
- Citrix recommends that user devices have at least 4 GB of RAM and a CPU with a clock speed of 1.6 GHz or higher. For optimum performance, we recommend that user devices have at least 8 GB of RAM and a dual-core CPU with a clock speed of 3 GHz or higher.
- For multi-monitor access, Citrix recommends user devices with quad-core CPUs.
- Citrix Workspace app must be installed.

For more information, see the HDX 3D Pro articles and www.citrix.com/xenapp/3d.

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

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 2022
- Windows Server 2019

Requirements:

- Microsoft Visual C++ 2015–2022 Redistributable
- Microsoft .NET Framework 4.8 (minimum)

For VDAs for Multi-session OS, 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.

Other

Only Citrix License Server 11.17.2 and later are supported. For more information, see Licensing.

See the Product Matrix for more information about version compatibility.

For supported StoreFront versions, see the StoreFront system requirements.

The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the site configuration database. If you install `CitrixGroupPolicyManagement_x64.msi` separately (for example, on a machine that does not have a Citrix Virtual Apps and Desktops core component installed), that machine must have Visual Studio 2015 runtime installed. For more information, see the Microsoft documentation.

If you want to edit domain GPOs using GPMC, enable the Group Policy Management feature (in the Windows Server Manager) on all machines containing Delivery Controllers.

Multiple NICs are supported.

By default, the Citrix Workspace app for Windows is not installed when you install a current VDA. For more information, see the Citrix Workspace app for Windows documentation.

See Local App Access for supported browser information for that feature.

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

This version of Citrix Virtual Apps and Desktops requires a minimum of HDX RealTime Connector 2.9 LTSR. For more information, see the HDX RealTime Optimization Pack documentation.

This product supports PowerShell versions 3 through 5.

Technical overview

September 13, 2025

Citrix Virtual Apps and Desktops™ are virtualization solutions that give IT control of virtual machines, applications, licensing, and security while providing anywhere access for any device.

Citrix Virtual Apps and Desktops allow:

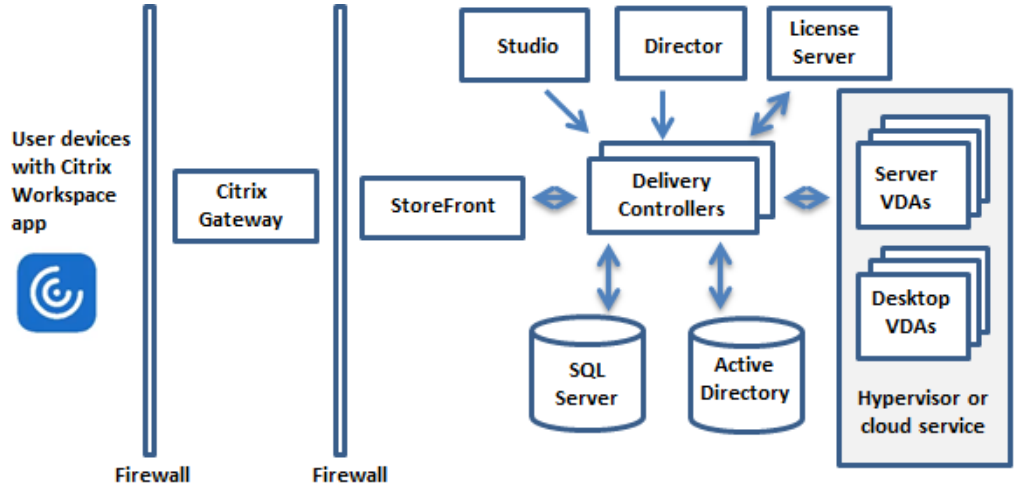
- End users to run applications and desktops independently of the device's operating system and interface.
- Administrators to manage the network and control access from selected devices or from all devices.
- Administrators to manage an entire network from a single data center.

Citrix Virtual Apps and Desktops share a unified architecture called FlexCast Management Architecture (FMA). FMA's key features are the ability to run multiple versions of Citrix Virtual Apps or Citrix Virtual Desktops™ from a single site and integrated provisioning.

Key components

This article is most helpful if you're new to Citrix Virtual Apps and Desktops.

This illustration shows the key components in a typical deployment, which is called a site.



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

Delivery Controller™

The Delivery Controller is the central management component of a site. Each site has one or more Delivery Controllers. It is installed on at least one server in the data center. For site reliability and availability, install Controllers on more than one server. If your deployment includes a hypervisor or other service, the Controller services communicate with it to:

- Distribute applications and desktops
- Authenticate and manage user access
- Broker connections between users and their desktops and applications
- Optimize user connections
- Load balance the connections

The Controller's Broker Service tracks which users are logged on and where, what session resources the users have, and if users need to reconnect to existing applications. The Broker Service runs PowerShell cmdlets and communicates with a broker agent on the VDAs over TCP port 80. It does not have the option to use TCP port 443.

The Monitor Service collects historical data and places it in the monitoring database. This service uses TCP port 80 or 443.

Data from the Controller services is stored in the site database.

The Controller manages the state of desktops, starting and stopping them based on demand and administrative configuration.

Database

At least one Microsoft SQL Server database is required for every site to store configuration and session information. This database stores the data collected and managed by the services that make up the Controller. Install the database within your data center, and ensure it has a persistent connection to the Controller.

The site also uses a configuration logging database and a monitoring database. By default, those databases are installed in the same location as the site database, but you can change this.

Virtual Delivery Agent (VDA)

The VDA is installed on each physical or virtual machine in your site that you make available to users. Those machines deliver applications or desktops. The VDA enables the machine to register with the Controller, which in turn allows the machine and the resources it is hosting to be made available to users. VDAs establish and manage the connection between the machine and the user device. VDAs

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

also verify that a Citrix® license is available for the user or session, and apply policies that are configured for the session.

The VDA communicates session information to the Broker Service in the Controller through the broker agent in the VDA. The broker agent hosts multiple plug-ins and collects real-time data. It communicates with the Controller over TCP port 80.

The word "VDA"is often used to refer to the agent and the machine on which it is installed.

VDAs are available for single-session and multi-session Windows operating systems. VDAs for multi-session Windows operating systems allow multiple users to connect to the server at a time. VDAs for single-session Windows operating systems allow only one user to connect to the desktop at a time. Linux VDAs are also available.

Citrix StoreFront™

StoreFront authenticates users and manages stores of desktops and applications that users access. It can host your enterprise application store, which gives users self-service access to the desktops and applications that you make available to them. It also keeps track of users'application subscriptions, shortcut names, and other data. This helps ensure that users have a consistent experience across multiple devices.

Citrix Workspace™ app

Installed on user devices and other endpoints (such as virtual desktops), Citrix Workspace app provides users with quick, secure, self-service access to documents, applications, and desktops. Citrix Workspace app provides on-demand access to Windows, web, and Software as a Service (SaaS) applications. For devices that can't install the device-specific Citrix Workspace app software, Citrix Workspace app for HTML5 provides a connection through an HTML5-compatible web browser.

Studio

You can manage your Citrix Virtual Apps and Desktops deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This product documentation covers only Web Studio. For information about Citrix Studio, see Citrix Virtual Apps and Desktops 7 2212 or earlier.

Web Studio Web Studio is a web-based management console that lets you configure and manage your on-premises Citrix Virtual Apps and Desktops deployment. It's designed for an improved user experience and generally responds faster than Citrix Studio, the Windows-based management console.

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

For more information, see Install Web Studio.

Citrix Studio Citrix Studio is the management console where you configure and manage your Citrix Virtual Apps and Desktops deployment. Citrix Studio eliminates the need for separate management consoles for managing delivery of applications and desktops. Citrix Studio provides wizards to guide you through environment setup, creating workloads to host applications and desktops, and assigning applications and desktops to users. You can also use Studio to allocate and track Citrix licenses for your site.

Citrix Studio gets the information it displays from the Broker Service in the Controller, communicating over TCP port 80.

Secure Private Access

Citrix Secure Private Access on-premises solution enhances an organization's overall security and compliance posture with the ability to easily deliver Zero Trust Network Access to browser-based apps (internal web apps and SaaS apps) using StoreFront as a unified access portal to web and SaaS apps, along with virtual apps and desktops as an integrated part of Citrix Workspace. The solution is compatible with existing releases of NetScaler and StoreFront without any changes to the versions. For details, see Secure Private Access for on-premises.

Citrix Director

Director is a web-based tool that enables IT support and help desk teams to monitor an environment, troubleshoot issues before they become system-critical, and perform support tasks for end users. You can use one Director deployment to connect to and monitor multiple Citrix Virtual Apps or Citrix Virtual Desktops sites.

Director displays:

- Real-time session data from the Broker Service in the Controller, which includes data the Broker Service gets from the broker agent in the VDA.
- Historical site data from the Monitor Service in the Controller.

Director uses the ICA® performance and heuristics data captured by the Citrix Gateway device to build analytics from the data and then presents it to the administrators.

You can also view and interact with a user's sessions through Director, using Windows Remote Assistance.

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

Citrix License Server

The License Server manages your Citrix product licenses. It communicates with the Controller to manage licensing for each user's session and with Studio to allocate license files. A site must have at least one license server to store and manage your license files.

Hypervisor or other service

The hypervisor or other service hosts the virtual machines in your site. These can be the VMs you use to host applications and desktops, and VMs you use to host the Citrix Virtual Apps and Desktops components. A hypervisor is installed on a host computer dedicated entirely to running the hypervisor and hosting virtual machines.

Citrix Virtual Apps and Desktops support various hypervisors and other services.

Although many deployments require a hypervisor, you don't need one to provide Remote PC Access. A hypervisor is also not required when you are using Provisioning Services (PVS) to provision VMs.

Additional components

The following components can also be included in Citrix Virtual Apps and Desktops deployments. For more information, see their documentation.

Citrix Provisioning™

Citrix Provisioning (formerly Provisioning Services) is an optional component that is available with some editions. It provides an alternative to MCS for provisioning virtual machines. Whereas MCS creates copies of a master image, PVS streams the master image to user devices. PVS doesn't require a hypervisor to do this, so you can use it to host physical machines. PVS communicates with the Controller to provide users with resources.

Citrix Gateway

When users connect from outside the corporate firewall, Citrix Virtual Apps and Desktops can use Citrix Gateway (formerly Access Gateway and NetScaler® Gateway) technology to secure these connections with TLS. The Citrix Gateway or VPX virtual appliance is an SSL VPN appliance that is deployed in the demilitarized zone (DMZ). It provides a single secure point of access through the corporate firewall.

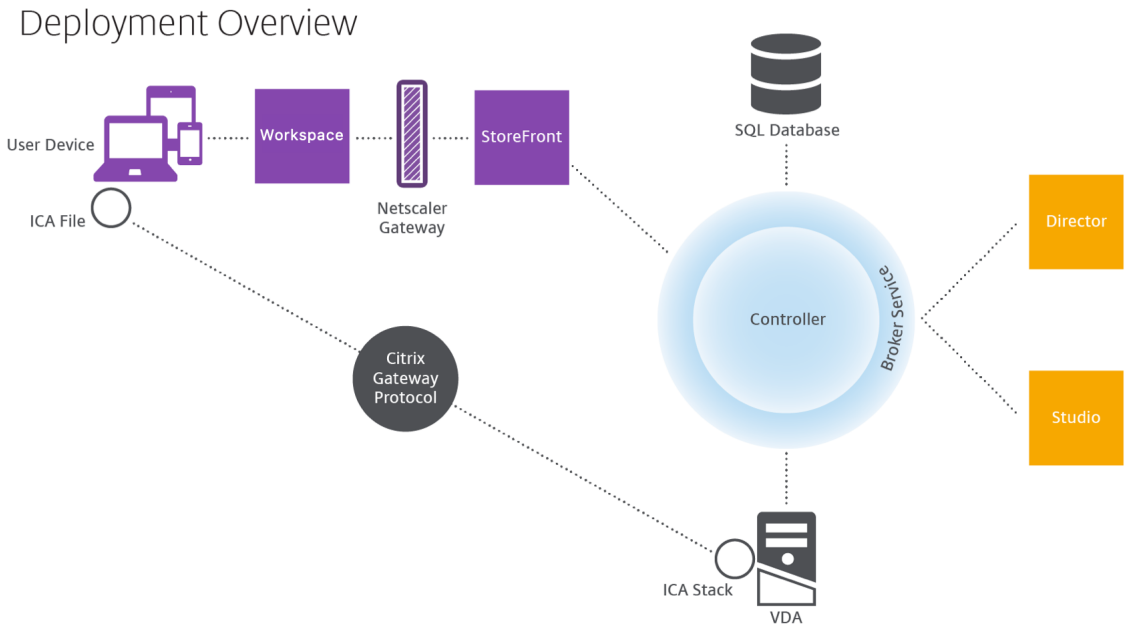
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix SD-WAN™

In deployments where virtual desktops are delivered to users at remote locations such as branch offices, Citrix SD-WAN technology can be employed to optimize performance. Repeaters accelerate performance across WANs. With repeaters in the network, users in the branch office experience LAN-like performance over the WAN. Citrix SD-WAN can prioritize different parts of the user experience so that, for example, the user experience does not degrade in the branch location when a large file or print job is sent over the network. HDX™ WAN optimization provides tokenized compression and data deduplication, dramatically reducing bandwidth requirements and improving performance.

How typical deployments work

A site is made up of machines with dedicated roles that allow for scalability, high availability, and failover, and provide a solution that is secure by design. A site consists of VDA-installed servers and desktop machines, and the Delivery Controller, which manages access.



The VDA enables users to connect to desktops and applications. It is installed on virtual machines in the data center for most delivery methods, but it can also be installed on physical PCs for Remote PC Access.

The Controller is made up of independent Windows services that manage resources, applications, and desktops, and optimize and balance user connections. Each site has one or more Controllers. Because sessions are affected by latency, bandwidth, and network reliability, place all Controllers on the same LAN, if possible.

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

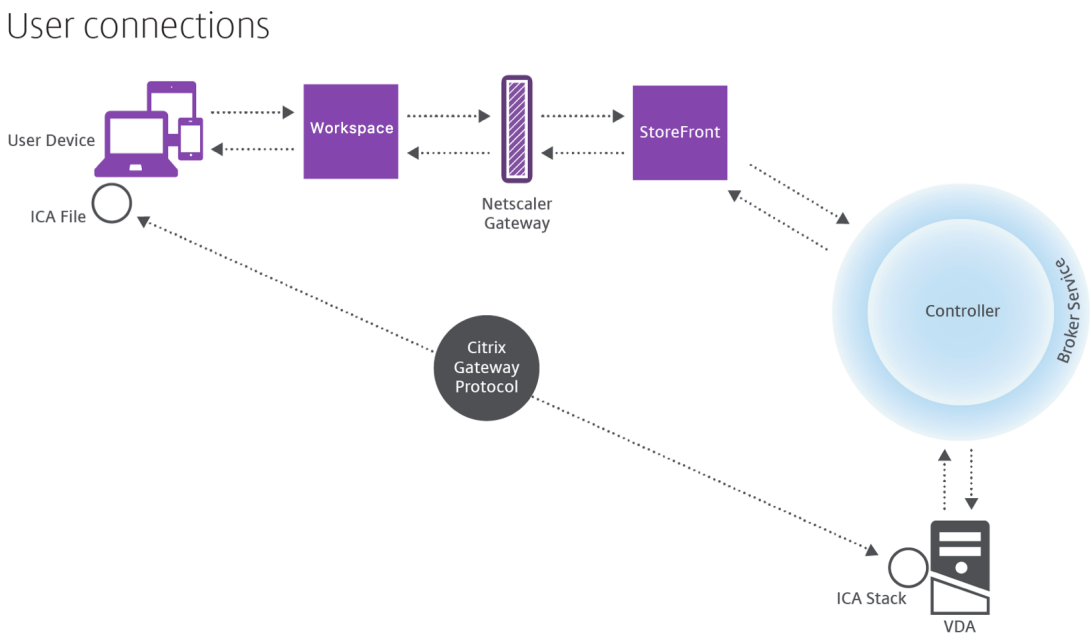
Users never directly access the Controller. The VDA serves as an intermediary between users and the Controller. When users log on using StoreFront, their credentials pass through to the Broker Service on the Controller. The Broker Service then obtains profiles and available resources based on the policies set for them.

How user connections are handled

To start a session, the user connects either through Citrix Workspace app installed on the user's device, or a StoreFront website.

The user selects the physical or virtual desktop or virtual application that is needed.

The user's credentials move through this pathway to access the Controller, which determines which resources are needed by communicating with a Broker Service. Citrix recommends that administrators place an SSL certificate on StoreFront to encrypt the credentials coming from Citrix Workspace app.



The Broker Service determines which desktops and applications the user is allowed to access.

After the credentials are verified, information about available applications or desktops is sent back to the user through the StoreFront-Citrix Workspace app pathway. When the user selects applications or desktops from this list, that information goes back down the pathway to the Controller. The Controller then determines the proper VDA to host the specific applications or desktop.

The Controller sends a message to the VDA with the user's credentials, and then sends all the data about the user and the connection to the VDA. The VDA accepts the connection and sends the information back through the same pathways to Citrix Workspace app. A set of required parameters is

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

collected on StoreFront. These parameters are then sent to Citrix Workspace app either as part of the Citrix-Workspace-app-StoreFront protocol conversation, or converted to an Independent Computing Architecture (ICA) file and downloaded. As long as the site was properly set up, the credentials remain encrypted throughout this process.

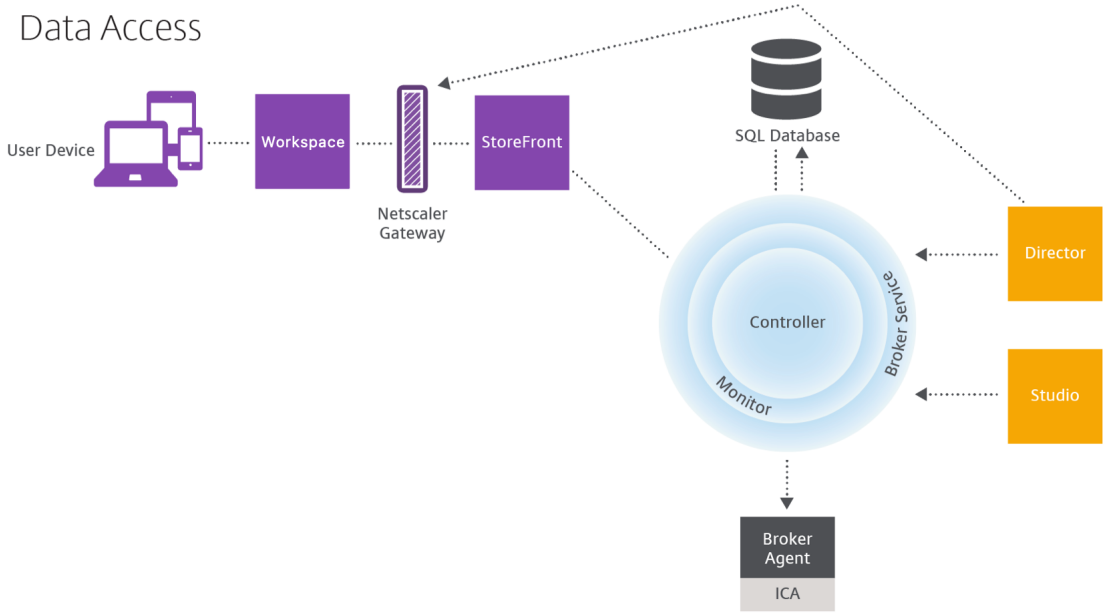
The ICA file is copied to the user's device and establishes a direct connection between the device and the ICA stack running on the VDA. This connection bypasses the management infrastructure (Citrix Workspace app, StoreFront, and Controller).

The connection between Citrix Workspace app and the VDA uses the Citrix Gateway Protocol (CGP). If a connection is lost, the Session Reliability feature enables the user to reconnect to the VDA rather than having to relaunch through the management infrastructure. Session Reliability can be enabled or disabled in Citrix policies.

After the client connects to the VDA, the VDA notifies the Controller that the user is logged on. The Controller then sends this information to the site database and starts logging data in the monitoring database.

How data access works

Every Citrix Virtual Apps and Desktops session produces data that IT can access through Studio or Director. Using Studio, administrators can access real-time data from the Broker Agent to manage sites. Director accesses the same data plus historical data stored in the monitoring database. It also accesses HDX data from NetScaler Gateway for help desk support and troubleshooting.



Within the Controller, the Broker Service reports session data for every session on the machine provid-

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

ing real-time data. The Monitor Service also tracks the real-time data and stores it as historical data in the monitoring database.

Studio communicates only with the Broker Service. It accesses only real-time data. Director communicates with the Broker Service (through a plug-in in the Broker Agent) to access the site database.

Director can also access Citrix Gateway to get information on the HDX data.

Deliver desktops and applications

You set up the machines that deliver applications and desktops with machine catalogs. Then, you create delivery groups that specify the applications and desktops that will be available (using machines in the catalogs), and which users can access them. Optionally, you can then create application groups to manage collections of applications.

Machine catalogs

Machine catalogs are collections of virtual or physical machines that you manage as a single entity. These machines, and the application or virtual desktops on them, are the resources you provide to your users. All the machines in a catalog have the same operating system and the same VDA installed. They also have the same applications or virtual desktops.

Typically, you create a master image and use it to create identical VMs in the catalog. For VMs you can specify the provisioning method for the machines in that catalog: Citrix tools (Citrix Provisioning or MCS) or other tools. Alternatively, you can use your own existing images. In that case, you must manage target devices on an individual basis or collectively using third-party electronic software distribution (ESD) tools.

Valid machine types are:

- **Multi-session OS:** Virtual or physical machines with a multi-session operating system. Used for delivering Citrix Virtual Apps published apps (also known as server-based hosted applications) and Citrix Virtual Apps published desktops (also known as server-hosted desktops). These machines allow multiple users to connect to them at one time.
- **Single-session OS:** Virtual or physical machines with a single-session operating system. Used for delivering VDI desktops (desktops running single-session OSs that can optionally be personalized), VM hosted apps (applications from single-session OSs), and hosted physical desktops. Only one user at a time can connect to each of these desktops.
- **Remote PC Access:** Enables remote users to access their physical office PCs from any device running Citrix Workspace app. The office PCs are managed through the Citrix Virtual Desktops deployment, and require user devices to be specified in an allow list.

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

For more information, see Citrix Virtual Apps and Desktops Image Management and Create machine catalogs.

Delivery groups

Delivery groups specify which users can access which applications, desktops, or both on which machines. Delivery groups contain machines from your machine catalogs, and Active Directory users who have access to your site. You might assign users to your delivery groups by their Active Directory group, because Active Directory groups and delivery groups are ways to group users with similar requirements.

Each delivery group can contain machines from more than one catalog, and each catalog can contribute machines to more than one delivery group. However, each individual machine can only belong to one delivery group at a time.

You define which resources users in the delivery group can access. For example, to deliver different applications to different users, you might install all the applications on the master image for one catalog and create enough machines in that catalog to distribute among several delivery groups. You can then configure each delivery group to deliver a different subset of applications that are installed on the machines.

For more information, see Create delivery groups.

Application groups

Application groups provide application management and resource control advantages over using more delivery groups. Using the tag restriction feature, you can use your existing machines for more than one publishing task, saving the costs associated with deployment and managing more machines. A tag restriction can be thought of as subdividing (or partitioning) the machines in a delivery group. Application groups can also be helpful when isolating and troubleshooting a subset of machines in a delivery group.

For more information, see Create application groups.

More information

- Citrix Virtual Apps and Desktops diagrams
- Network ports
- Databases
- Supported hypervisors and other services

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

Databases

July 16, 2026

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

A Citrix Virtual Apps or Citrix Virtual Desktops™ site uses three SQL Server databases:

- **Site:** (also known as site configuration) stores the running site configuration, plus the current session state and connection information.
- **Logging:** (also known as Configuration Logging) stores information about site configuration changes and administrative activities. This database is used when the configuring logging feature is enabled (default = enabled).
- **Monitoring:** stores data used by Director, such as session and connection information.

Each Delivery Controller communicates with the site database. Windows authentication is required between the Controller and the databases. A Controller can be unplugged or turned off without affecting other Controllers in the site. This means, however, that the site database forms a single point of failure. If the database server fails, existing connections continue to function until a user either logs off or disconnects. For information about connection behavior when the site database becomes unavailable, see Local Host Cache.

Citrix recommends the following regarding databases:

- **Back up regularly.** Back up the databases regularly so that you can restore from the backup if the database server fails. The backup strategy for each database can differ. For more information, see CTX135207; note, however, that it refers to CitrixXenDesktopDB, which is no longer supported or available to customers.
- **Back up and restore the Site, Monitoring and Logging SQL Server databases regularly.** For specific information about SQL Server databases, see Creating Full and Differential Backups of a SQL Server Database.

If your site contains more than one zone, ensure that the primary zone always contains the site database. Controllers in every zone communicate with that database.

High availability

There are several high availability solutions to consider for ensuring automatic failover:

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

- **AlwaysOn Availability Groups (including Basic Availability Groups):** This enterprise-level high availability and disaster recovery solution introduced in SQL Server 2012 enables you to maximize availability for one or more databases. AlwaysOn Availability Groups requires that the SQL Server instances reside on Windows Server Failover Clustering (WSFC) nodes. For more information, see Windows Server Failover Clustering with SQL Server.
- **SQL Server database mirroring:** Mirroring the database ensures that, if you lose the active database server, an automatic failover process happens in a matter of seconds, so that users are generally unaffected. This method is more expensive than other solutions because full SQL Server licenses are required on each database server. You cannot use SQL Server Express edition in a mirrored environment.
- **SQL clustering:** The Microsoft SQL clustering technology can be used to automatically allow one server to take over the tasks and responsibilities of another server that has failed. However, setting up this solution is more complicated, and the automatic failover process is typically slower than alternatives such as SQL mirroring.
- **Using the hypervisor's high availability features:** With this method, you deploy the database as a virtual machine and use your hypervisor's high availability features. This solution is less expensive than mirroring because it uses your existing hypervisor software and you can also use SQL Server Express edition. However, the automatic failover process is slower, as it can take time for a new machine to start for the database, which might interrupt the service to users.

The Local Host Cache feature supplements the SQL Server high availability best practices. Local Host Cache enables users to connect and reconnect to applications and desktops even when the site database is not available. For more information, see Local Host Cache.

If all Controllers in a site fail, you can configure the VDAs to operate in high availability mode, which allows users to continue to access their desktops and applications. In high availability mode, the VDA accepts direct ICA connections from users, rather than connections brokered by the Controller. Use this feature only on the rare occasion when communication with all Controllers fails. The feature is not an alternative to other high availability solutions. For more information, see CTX 127564.

Installing a Controller on a node in an SQL clustering or SQL mirroring installation is not supported.

Install database software

> **Note:**
>
> Starting with version 2411, you can use Azure SQL Managed Instance for databases.

By default, SQL Server Express edition is installed when you install the first Delivery Controller™ if another SQL Server instance is not detected on that server. That default action is usually sufficient for proof of concept or pilot deployments. However, SQL Server Express does not support Microsoft high availability features.

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

The default installation uses the default Windows service accounts and permissions. See the Microsoft documentation for details of these defaults, including the addition of Windows service accounts to the sysadmin role. The Controller uses the Network Service account in this configuration. The Controller does not require any additional SQL Server roles or permissions.

If necessary, you can select **Hide instance** for the database instance. When configuring the address of the database in Web Studio, enter the instance's static port number, rather than its name. See the Microsoft documentation for details about hiding an instance of SQL Server Database Engine.

For most production deployments, and any deployment that uses Microsoft high availability features, we recommend using only supported non-Express editions of SQL Server. Install SQL Server on machines other than the server where the first Controller is installed. System requirements lists the supported SQL Server versions. The databases can reside on one or more machines.

Ensure the SQL Server software is installed before creating a site. You don't have to create the database, but if you do, it must be empty. Configuring Microsoft high availability technologies is also recommended.

Use Windows Update to keep SQL Server up-to-date.

Set up the databases from the site creation wizard

Specify the database names and addresses (location) on the **Databases** page in the site creation wizard. (See Database address formats.) To avoid potential errors when Director queries the Monitor Service, do not use whitespace in the name of the monitoring database.

The **Databases** page offers two options for setting up the databases: automatic and using scripts. Generally, you can use the automatic option if you (the Web Studio user and Citrix administrator) have the required database privileges. (See Permissions required to set up databases.)

You can change the location of the configuration logging and monitoring database later, after you create the site. See Change database locations.

To configure a site to use a mirror database, complete the following and then proceed with the automatic or scripted setup procedures.

1. Install the SQL Server software on two servers, A and B.
2. On Server A, create the database intended to be used as the principal. Back up the database on Server A and then copy it to server B.
3. On Server B, restore the backup file.
4. Start mirroring on server A.

To verify mirroring after creating the site, run the PowerShell cmdlet `get-configdbconnection` to ensure that the Failover Partner has been set in the connection string to the mirror.

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

If you later add, move, or remove a Delivery Controller in a mirrored database environment, see Delivery Controllers.

Automatic setup

If you have the required database privileges, select **Create and set up databases from Studio** on the **Databases** page of the site creation wizard. Then provide the names and addresses of the principal databases.

If a database exists at an address you specify, it must be empty. If databases don't exist at a specified address, you are informed that a database cannot be found, and then asked if you want the database to be created for you. When you confirm that action, Web Studio automatically creates the databases, and then applies the initialization scripts for the principal and replica databases.

Scripted setup

If you do not have the required database rights, request assistance from someone who does, such as a database administrator. Here is the sequence:

1. On the **Databases** page in the site creation wizard, select **Generate scripts to manually set up**. This action generates the following three types of scripts for each of the following principal and the replica databases: site, monitoring, and logging databases.

   - *Script containing "SysAdmin" in its name*. A script that creates the databases and the Delivery Controller login. These tasks require securityadmin rights.
   - *Script containing "DbOwner" in its name*. A script that creates the user roles in the database, adds the logins, and then creates the database schemas. These tasks require `db_owner` rights.
   - *Script containing "Mixed" in its name*. All tasks in one script, regardless of required rights.

   You can indicate where to store the scripts.

   > **Note:**
   >
   > In enterprise environments, database setup includes scripts that might be handled by different teams with different roles (rights): `securityadmin` or `db_owner`. If applicable, you first have "SysAdmin" scripts run by administrators with the `securityadmin` role and then "DbOwner" scripts run by administrators with `db_owner` rights. To generate those scripts, you can also use PowerShell. For details, see Preferred database rights scripts.

2. Give those scripts to your database administrator. The site creation wizard stops automatically at this point. You are prompted when you return later to continue the site creation.

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

The database administrator then creates the databases. Each database must have the following characteristics:

- Use a collation that ends with `_CI_AS_KS`. We recommend using a collation that ends with `_100_CI_AS_KS`.
- For optimum performance, enable the SQL Server Read-Committed Snapshot. For details, see CTX 137161.
- Configured high availability features, if applicable.
- To configure mirroring, first set the database to use the full recovery model (simple model is the default). Back up the principal database to a file and copy it to the mirror server. Then, restore the backup file on the mirror server. Finally, start mirroring on the principal server.

The database administrator uses the SQLCMD command-line utility or SQL Server Management Studio in SQLCMD mode to:

- Run each of the `xxx_Replica.sql` scripts on the high availability SQL Server database instances (if high availability is configured)
- Run each of the `xxx\\_Principal.sql` scripts on the principal SQL Server database instances.

See the Microsoft documentation for SQLCMD details.

When all the scripts complete successfully, the database administrator gives the Citrix administrator the three principal database addresses.

Web Studio prompts you to continue the site creation. You are returned to the **Databases** page. Enter the addresses. If any of the servers hosting a database cannot be contacted, an error message appears.

Permissions required to set up databases

You must be a local administrator and a domain user to create and initialize the databases (or change the database location). You must also have certain SQL Server permissions. The following permissions can be explicitly configured or acquired by Active Directory group membership. If your Web Studio user credentials do not include these permissions, you are prompted for SQL Server user credentials.

Operation	Purpose	Server role	Database role
Create a database	Create a suitable empty database	`dbcreator`	

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

Operation	Purpose	Server role	Database role
Create a schema	Create all service-specific schemas and add the first Controller to the site	securityadmin*	db_owner
Add a Controller	Add a Controller (other than the first) to the site	securityadmin*	db_owner
Add a Controller (mirror server)	Add a Controller login to the database server currently in the mirror role of a mirrored database	securityadmin*	
Remove Controller	Remove controller from site	**	db_owner
Update a schema	Apply schema updates or hotfixes		db_owner

* While technically more restrictive, in practice, you can treat the securityadmin server role as equivalent to the sysadmin server role.

** When a Controller is removed from a site, the Controller logon to the database server is not removed. This is to avoid potentially removing a logon being used by services other than this Citrix product on the same machine. The logon must be removed manually if it is no longer required. This action requires securityadmin server role membership.

When using Web Studio to perform these operations, the Web Studio user must either have a database server account that is explicitly a member of the appropriate server roles, or be able to provide credentials of an account that is.

Preferred database rights scripts

In enterprise environments, database setup includes scripts that must be handled by different teams with different roles (rights): securityadmin or db_owner.

Using PowerShell, you can specify the preferred database rights. Specifying a nondefault value results in the creation of separate scripts. One script contains tasks that need the securityadmin role. The other script requires only db_owner rights and can be run by a Citrix administrator, without having to contact a database administrator.

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

In the `get-*DBSchema` cmdlets, the `-DatabaseRights` option has the following valid values:

- `SA`: Generates a script that creates the databases and the Delivery Controller login. These tasks require `securityadmin` rights.
- `DBO`: Generates a script that creates the user roles in the database, adds the logins, and then creates the database schemas. These tasks require `db_owner` rights.
- `Mixed`: (Default) All tasks in one script, regardless of required rights.

For more information, see the cmdlet help.

Database address formats

You can specify a database address in one of the following forms:

- `ServerName`
- `ServerName\InstanceName`
- `ServerName,PortNumber`

For an AlwaysOn Availability Group, specify the group's listener in the location field.

For database mirroring, specify only the principal server address. Citrix Site Manager locates the mirror server based on the principal server.

For more information about how to configure standalone SQL server, Database Mirroring, and Always on High Availability, see this CTX article.

Change database locations

After you create a site, you can change the location of the *configuration logging* and *monitoring* databases. However, you cannot change the location of the *site* database. When you change the location of a database, keep the following notes in mind:

- The data in the previous database is not imported to the new database.
- Logs cannot be aggregated from both databases when retrieving logs.
- The first log entry in the new database indicates that a database change occurred, but it does not identify the previous database.
- You cannot change the location of the configuration logging database when mandatory logging is enabled.
- Changing database locations between SQL Server and Azure SQL isn't supported.

To change the location of a database:

1. If you use Microsoft SQL Server, ensure that a supported version is installed on the server where you want the database to reside. Set up high-availability features as needed.

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

2. Sign in to Web Studio, and then select **Settings** in the left pane.
3. Locate the **Database** tile and select **Edit**.
4. On the **Manage Database** page, select the database for which you want to specify a new location and then select **Change Database** in the action bar.
5. Specify the new location and the database name. If the database is hosted on Azure SQL, type the credentials of a service principal with permission to manage the database.
6. If you want Web Studio to create the database and you have the appropriate permissions, click **Done**. When prompted, click **Done**, and then Web Studio creates the database automatically. Web Studio attempts to access the database using your credentials. If that fails, you are prompted for the database user's credentials. Web Studio then uploads the database schema to the database. The credentials are retained only for the database creation time frame.
7. If you do not want Web Studio to create the database, or you do not have sufficient permissions, click **Generate database script**. The generated scripts include instructions for manually creating the database and a mirror database, if needed. Before uploading the schema, ensure that the database is empty and that at least one user has permission to access and change the database.

More information

- Database sizing tool.
- Sizing the site database and configuring connection strings when using SQL Server high availability solutions.

Delivery methods

September 6, 2025

Citrix Virtual Apps and Desktops™ offers various delivery methods. A single delivery method will likely not meet all of your requirements.

Introduction

Choosing the appropriate application delivery 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.

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

- **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 and isolated from the base operating system and each other. This isolation helps address compatibility issues. For details, see Deploy and deliver App-V applications.
- **Layered app (Citrix App Layering):** Each layer contains a single application, agent, or operating system. By integrating one OS layer, one platform layer (VDA, Citrix Provisioning agent) 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. For details, 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 executing 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 executes on the endpoint. For details, see Local App Access and URL redirection.

For desktops, consider published desktops or VDI desktops.

Citrix Virtual Apps™ published apps and desktops

Use multi-session OS machines to deliver Citrix Virtual Apps and Desktops published apps and published desktops.

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. This provides a user experience that is consistent, safe, and reliable.
- Users must be online to access their applications.

User experience:

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

- User requests one or more applications from StoreFront™, their **Start** menu, or a URL you provide.
- 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:

- 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 same machine, that single machine is now using 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.

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

- 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 master image are securely managed, hosted, and run on machines within your data center, providing a more cost-effective application delivery solution.
- On 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.
- 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' data.

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, a single user can use multiple applications (and is not limited to a single application) because the operating system sees each application as a new session.
- Within a delivery group, when users log on they 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 Apps and Desktops VDI desktops.

VDI desktops are hosted on virtual machines and provide each user with a desktop operating system.

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

VDI desktops require more resources than 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 master image. All changes to the desktop are lost when the machine restarts.
- **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 master image.) After the first use, each time a user logs on to use a desktop, 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 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 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.

For more information, Remote PC Access.

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

Network ports

September 6, 2025

Complete network port information is provided in Communication Ports Used by Citrix Technologies.

When Citrix® components are installed, the operating system's host firewall is also updated, by default, to match the default network ports.

You might need port information:

- For regulatory compliance.
- If there is a network firewall between the Citrix Virtual Apps and Desktops™ components and other Citrix products or components, so you can configure that firewall appropriately.
- If you use a third-party host firewall, such as one provided with an anti-malware package, rather than the operating system's host firewall.
- If you alter the configuration of the host firewall on these components (usually Windows Firewall Service).
- If you reconfigure component features to use a different port or port range, and then want to disable or block ports that aren't used in your configuration.

Some of the ports are registered with the Internet Assigned Numbers Authority (IANA). Details about these assignments are available at http://www.iana.org/assignments/port-numbers. However, the descriptive information held by IANA does not always reflect today's usage.

Also, the operating systems on the VDA and Delivery Controller™ require incoming ports for their own use. See the Microsoft Windows documentation for details.

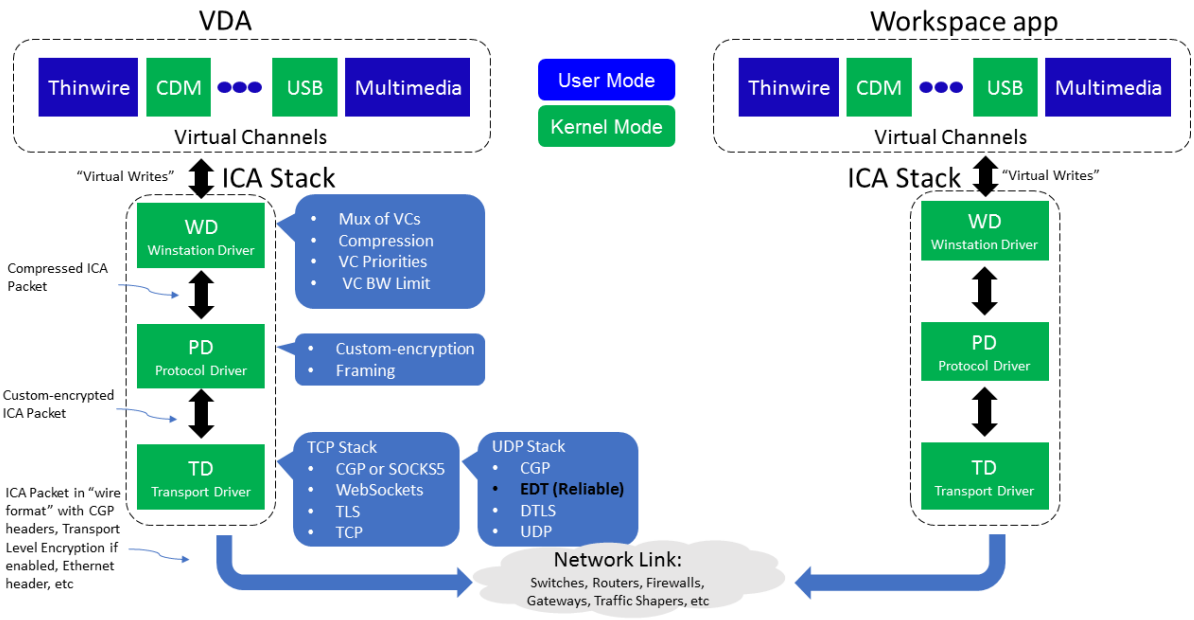
HDX™

September 6, 2025

> **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.

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



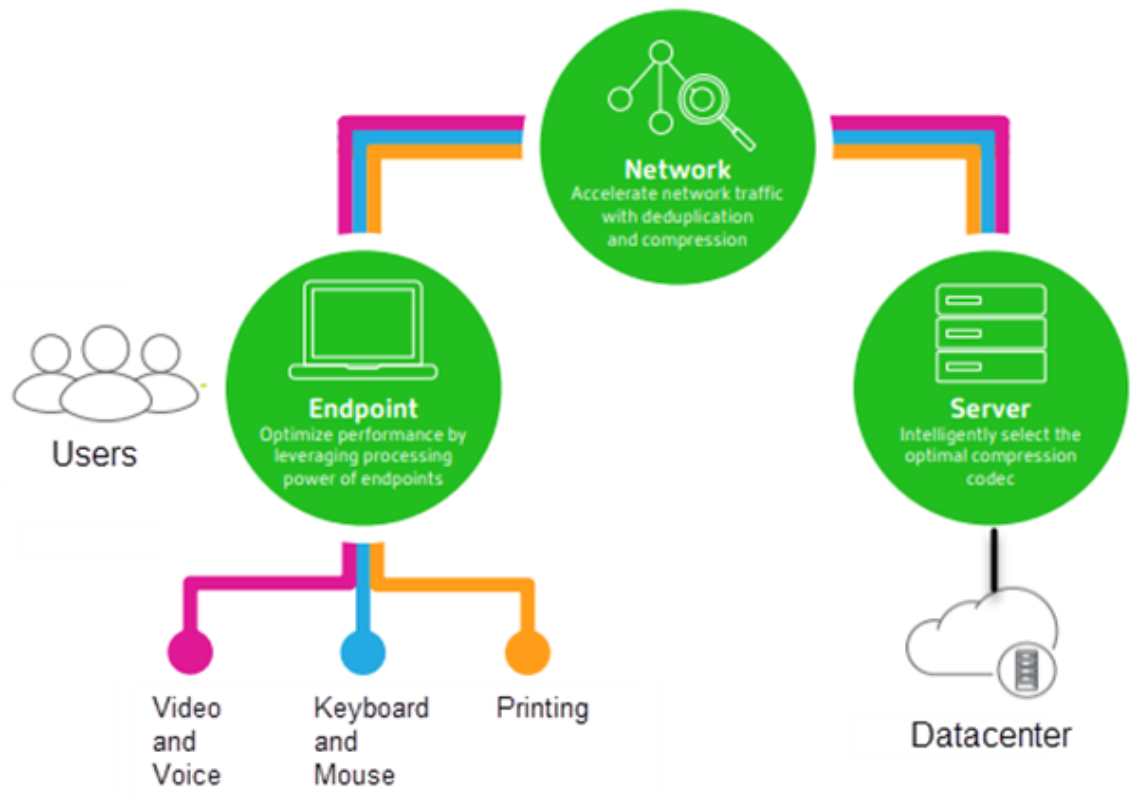
HDX is designed around three technical principles:

- 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.

- **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.

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



- **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.

For more information, see Boost productivity with a high-definition user workspace.

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. Workspace control enables users to pause virtual desktops and applications and resume working from a different device at the point where they left off.

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

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.

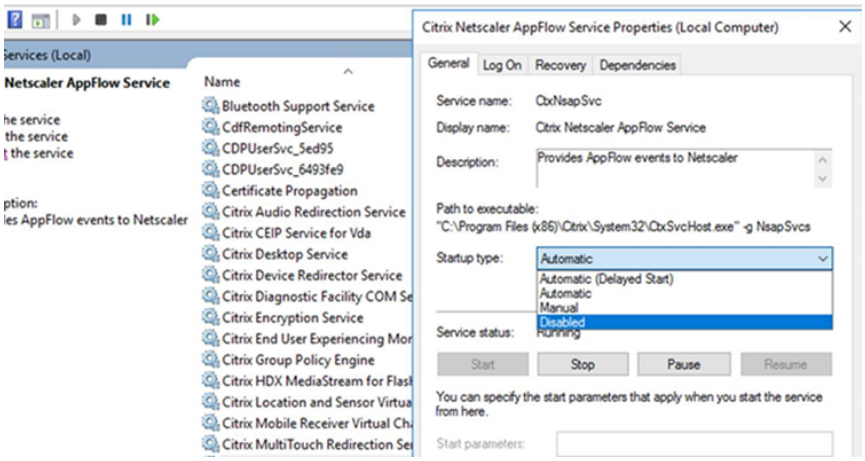
Minimum requirements:

- 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).

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



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:

  1. Download the Chrome browser extension and install it on the virtual desktop.
  2. 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. 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:

  1. Configure your Citrix client for maximum audio quality; see the Citrix Workspace app documentation for details.
  2. 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

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

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.

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 an application and desktops network interruption notification to the user as follows:

- **Desktops.** The session window is grayed out and a countdown timer displays 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. The user cannot interact with sessions while an 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.

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

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:

- **Desktops.** The session window becomes translucent and a countdown timer displays 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 a 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.

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

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.

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.

> **Note:**
>
> The **Display Memory Limit** setting has been deprecated. With this change, Citrix now no longer limits the display memory. Instead, the minimum amount of memory required is allocated to ensure the client's display layout is fully accommodated.

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

Improve video conference performance

Several popular video conferencing applications are optimized for delivery from Citrix Virtual Apps and Desktops 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 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

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, Windows 8, and Windows 7 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 NetScaler SD-WAN 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 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
2. Create a DWORD value key, SeamlessFlags, and set it to 0x40000.

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

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 the 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

Type: DWORD

Value: 1

To use normal Unicode keyboard layout mapping, set **DisableWindowHook** to 0.

Citrix ICA® virtual channels

September 13, 2025

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

> **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.

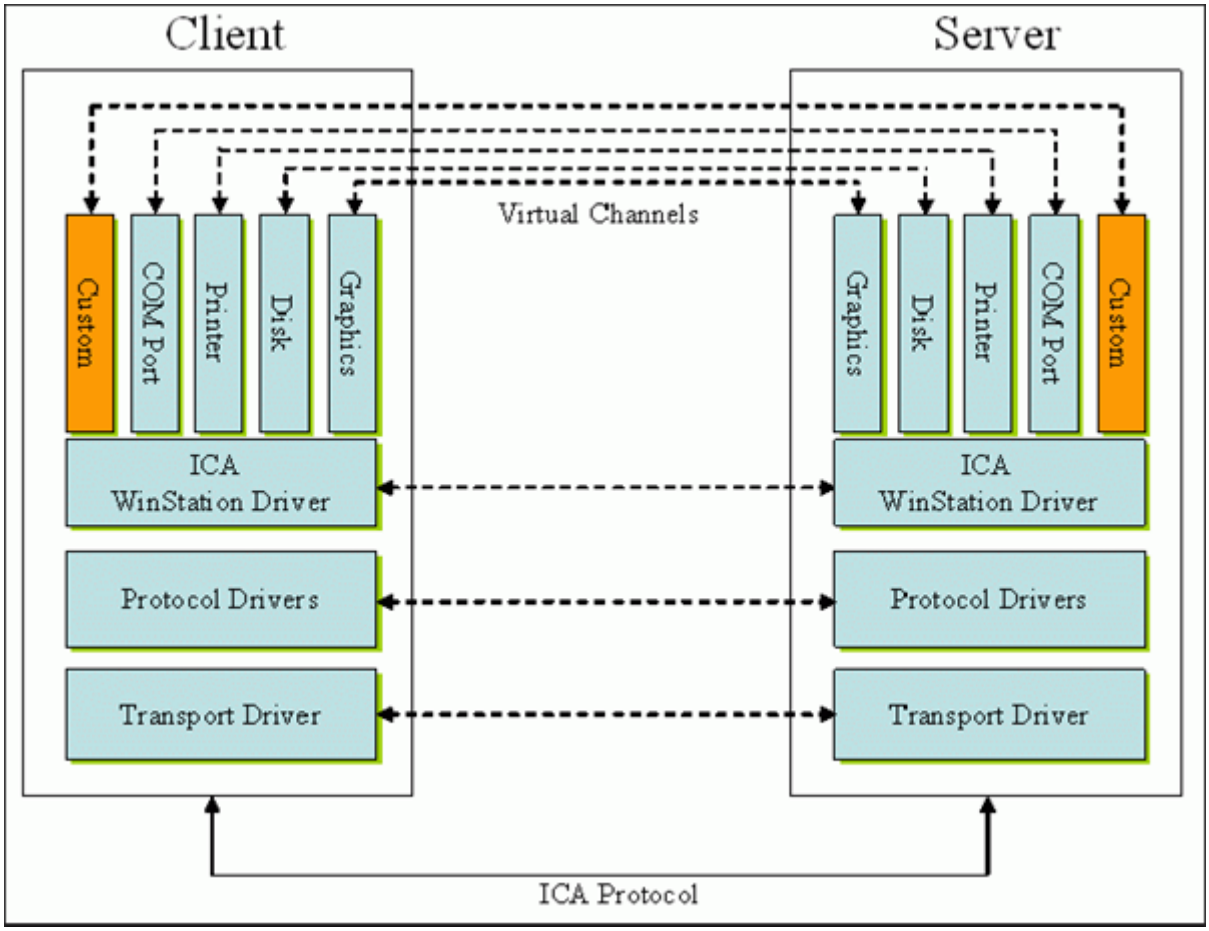
What are ICA virtual channels?

A large portion of the functionality and communication between the Citrix Workspace™ app and the Citrix Virtual Apps and Desktops™ servers occurs over virtual channels. Virtual channels are a necessary part of the remote computing experience with the Citrix Virtual Apps and Desktops 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 new versions of the Citrix Virtual Apps and Desktops servers 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 Virtual Apps and Desktops ship 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 the 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
- 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

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

- 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
- 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 the virtual channel driver vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

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

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

Graphics virtual channel on the server side

The `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 Virtual Apps and Desktops 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:

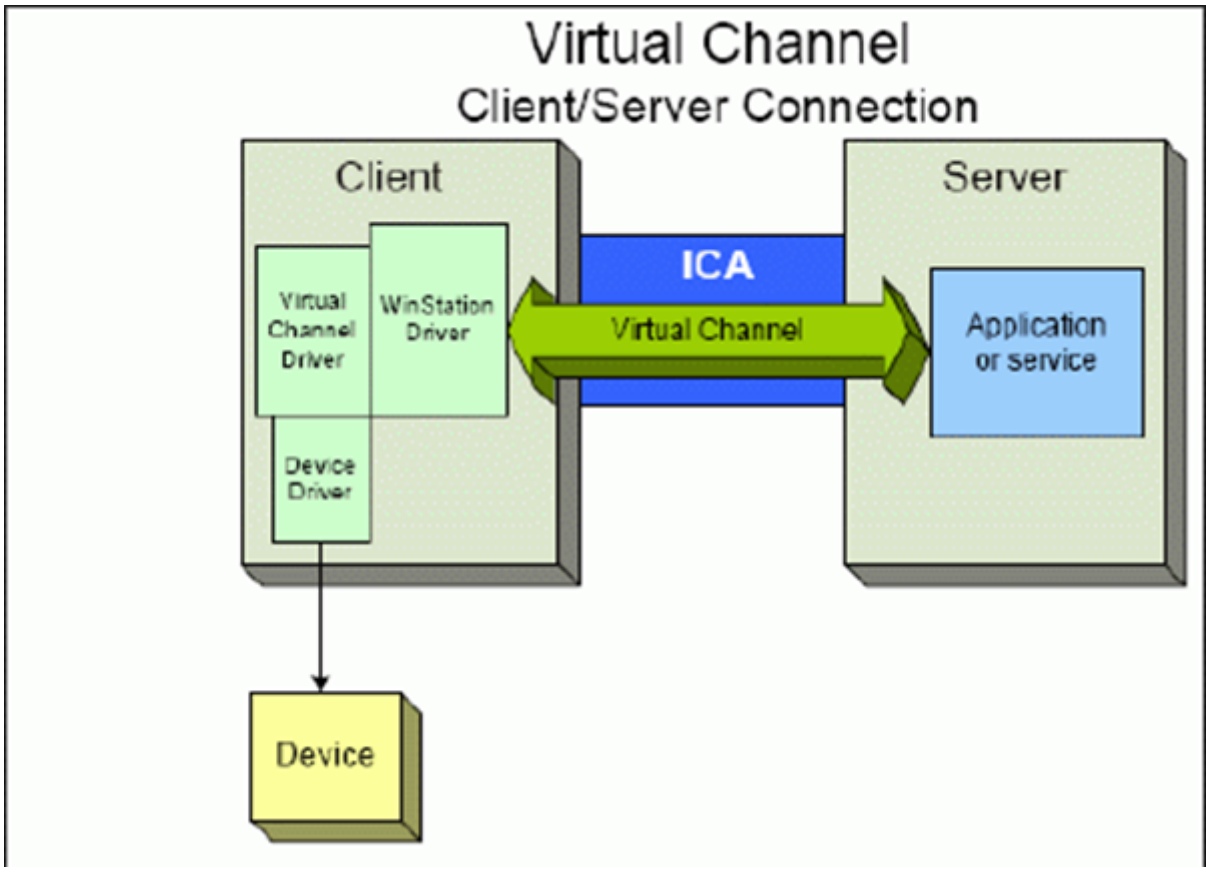
- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service

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

- 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.



This overview contains a client-server data exchange using a virtual channel.

1. The client connects to the Citrix Virtual Apps and Desktops 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.

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

- 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.

Creating your own virtual channel using the Virtual Channel SDK

> **Note:**
>
> Citrix SDKs are available in the Citrix Developer portal at https://developer.cloud.com.

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 Virtual Apps and Desktops, 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.

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).

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

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

- 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.

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

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

Virtual Channel	Is double hop supported?
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
USB VC	Yes
WAYCOM devices -K2M using USB VC	Yes
Webcam Video Compression	Yes
Windows Media Redirection	Yes

See also

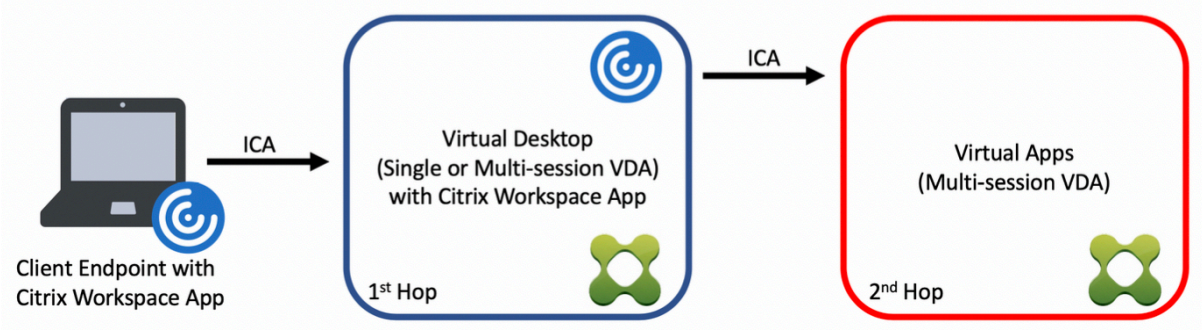
- ICA Virtual Channel SDK
- The Citrix Developer Network is the home for all technical resources and discussions involving the use of Citrix SDKs. In this network, you can find access to SDKs, sample code and scripts, extensions and plug-ins, and SDK documentation. Also included are the Citrix Developer Network forums, where technical discussions take place around each of the Citrix SDKs.

Double hop in Citrix Virtual Apps and Desktops™

September 6, 2025

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

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 Virtual Apps and Desktops editions including the Citrix Cloud™ service 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 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

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

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.

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.

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

First hop (VDI or published desktop)	Second hop (Virtual apps)	Support notes
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

Install and configure

September 13, 2025

Review the referenced articles before starting each deployment step, to learn about what you see and specify during the deployment.

Use the following sequence to deploy Citrix Virtual Apps and Desktops.

Prepare

Review Prepare to install and complete any necessary tasks.

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

- Where to find information about concepts, features, differences from earlier releases, system requirements, and databases.
- Considerations when deciding where to install core components.
- Permission and Active Directory requirements.
- Information about the available installers, tools, and interfaces.

Install core components

Install the Delivery Controller, Web Studio, Citrix Director, and Citrix License Server. You can also install Citrix StoreFront. For details, see Install core components or Install using the command line.

Create a site

After you install the core components and launch Studio, you are prompted to create a site.

Install one or more Virtual Delivery Agents (VDAs)

Install a VDA on a machine running a Windows operating system, either on a master image or directly on each machine. See Install VDAs or Install using the command line. Sample scripts are provided if you want to install VDAs through Active Directory.

For machines with a Linux operating system, follow the guidance in Linux Virtual Delivery Agent.

For a Remote PC Access deployment, install a VDA for a single-session OS on each office PC. If you need only the core VDA services, use the standalone `VDAWorkstationCoreSetup.exe` installer and your existing Electronic Software Distribution (ESD) methods. (Prepare to install describes the available VDA installers.)

Install optional components

If you plan to use the Citrix Universal Print Server, install its server component on your print servers. See Install core components or Install using the command line.

To allow StoreFront to use authentication options such as SAML assertions, install the Citrix Federated Authentication Service.

To enable end users to have greater control over their user accounts, install Self-Service Password Reset.

Optionally, integrate more Citrix components into your Citrix Virtual Apps and Desktops deployment.

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

- Citrix Provisioning is an optional component that provisions machines by streaming a master image to target devices.
- Citrix Gateway is a secure application access solution that provides administrators with granular application-level policy and action controls to secure access to applications and data.
- Citrix SD-WAN is a set of appliances that optimize WAN performance.

Create a machine catalog

After you create a site in Studio, you are guided to create a machine catalog.

A catalog can contain physical or virtual machines (VMs). Virtual machines can be created from a master image. When using a hypervisor or other service to provide VMs, you first create a master image on that host. Then, when you create the catalog, you specify that image, which is used when creating VMs.

Create a delivery group

After you create your first machine catalog in Web Studio, you are guided to create a delivery group.

A delivery group specifies which users can access machines in a selected catalog and the applications available to those users.

Create an application group (optional)

After you create a delivery group, you can optionally create an application group. You can create application groups for applications that are shared across different delivery groups or used by a subset of users within delivery groups.

Known limitation

When you use Citrix Workspace™ app for Windows version 1912 or earlier, the session drops after a while. This issue is fixed in the newer LTSR and CR versions of Citrix Workspace app.
For more information on the supported release versions, see Citrix Workspace app for Windows / Citrix Receiver for Windows Long Term Service Releases.

Machine identities

September 6, 2025

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

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. Citrix® supports hosting virtual applications and desktops on machines that are Active Directory joined, Hybrid Azure Active Directory 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.
Hybrid Azure AD joined	Identities are created in on-premises Active Directory and are synced with Azure AD through Azure AD Connect. Provisioned machines are joined to on-premises Active Directory. The machines are then Hybrid Azure AD joined. For importing a Hybrid Azure AD joined VM, the VM is treated as an Active Directory joined VM by Citrix Virtual Apps and Desktops.
Non-domain-joined	Identities are created and managed in the machines locally. Importing VMs to Citrix Virtual Apps and Desktops is not supported.

Supported Configurations

The following are details of the supported configurations for each scenario.

Supported infrastructure

Machine identity	Citrix Virtual Apps and Desktops™	Citrix Workspace™	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
AD joined	Yes	Yes	Yes	Yes	Yes

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

Machine identity	Citrix Virtual Apps and Desktops™	Citrix Workspace™	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
Azure Active Directory joined	No	Yes	No	Yes	No
Hybrid Azure AD joined	Yes	Yes	Yes	Yes	Yes
Non-domain-joined	Yes	Yes	No	Yes	No

Supported workspace authentication identity providers

Machine identity	Azure Active Directory	Active Directory	Active Directory and Token	Okta	SAML	Citrix Gateway	Adaptive Authentication
AD joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hybrid Azure AD joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non-domain-joined	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Active Directory joined

September 6, 2025

Active Directory is required for authentication and authorization. The Kerberos infrastructure in Active Directory is used to guarantee the authenticity and confidentiality of communications with the Delivery Controllers. For information about Kerberos, see the Microsoft documentation.

The System requirements article lists the supported functional levels for the forest and domain. To use Policy Modeling, the domain controller must be running on all supported Server OSs. This does not affect the domain functional level.

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

This product supports:

- **Deployments in which the user accounts and computer accounts exist in domains in a single Active Directory forest.** User and computer accounts can exist in arbitrary domains within a single forest. All domain functional levels and forest functional levels are supported in this type of deployment.
- **Deployments in which user accounts exist in an Active Directory forest that is different from the Active Directory forest containing the computer accounts of the Controllers and virtual desktops.** In this type of deployment, the domains containing the Controller and virtual desktop computer accounts must trust the domains containing user accounts. Forest trusts or external trusts can be used. All domain functional levels and forest functional levels are supported in this type of deployment.
- **Deployments in which the computer accounts for Controllers exist in an Active Directory forest that is different from one or more additional Active Directory forests that contain the computer accounts of the virtual desktops.** In this type of deployment a bi-directional trust must exist between the domains containing the Controller computer accounts and all domains containing the virtual desktop computer accounts. In this type of deployment, all domains containing Controller or virtual desktop computer accounts must be at "Windows 2000 native"functional level or higher. All forest functional levels are supported.
- **Writable domain controllers.** Read-only domain controllers are not supported.

Optionally, Virtual Delivery Agents (VDAs) can use information published in Active Directory to determine which Controllers they can register with (discovery). This method is supported primarily for backward compatibility, and is available only if the VDAs are in the same Active Directory forest as the Controllers. For information about this discovery method see Active Directory OU-based discovery and CTX118976.

> **Note:**
>
> Do not change the computer name or the domain membership of a Delivery Controller™ after the site is configured.

Deploy in a multiple Active Directory forest environment

In an Active Directory environment with multiple forests, if one-way or two-way trusts are in place you can use DNS forwarders or conditional forwarders for name lookup and registration. To allow the appropriate Active Directory users to create computer accounts, use the Delegation of Control wizard. See the Microsoft documentation for details about this wizard.

No reverse DNS zones are necessary in the DNS infrastructure if appropriate DNS forwarders are in place between forests.

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

The SupportMultipleForest key is necessary if the VDA and Controller are in separate forests, regardless of whether the Active Directory and NetBIOS names are different. Use the following information to add the registry key to the VDA and the Delivery Controllers:

> **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. Back up the registry before you edit it.

On the VDA, configure: HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest.

- Name: SupportMultipleForest
- Type: REG_DWORD
- Data: 0x00000001 (1)

On all Delivery Controllers, configure: HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest.

- Name: SupportMultipleForest
- Type: REG_DWORD
- Data: 0x00000001 (1)

You might need reverse DNS configuration if your DNS namespace is different than that of Active Directory.

A registry entry has been added to avoid unwanted enabling of NTLM authentication in VDAs, which is less secure than Kerberos. This entry can be used instead of the SupportMultipleForest entry, which can still be used for backwards compatibility.

On the VDA, configure: HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent
.

- Name: SupportMultipleForestDdcLookup
- Type: REG_DWORD
- Data: 0x00000001 (1)

This registry key performs a DDC lookup in a two-way trust multiple forest environment that allows you to remove NTLM-based authentication during the initial registration process.

If external trusts are in place during setup, the ListOfSIDs registry key is required. The ListOfSIDs registry key is also necessary if the Active Directory FQDN is different than the DNS FQDN, or if the domain containing the Domain Controller has a different NetBIOS name than the Active Directory FQDN. To add the registry key, use the following information:

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

For the VDA, locate the registry key `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`.

- Name: `ListOfSIDs`
- Type: `REG_SZ`
- Data: Security Identifier (SID) of the Controllers. (SIDs are included in the results of the `Get-BrokerController` cmdlet.)

When external trusts are in place, make the following change on the VDA:

1. Locate the file `Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`.
2. Make a backup copy of the file.
3. Open the file in a text editing program such as Notepad.
4. Locate the text `allowNtlm="false"` and change the text to `allowNtlm="true"`.
5. Save the file.

After adding the `ListOfSIDs` registry key and editing the `brokeragent.exe.config` file, restart the Citrix Desktop Service to apply the changes.

The following table lists the supported trust types:

Trust type	Transitivity	Direction	Supported in this release
Parent and child	Transitive	Two-way	Yes
Tree-root	Transitive	Two-way	Yes
External	Nontransitive	One-way or two-way	Yes
Forest	Transitive	One-way or two-way	Yes
Shortcut	Transitive	One-way or two-way	Yes
Realm	Transitive or nontransitive	One-way or two-way	No

For more information about complex Active Directory environments, see CTX134971.

Where to go next

For information on how to create identity pool of on-premises Active Directory (AD) joined machine identity, see Identity pool of on-premises Active Directory joined machine identity.

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

Microsoft Entra hybrid joined

April 2, 2026

This article describes the requirements to create identity pool of Microsoft Entra hybrid joined catalogs and Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune in addition to the requirements outlined in the system requirements section.

Microsoft Entra hybrid 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 Microsoft Entra ID seamless SSO experience, you need to have the domain users synced to Microsoft Entra ID.

> **Note:**
>
> Microsoft Entra hybrid joined VMs are supported in both federated and managed identity infrastructures.

Requirements for Microsoft Entra hybrid joined

- VDA type: Single-session (desktops only) or multi-session (apps and desktops)
- 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 for Microsoft Entra hybrid joined

- 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.

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

Considerations for Microsoft Entra hybrid joined

- 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 Microsoft Entra hybrid 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.

  1. Run `gpedit.msc`.
  2. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Device Registration**.
  3. 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.

```
$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
```

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

```
            dsregcmd /join
            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.

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

- VDA type: Single-session or multi-session
- VDA version: 2407 or later
- Provisioning type: Machine Creation Service (MCS), Persistent. Hybrid Azure AD joined catalogs enrolled in Microsoft Intune for non-persistent single and multi-session VMs is currently under Preview. See Enrollment of Hybrid Entra ID joined non-persistent VMs into Microsoft Intune.
- 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.

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

- 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.

  For non-persistent machines, consider limiting the concurrent power actions in either Autoscale™ or manual power actions.

- 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:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MachineIdentityServiceAgent\
     DeviceManagement
  ```

  Value name: `MdmSccmSiteCode`

  Value type: **String**

  Value data: `the site code to be assigned`

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

Where to go next

For more information on creating identity pool of Microsoft Entra hybrid joined catalogs, see Identity pool of Microsoft Entra hybrid joined machine identity.

Non-domain-joined

September 6, 2025

This article describes the requirements to create non-domain-joined catalogs using using Citrix Virtual Apps and Desktops in addition to the requirements outlined in the System Requirements section.

Requirements

- Control plane: See Supported Configurations
- VDA type: Single-session (desktops only) or multi-session (apps and desktops)
- VDA version: 2311 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

Limitations

- Service continuity is not supported.
- Whenever we use a multi session non domain joined VDA, the local user's profile data is not retained and is deleted on logoff.

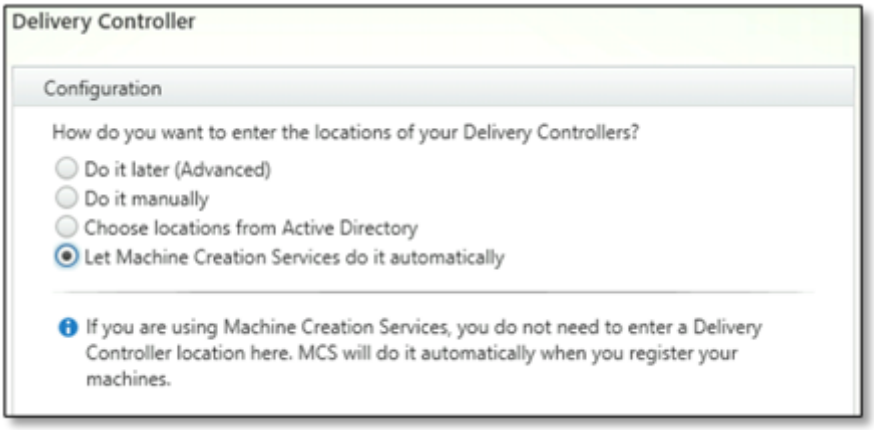
VDA installation and configuration

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**.

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

- In the Delivery Controller™ page, select **Let Machine Creation Services do it automatically**.



Where to go next

Once the resource location and hosting connection are available, proceed to create the identity pool. For more information on creating identity pool of non-domain-joined machine identity, see Identity pool of non-domain-joined machine identity.

Prepare to install

August 19, 2026

Deploying Citrix Virtual Apps and Desktops™ begins with installing the following components. This process prepares for the delivery of applications and desktops to users inside your firewall.

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

- One or more Delivery Controllers
- Citrix Director
- Citrix StoreFront™
- Citrix License Server
- One or more Citrix Virtual Delivery Agents (VDAs)
- Optional components and technologies such as the Universal Print Server, the Federated Authentication Service, and Self-Service Password Reset

For users outside your firewall, install and configure an extra component, such as Citrix Gateway. For an introduction, see Integrate Citrix Virtual Apps and Desktops with Citrix Gateway.

> **Note:**
>
> Make sure that the following Microsoft prerequisites are met on the server OS and the workstation OS:
>
> - Microsoft **Volume Shadow Copy** and **Microsoft Software Shadow Copy Provider** services are running. For more information, see Volume Shadow Copy Service.
> - The **MS-Defender** version must be higher than 4.18.2105.5. For more information, see Microsoft Defender Antivirus security intelligence and product updates.

If your deployment includes Windows Server workloads, configure a Microsoft RDS License Server.

You can use the full-product installer on the product ISO to deploy many components and technologies. You can use a standalone VDA installer to install VDAs. The standalone VDA installers are available on the Citrix download site. All installers offer graphical and command line interfaces. See Installers.

The product ISO contains sample scripts that install, upgrade, or remove VDAs for machines in an Active Directory. You can also use the scripts to manage images used by Machine Creation Services (MCS) and Citrix Provisioning (formerly Provisioning Services). For details, see Install VDAs using scripts.

Information to review before installation

- Technical overview: To familiarize yourself with the product and its components.
- Security: When planning your deployment environment.
- Known issues: Issues you might come across in this version.
- Databases: Learn about the system databases and how to configure them. During Controller installation, you can install SQL Server Express for use as the site database. You configure most database information when you create a site, after you install the core components.
- Remote PC Access: If you're deploying an environment that enables your users to access their physical machines in the office remotely.

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

- Connections and resources: If you're using a hypervisor or other service to host or provision VMs for applications and desktops. You can configure the first connection when you create a site (after you install the core components). Set up your virtualization environment before then.
- Microsoft System Center Configuration Manager: If you're using ConfigMgr to manage access to applications and desktops, or if you're using the Wake on LAN feature with Remote PC Access.
- **Public Cloud host connections:** If you have a Hybrid Rights License, you can create host connections to the public cloud. For information related to the Hybrid Rights License, see Hybrid Rights Renewals. For information related to public cloud entitlement and the reasons for this change, see CTX270373.

Where to install components

Review the System requirements for supported platforms, operating systems, and versions. Component prerequisites are installed automatically, except as noted. See the Citrix StoreFront and the Citrix License Server documentation for their supported platforms and prerequisites.

You can install the core components on the same server or on different servers.

- Installing all the core components on one server can work for evaluation, test, or small production deployments.
- To accommodate future expansion, consider installing components on different servers. For example, installing Studio on a different machine than the server where you installed the Controller allows you to manage the site remotely.
- For most production deployments, installing core components on separate servers is recommended.

  Install the Citrix License Server and licenses before installing other components on other servers.
- To install a supported component on a Server CoreOS (such as a Delivery Controller), you must use the command line. That OS type does not offer a graphical interface, so install Studio and other tools elsewhere, and then point them to the Controller server.

You can install both a Delivery Controller™ and a VDA for multi-session OS on the same server. Launch the installer and select the Delivery Controller (plus any other core components you want on that machine). Then launch the installer again and select the **Virtual Delivery Agent** for multi-session OS.

Make sure that each operating system has the latest updates.

Make sure that all machines have synchronized system clocks. The Kerberos infrastructure that secures communication between the machines requires synchronization.

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

With XenServers, the virtual machine's power state might appear as unknown even if it appears registered. To resolve this issue, edit the registry key `HostTime` value to disable time synchronization with the host:

`HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"`

`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"`

> **Tip:**
>
> The default value is `HostTime="UTC"`. Change this value to something other than UTC, for example, `Local`. This change effectively disables time synchronization with the host.

Optimization guidance for Windows 10 single-session machines is available in CTX216252.

Where NOT to install components:

- Do not install any components on an Active Directory domain controller.
- Installing a Controller on a node in a SQL Server clustering installation, SQL Server mirroring installation, or on a server running Hyper-V is not supported.

If you try to install or upgrade a VDA on a Windows OS that this product version doesn't support, a message guides you to an article describing options.

Permission and Active Directory requirements

You must be a domain user and a local administrator on the machines where you are installing components.

To use a standalone VDA installer, you must have elevated administrative privileges or use **Run as administrator**.

Configure your Active Directory domain before starting an installation.

- System requirements lists the supported Active Directory functional levels. Active Directory joined contains more information.
- You must have at least one domain controller running Active Directory Domain Services.
- Do not install any Citrix Virtual Apps and Desktops components on a domain controller.
- Do not use a forward slash (/) when specifying Organizational Unit names in Studio.

The Windows user account used to install the Citrix License Server is automatically configured as a delegated administration full administrator.

For more information:

- Security best practices

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

- Delegated administration
- Microsoft documentation for Active Directory configuration

Installation guidance, considerations, and best practice

During installation of any component

- When installing or upgrading a Delivery Controller, Studio, License Server, or Director from the full-product media, if the Citrix installer detects that a restart is pending from a previous Windows installation on the machine, the installer stops with exit/return code 9. You are prompted to restart the machine.

  This is not a Citrix forced restart. It is due to other components installed earlier on the machine. If this occurs, restart the machine and then launch the Citrix installer again.

  When using the command-line interface, you can prevent the check for the pending restart by including the `/no_pending_reboot_check` option in the command.

- Usually, if a component has prerequisites, the installer deploys them if they are not present. Some prerequisites might require a machine restart.
- When you create objects before, during, and after installation, specify unique names for each object. For example, provide unique names for networks, groups, catalogs, and resources.
- If a component does not install successfully, the installation stops with an error message. Components that installed successfully are retained. You do not need to reinstall them.
- Citrix 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.

  During installation, you can also choose to participate in other Citrix technologies that collect diagnostics for maintenance and troubleshooting. For information about these programs, see Citrix Insight Services.

- Google Analytics are collected (and later uploaded) automatically when you install (or upgrade) Studio. After installing Studio, you can change this setting with the registry key `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. A value of **1** enables collection and upload, **0** disables collection and upload.
- 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's 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.

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

During VDA installation

- The Citrix Workspace™ app for Windows is available, but not installed by default when you install a VDA. You or your users can download and install (and upgrade) Citrix Workspace app for Windows and other Citrix Workspace apps from the Citrix website. Alternatively, you can make those Citrix Workspace apps available from your StoreFront server. See the StoreFront documentation.
- The Microsoft Print Spooler Service must be enabled. You cannot successfully install a VDA if that service is disabled.
- Windows Protected Print (WPP) mode must be disabled. You cannot successfully install a VDA if WPP mode is enabled.
- Most supported Windows editions come with Microsoft Media Foundation already installed. If the machine does not have Media Foundation (such as N editions), several multimedia features are not installed and will not work.

  - 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.
- When you install the VDA, a new local user group called **Direct Access Users** is created automatically. On a VDA for single-session OS, this group applies only to RDP connections. On a VDA for multi-session OS, this group applies to ICA® and RDP connections.
- The VDA must have valid Controller addresses with which to communicate. Otherwise, sessions cannot be established. You can specify Controller addresses when you install the VDA or later. Remember that it must be done. For more information, see VDA registration.

Restarts after and during VDA installation

A restart is required at the end of the VDA installation. That restart occurs automatically by default.

When you're upgrading a VDA to version 7.17 (or a later supported version), a restart occurs during the upgrade. This cannot be avoided.

To minimize the number of restarts needed during VDA installation:

- Ensure that a supported .NET Framework version is installed before beginning the VDA installation.

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

- 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.

When you're upgrading a VDA version, a restart occurs during the upgrade. This cannot be avoided.

Restore on install or upgrade failure

> **Note:**
>
> This feature is available for single-session and multi-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.

If a multi-session VDA installation or upgrade fails, and the "restore on failure"feature is enabled, the machine is returned to a backup that was performed before the installation or upgrade began.

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.

When a multi-session VDA installation or upgrade starts with this feature enabled, the installer creates a server backup before beginning the actual install or upgrade. If the VDA installation or upgrade fails, the machine is returned to the backup state. The `%temp%/Citrix` folder contains deployment logs and other information about the restore. The amount of time to create the server backup is based on the size of the backup needed and the amount of resources available to the server. The backup is stored in *C:\WindowsImageBackup\servername*.

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`).

> **Note:**
>
> This GPO setting does not apply to restoring a multi-session VDA.

To enable this feature when installing or upgrading a single or multi-session VDA:

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

- 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/backup is not used, but is retained.

- Run a VDA installer with either the `/enablerestore` or `/enablerestorecleanup` option using the command line.

  - If you use the `/enablerestorecleanup` option, and the install/upgrade completes successfully, the restore point/server backup is removed automatically.
  - If you use the `/enablerestore` option, and the install/upgrade completes successfully, the restore point is not used, but is retained.

Installers

Full-product installer

Using the full-product installer provided in the ISO, you can:

- Install, upgrade, or remove core components: Delivery Controller, Studio, Director, and License Server.
- Install or upgrade StoreFront.
- Install or upgrade Windows VDAs for single-session or multi-session operating systems.
- Install the Universal Print Server `UpsServer` component on your print servers.
- Install the Federated Authentication Service.
- Install Session Recording.
- Install Workspace Environment Management.

> **Note:**
>
> The Workspace Environment Management™ Agent installer is not localized. It is available only in English.

To deliver a desktop from a multi-session OS for one user (for example, for web development), use the full-product installer's command-line interface. For details, see Server VDI.

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

Standalone VDA installers

Standalone VDA installers are available on the Citrix download pages. (They are not available from the product installation media.) The standalone VDA installers are much smaller than the full-product ISO. They more easily accommodate deployments that:

- Use Electronic Software Distribution (ESD) packages that are staged or copied locally
- Have physical machines
- Have remote offices

By default, files in the self-extracting standalone VDAs are extracted to the **Temp** folder. More disk space is required on the machine when extracting to the **Temp** folder than when using the full-product installer. However, files extracted to the **Temp** folder are automatically deleted after the installation completes. Alternatively, you can use the `/extract` command with an absolute path.

Four standalone VDA installers are available for download.

Multi-session OS Virtual Delivery Agent (VDAServerSetup.exe):

Installs a VDA for multi-session OS. It supports all the VDA for multi-session OS options that are available with the full-product installer.

Single-session OS Virtual Delivery Agent (VDAWorkstationSetup.exe):

Installs a VDA for single-session OS. It supports all the VDA for single-session OS options that are available with the full-product installer.

Single-session OS Core Services Virtual Delivery Agent (VDAWorkstationCoreSetup.exe):

Installs a VDA for single-session OS 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. It installs only the core services necessary for VDA connections such deployments. Therefore, it supports only a subset of the options that are valid with the full-product or `VDAWorkstationSetup.exe` installers.

This installer does not install or contain the components used for:

- App-V.
- Profile Management. Excluding Citrix Profile Management from the installation affects Citrix Director displays. For details, see Install VDAs.
- Machine Identity Service.
- Citrix MCS IODriver
- Citrix Backup and Restore
- deviceTRUST
- uberAgent
- WEM

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

The `VDAWorkstationCoreSetup.exe` installer does not install or contain the following components: Citrix Workspace app for Windows (CWA), Citrix Secure Access Client (CSA), and Citrix User Personalization Layer (UPL).

Using `VDAWorkstationCoreSetup.exe` is equivalent to using the full-product or `VDAWorkstationSetup` installer to install a single-session OS VDA and either:

- In the graphical interface: Selecting the Remote PC Access option on the **Environment** page.
- In the command line interface: Specifying the `/remotepc` option.
- In the command line interface: Specifying `/components vda` plus the `/exclude` option that lists all of the valid additional component names.

You can install the omitted components/features later by running the full-product installer. That action enables you to install all missing components.

The `VDAWorkstationCoreSetup.exe` installer automatically installs the Browser Content Redirection MSI. This automatic installation applies to VDA release 2003 and later supported releases.

Single-session Core Services Virtual Delivery Agent (VDASingleSessionCoreSetup.exe):

Starting with release 2507 CU1, a new lightweight Single-Session VDA Meta Installer available for Windows 365 Cloud PC and Remote PC deployments. This installer is built on the existing VDAWorkstationCoreSetup.exe installer, delivering essential VDA components along with Profile Management, deviceTRUST, uberAgent, WEM, Backup and Restore, and the VDA Upgrade Agent. Backup and Restore functionality can be enabled using the command line option /enablerestore or /enablerestorecleanup.

It significantly reduces package size and improves installation reliability for cloud-based workloads. Designed for modern Remote PC scenarios, this installer provides a simplified and high-performance option for deploying Citrix workloads on Windows 365 and Remote PC.

Best practices for using single-session VDA installers

For single-session operating systems, four different installers are available. The full-product VDA installer and VDAWorkstationSetup.exe installer provide installation of all components, while some default and additional components are not included in VDAWorkstationCoreSetup.exe and VDASingleSessionCoreSetup.exe installers.

To maintain environment stability, consistent performance, and ongoing supportability, Citrix advises using a consistent installer type throughout the entire life cycle of a Citrix VDA—including installation, upgrade, and uninstallation. Mixing installer types can introduce certain risks.

Risks associated with mixing installer types:

Scenario 1: If a single-session VDA was initially installed using the VDAWorkstationCoreSetup.exe or VDASingleSessionCoreSetup.exe installer and subsequently upgraded with either the full-product

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

VDA installer or the VDAWorkstationSetup.exe installer, components that were previously excluded might be installed during the upgrade unless they are specifically excluded.

Scenario 2: If a single-session VDA is initially installed using the full-product VDA installer or VDAWorkstationSetup.exe and is later upgraded using VDAWorkstationCoreSetup.exe or VDASingleSessionCoreSetup.exe, any components not installed by the core services VDA installer are excluded from the upgrade. These components are neither upgraded during the upgrade process nor removed during uninstallation.

Scenario 3: If a single-session VDA is initially installed using the VDAWorkstationCoreSetup.exe installer, and subsequently upgraded with VDASingleSessionCoreSetup.exe, you'll experience the new features. If you upgrade with VDAWorkstationCoreSetup.exe next time, the newly added components by VDASingleSessionCoreSetup.exe will neither be upgraded in the upgrade process nor removed during uninstallation.

Guidance for addressing mixed installer types:

If it becomes necessary to mix installer types, it is essential to ensure that the same components are included during the upgrade process.

In cases where installer types have inadvertently been mixed, resulting in additional components being installed or certain components falling out of management, and there is a need to restore the previous environment, please proceed as follows:

- **For scenario 1:** Uninstall the VDA from the Windows feature for uninstalling or changing programs, then reinstall the VDA using the installer you originally used (VDAWorkstationCoreSetup.exe or VDASingleSessionCoreSetup.exe).
- **For scenario 2:** Upgrade the missing components utilizing the full-product VDA installer or the VDAWorkstationSetup.exe installer.
- **For scenario 3:** If you intend to continue leveraging new features, upgrade the missing components using the VDASingleSessionCoreSetup.exe installer. Alternatively, if you prefer not to use the new features after upgrading with VDASingleSessionCoreSetup.exe, first uninstall the VDA from the Windows feature for uninstalling or changing programs, then reinstall the VDA using VDAWorkstationCoreSetup.exe.

Citrix installation return codes

The installation log contains the result of component installations as a Citrix return code, not a Microsoft value.

- 0 = Success
- 1 = Failed
- 2 = PartialSuccess

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

- 3 = PartialSuccessAndRebootNeeded
- 4 = FailureAndRebootNeeded
- 5 = UserCanceled
- 6 = BadCommandLineArgument
- 7 = NewerVersionFound
- 8 = SuccessRebootNeeded
- 9 = FileLockReboot
- 10 = Aborted
- 11 = FailedMedia
- 12 = FailedLicense
- 13 = FailedPrecheck
- 14 = AbortedPendingRebootCheck
- 15 = PrecheckPass - This is returned when the pre-checks pass after using the new /precheckonly command line option.
- 16 = PrecheckFail - This is returned when the pre-checks fail after using the new /precheckonly command line option.
- 17 = OptionalSoftwareFailed - This is returned when one of the new Optional Software components fails to installed and the "Proceed with the VDA installation or upgrade if any other selected components fail."has been selected.

For example, when using tools such as Microsoft System Center Configuration Manager, a scripted VDA installation might appear to fail when the installation log contains the return code 3. This can occur when the VDA installer is waiting for a restart that you must initiate (for example, after an RDS role prerequisite installation on a server). A VDA installation is considered successful only after all prerequisites and selected components are installed, and the machine is restarted after the installation.

Alternatively, you can wrap your installation in CMD scripts (which return Microsoft exit codes) or change the success codes in your Configuration Manager package.

Configure a Microsoft RDS License Server for Windows Server workloads

This product accesses Windows Server remote session capabilities when delivering a Windows Server workload, such as Windows 2016. 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

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

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 Group Policy settings:

1. Install a Remote Desktop Services License Server on an available machine. The machine must always be available. The Citrix product workloads must be able to reach this license server.
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 Mode 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.

More information

For setting up resource location for specific host types:

- AWS cloud environments
- XenServer virtualization environments
- Google Cloud environments
- Microsoft Azure Resource Manager cloud environments
- Microsoft System Center Configuration Manager 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

AWS cloud environments

May 5, 2025

This article walks you through setting up your AWS account as a resource location you can use with Citrix Virtual Apps and Desktops. 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. After you complete these tasks, you can install VDAs, provision machines, create machine catalogs, and create Delivery Groups.

When you complete the tasks in this article, your resource location includes the following components:

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

- 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.
- An instance that acts as a bastion host 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.

Task overview

Set up a virtual private cloud (VPC) with public and private subnets. When you complete this task, AWS deploys a NAT gateway with an Elastic IP address in the public subnet. This action 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. With 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 and Domain Controller to the VPC. Through the bastion host, you can log on to instances in the private subnet to set up the domain and join instances to the domain.

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**.
5. Under DNS options, leave **Enable DNS hostnames** selected.

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

6. Select **Create VPC**. AWS creates the public and private subnets, Internet gateway, route tables, and default security group.

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
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:

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

Type	Destination
ALL Traffic	Select the Private security group.
ALL Traffic	0.0.0.0/0
ICMP	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 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
ALL Traffic	Select the Private security group.
ALL Traffic	Select the Public security group.
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.
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:

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

Type	Destination
ALL Traffic	Select the Private security group.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. When finished, select **Save**.

Task 3: Launch instances

Do the following steps to create two 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 you set up earlier.
5. In **Subnet**, make the following selections for each instance:
   - Bastion host: Select the Public subnet
   - Domain Controller: Select the Private subnet
6. In **Auto-assign Public IP address**, make the following selections for each instance:
   - Bastion host: Select **Enable.**
   - Domain Controller: Select **Use default setting** or **Disable**.
7. In **Network Interfaces**, enter a primary IP address within the IP range of your private subnet for the Domain Controller.
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: Select the Private security group.

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

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, 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 the steps from step 2 until you have created two instances:
    - One bastion host instance in your public subnet
    - One instance in your private subnet that is for use as a Domain Controller.

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.
    - 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**.

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

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 select **OK**:
      - Register this connection's addresses in DNS
      - Use this connection's DNS suffix in DNS registration
4. To configure the Domain Controller:
   a) Using Server Manager, add the Active Directory Domain Services role with all default features.
   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.

Where to go next

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection in AWS, see Connection to AWS

More information

- Create and manage connections and resources
- Create machine catalogs

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

Azure Local environments

August 18, 2025

Azure Local (based on Azure Arc) is a hyper-converged infrastructure (HCI) solution that connects the on-premises system to Azure for cloud-based services, monitoring, and management.

> **Note:**
>
> Azure Local for Citrix Virtual Apps and Desktops 2507 LTSR is only available for customers with Hybrid Rights/Universal License.

Prerequisites

- Azure Local cluster: 2503 or later
  - Storage path created
  - Logical network created with DHCP enabled
- To deploy an Azure Local cluster, refer to the Microsoft documentation About Azure Local deployment.

Key steps

Following are the key steps to create an MCS catalog in the Azure Local cluster:

1. Create a host connection.
2. Create a catalog by importing VMs created on Azure Local.

Where to go next

- For creating a connection to Azure Local, see Connection to Azure Local.

More information

- Create and manage connections and resources

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

XenServer® virtualization environments

September 6, 2025

XenServer simplifies your operational management, ensuring a high-definition user experience for intensive workloads.

To set up your XenServer, see Prepare to install.

Where to go next

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection in XenServer, see Connection to XenServer

More information

- Create and manage connections and resources
- Create machine catalogs

Google Cloud environments

September 13, 2025

Citrix Virtual Apps and Desktops™ lets you provision and manage machines on Google Cloud.

Requirements

- Citrix Cloud™ account. The feature described in this article is available only in Citrix Cloud.
- A Google Cloud project. The project stores all compute resources associated with the machine catalog. It can be an existing project or a new one.
- Enable four APIs in your Google Cloud project. For details, see Enable Google Cloud APIs.
- Google Cloud service account. The service account authenticates to Google Cloud to enable access to the project. For details, see Configure and update service accounts.
- Enable Google private access. For details, see Enable-private-google-access.

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

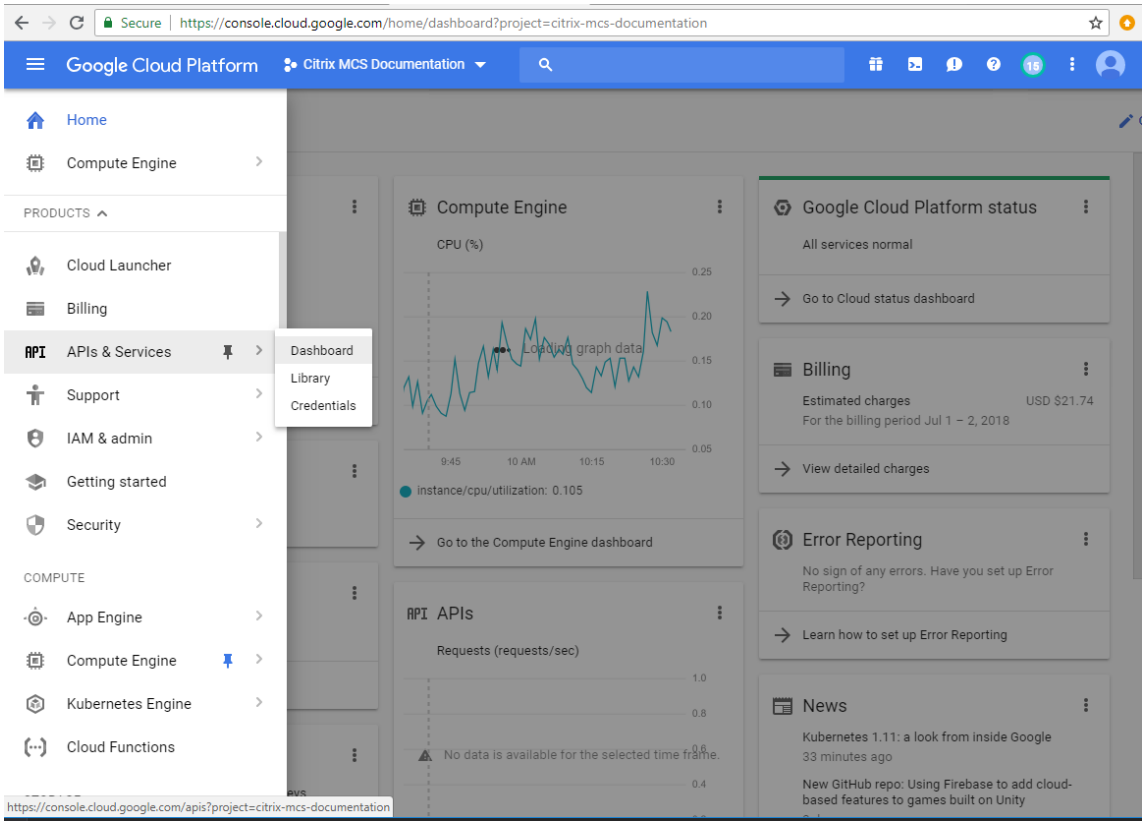
Enable Google Cloud APIs

To use the Google Cloud functionality through Web 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
- Cloud Key Management Service (KMS)

From the Google Cloud console, complete these steps:

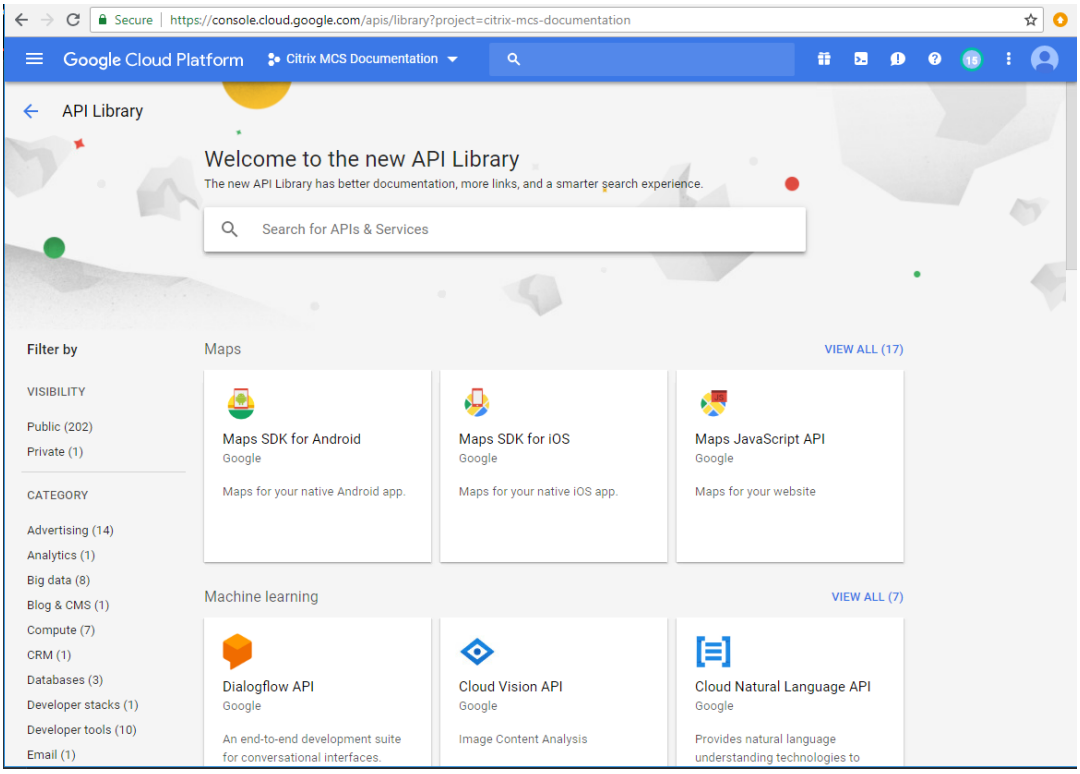
1. In the upper left menu, select **APIs and Services > Dashboard**.



2. On the **Dashboard** screen, ensure that Compute Engine API is enabled. If not, follow these steps:

    a) Navigate to **APIs and Services > Library**.

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



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**.

You can also use Google Cloud Shell to enable the APIs. To do this:

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

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

3. Click **Authorize** if 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 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

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

- *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:

   - 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

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

> **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.
- 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, Web Stduio 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 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**.

   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

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

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.

- 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

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

- cloudkms.keyRings.list

> **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.
- 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, Web 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.

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

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 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 Virtual Apps and Desktops improves the process of reporting cloud build failures for the Google Cloud service. This service runs builds on the Google Cloud. Citrix Virtual Apps and Desktops 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 Virtual Apps and Desktops 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

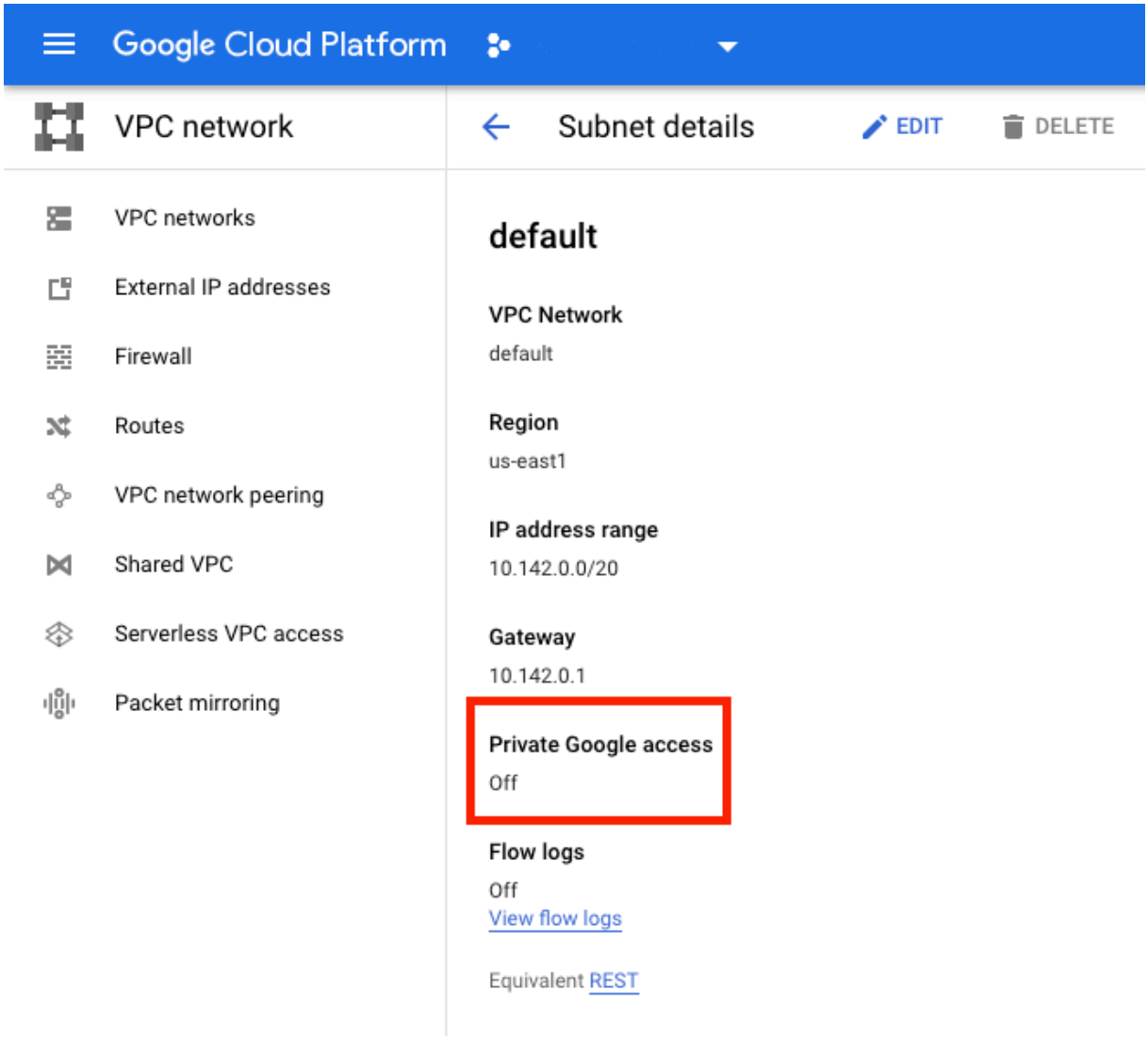
When a VM lacks an external IP address assigned to its network interface, packets are only sent to other internal IP addresses destinations. When you enable private access, the VM connects to the set of external IP addresses used by the Google API and associated services.

> **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. In the Subnet details screen, turn on **Private Google access**.

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



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

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection in Google Cloud environments, see Connection to Google cloud environments

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

More information

- Create and manage connections and resources
- Create machine catalogs

HPE Moonshot virtualization environments

September 6, 2025

Citrix Virtual Apps and Desktops™ manages your HPE Moonshot workloads through a Citrix-managed HPE Moonshot plug-in present. The Citrix-managed HPE Moonshot plug-in is installed automatically while upgrading or installing Citrix Virtual Apps and Desktops version 2503. 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.

> **Note:**
>
> Use Web Studio instead of MMC-based Studio.

Troubleshooting

If both Citrix-managed and HPE-managed HPE Moonshot plug-ins are installed, and

- If you want to use the **HPE-managed Moonshot plug-in**, then you must uninstall Citrix-managed HPE Moonshot plug-in and update the `RegisterPlugin` cache. To do so:

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

1. Open the PowerShell as an Administrator and run the following command to uninstall Citrix-managed HPE Moonshot plug-in:

```
$CtxMnsht = Get-WmiObject -Class Win32_Product | Where-Object{
 $_.Name -Contains "Citrix HPE Moonshot Plugin" }

$CtxMnsht.Uninstall()
```

2. Run the following command to register HPE-managed Moonshot plug-in:

```
cd "C:\Program Files\Common Files\Citrix\HCLPlugins\"
.\RegisterPlugins.exe -PluginsRoot "C:\Program Files\Common
   Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0\"
```

3. After the plug-in registration is successful, restart the following services from the **Task Manager**:

   a) CitrixBrokerService
   b) CitrixHostService
   c) CitrixMachineCreationService

4. Run `Get-HypHypervisorPlugins` to check if the plug-in is installed on the Delivery controller. The `DisplayName` field in the output must show as HPE Moonshot Machine Manager.

- If you want to install the Citrix-managed HPE Moonshot plug-in again, do the following:

1. Install `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin.msi`. The `E:\` is the ISO.
2. Open the PowerShell as an Administrator and run the following command to register Citrix-managed HPE Moonshot plug-in:

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\
   RegisterPlugins.exe -pluginsroot .\CitrixMachineCreation\v1
   .0.0.0\
```

3. After the plug-in registration is successful, restart the following services from the Task Manager:

   a) CitrixBrokerService
   b) CitrixHostService
   c) CitrixMachineCreationService

1. Run `Get-HypHypervisorPlugins` to check if the plug-in is installed on the Delivery controller. The DisplayName field in the output must show as HPE Moonshot.

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

Where to go next

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection in HPE Moonshot, see Connection to HPE Moonshot

More information

- Create and manage connections and resources
- Create machine catalogs

Microsoft Azure Resource Manager cloud environments

September 6, 2025

When using the Microsoft Azure Resource Manager to provision virtual machines in your Citrix Virtual Apps and Desktops™ deployment, get familiar with the following:

- Azure Active Directory: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/
- Consent framework: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration
- Service principal: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

To set up your Microsoft Azure Resource Manager, see Prepare to install.

Where to go next

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection in Azure environments, see Connection to Microsoft Azure

More information

- Create and manage connections and resources

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

- Create machine catalogs
- CTX219211: Set up a Microsoft Azure Active Directory account
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Microsoft System Center Configuration Manager environments

September 6, 2025

Sites using Microsoft System Center Configuration Manager (Configuration Manager) to manage access to applications and desktops can extend that use to Citrix Virtual Apps and Desktops™ using these options:

- Install VDAs using SCCM.
- **Configuration Manager Wake Proxy feature:** The Remote PC Access Wake on LAN feature is supported with Configuration Manager. For details, see Wake on LAN - SCCM integrated.
- **Citrix Virtual Apps and Desktops properties:** Properties enable you to identify Citrix Virtual Desktops™ for management through Configuration Manager. (In some versions, Configuration Manager uses the former name of Citrix Virtual Apps and Desktops: XenApp and XenDesktop.)

Properties

Properties are available to Microsoft System Center Configuration Manager to manage virtual desktops.

Boolean properties displayed in Configuration Manager appear as `1` or `0`, not true or false.

The properties are available for the `Citrix_virtualDesktopInfo` class in the `Root\Citrix\DesktopInformation` namespace. Property names come from the Windows Management Instrumentation (WMI) provider.

Property	Description
`AssignmentType`	Sets the value of IsAssigned. Valid values are: `ClientIP`, `ClientName`, `None`, and `User` (sets `IsAssigned` to `True`)
`BrokerSiteName`	Returns the same value as `HostIdentifier`
`DesktopCatalogName`	Machine catalog associated with the desktop.
`DesktopGroupName`	Delivery group associated with the desktop.

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

Property	Description
HostIdentifier	Returns the same value as BrokerSiteName.
IsAssigned	True to assign the desktop to a user, set to False for a random desktop
IsMasterImage	Allows decisions about the environment. For example, install applications on the image and not on the provisioned machines. Valid values are: True on a VM that is used as an image. This value is set during installation based on a selection, or cleared on a VM that is provisioned from that image.
IsVirtualMachine	True for a virtual machine, **false** for a physical machine.
OSChangesPersist	False if the desktop operating system image is reset to a clean state every time it is restarted; otherwise, **true**.
PersistentDataLocation	The location where Configuration Manager stores persistent data. This is not accessible to users.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Determined when the desktop registers with the Controller. They are null for a desktop that has not fully registered.

To collect the properties, run a hardware inventory in Configuration Manager. To view the properties, use the Configuration Manager Resource Explorer. In these instances, the names include spaces or vary slightly from the property names. For example, BrokerSiteName appears as Broker Site Name.

- Configure Configuration Manager to collect Citrix WMI properties from the Citrix VDA
- Create query-based device collections using Citrix WMI properties
- Create global conditions based on Citrix WMI properties
- Use global conditions to define application deployment type requirements

You can also use Microsoft properties in the Microsoft class CCM_DesktopMachine in the Root\ccm_vdi namespace. For more information, see the Microsoft documentation.

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

Microsoft System Center Virtual Machine Manager virtualization environments

September 6, 2025

Follow this guidance if you use Hyper-V with Microsoft System Center Virtual Machine Manager (VMM) to provide virtual machines.

This release supports the VMM versions listed in System requirements.

> **Note:**
>
> Mixed Hyper-V clusters (containing servers running different Hyper-V versions) are not supported.

You can use Citrix Provisioning (formerly Provisioning Services) and Machine Creation Services™ to provision:

- Generation 1 supported Desktop or Server OS VMs.
- Generation 2 supported Desktop or Server OS VMs, including Secure Boot support.

Install and configure a hypervisor

> **Important:**
>
> All Delivery Controllers must be in the same forest as the VMM servers.

1. Install Microsoft Hyper-V server and VMM on your servers.
2. Install the System Center Virtual Machine Manager console on all Controllers. 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.
3. Verify the following account information:

   The account you use to specify hosts in Studio is a VMM administrator or VMM delegated administrator for the relevant Hyper-V machines. If this account only has the delegated administrator role in VMM, the storage data is not listed in Studio during the host creation process.

   The user account used for Studio integration must also be a member of the administrators local security group on each Hyper-V server. This configuration supports VM life cycle management, such as VM creation, update, and deletion.

   Installing a Controller on a server running Hyper-V is not supported.

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

In large deployments where a single SCVMM manages multiple clusters in different data centers, you can limit the host groups scope of delegated admins.

To limit the host groups scope, use the Delegated Admin role in 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.

Where to go next

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection in SCVMM, see Connection to Microsoft System Center Virtual Machine Manager

More information

- Create and manage connections and resources
- Create machine catalogs

Nutanix virtualization environments

July 17, 2026

Connect Citrix Virtual Apps and Desktops 2507 CU1 and later 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.

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

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 Virtual Apps and Desktops deployment. However, this setup process requires installing and registering the Nutanix plug-in in your Citrix Virtual Apps and Desktops 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 Virtual Apps and Desktops 2507 CU1 and later 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, eliminating the need for separate installation on Delivery Controllers. For information on Citrix-managed components and services, see Technical overview.

Prerequisites

You need the following for Nutanix AHV Prism Central:

- Prism Central version pc.2024.3 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 7.0 or later for the Nutanix AHV clusters.
- Nutanix AHV clusters must register to the Prism Central.
- 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.

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

Key steps

1. Set up your Nutanix virtualization environments. For information, see Prepare to install 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 Delivery Controllers where Citrix Virtual Apps and Desktops 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.

Where to go next

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection in Nutanix environments, see Connection to Nutanix

More information

- Create and manage connections and resources
- Create machine catalogs

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

Nutanix cloud and partner solutions

November 12, 2025

Nutanix AHV Prism Central

Citrix Virtual Apps and Desktops 2507 CU1 and later 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 Virtual Apps and Desktops 2507 CU1 and later 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
- 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

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

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/*
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 Microsoft.Resources/subscriptions/tagNames/tagValues/read
```

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

```
      Microsoft.Resources/subscriptions/tagNames/tagValues/delete
      Microsoft.Resources/tags/read
28 Microsoft.Resources/tags/write
29 Microsoft.Resources/tags/delete
30 Microsoft.Resources/providers/read
31 Microsoft.Compute/sshPublicKeys/read
32 Microsoft.Compute/sshPublicKeys/write
33 Microsoft.Compute/sshPublicKeys/delete Microsoft.Compute/sshPublicKeys/
      generateKeyPair/action Microsoft.Nutanix/Interfaces/read
34 Microsoft.Nutanix/Interfaces/write
35 Microsoft.Nutanix/Interfaces/delete
36 Microsoft.Nutanix/Nodes/read
37 Microsoft.Nutanix/Nodes/write
38 Microsoft.Nutanix/Nodes/delete
39 Microsoft.Nutanix/register/action
40 Microsoft.Network/virtualHubs/*
41 Microsoft.Network/routeTables/read
42 Microsoft.Network/routeTables/write
43 Microsoft.Network/routeTables/delete
44 Microsoft.Network/routeTables/join/action
45 Microsoft.Network/routeTables/routes/read Microsoft.Network/routeTables
      /routes/write Microsoft.Network/routeTables/routes/delete Microsoft.
      CostManagement/query/read
46 Microsoft.CostManagement/views/read Microsoft.CostManagement/
      externalSubscriptions/query/read Microsoft.CostManagement/
      externalSubscriptions/dimensions/read Microsoft.CostManagement/
      externalSubscriptions/read Microsoft.CostManagement/
      externalBillingAccounts/forecast/read
47 Microsoft.CostManagement/externalBillingAccounts/read
48 Microsoft.CostManagement/externalBillingAccounts/query/read Microsoft.
      CostManagement/externalBillingAccounts/ externalSubscriptions/read
      Microsoft.CostManagement/externalSubscriptions/forecast/read
      Microsoft.CostManagement/operations/read Microsoft.CostManagement/
      forecast/read
49 Microsoft.Network/virtualWans/write
50 Microsoft.Network/virtualWans/read
51 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
52 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
53 Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read Microsoft.
      Network/privateEndpoints/privateDnsZoneGroups/delete
54 Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/
      action Microsoft.Storage/storageAccounts/blobServices/containers/
      blobs/delete
```

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

```
55 Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
       deleteBlobVersion/action
56 Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
       action Microsoft.Storage/storageAccounts/blobServices/containers/
       blobs/read Microsoft.Storage/storageAccounts/blobServices/containers
       /blobs/tags/read
57 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 Virtual Apps and Desktops 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

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection of Nutanix cloud and partner solutions, see Connection to Nutanix cloud and partner solutions

More information

- Create and manage connections and resources
- Create machine catalogs

Red Hat OpenShift virtualization environments

December 15, 2025

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: Currently available for cluster networking.
  - OVS Bridge: Scheduled for upcoming release.
- 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.

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

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.
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:

```
1  .\oc.exe login --token=<token> --server=<server address>
```

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

6. Create a service account.

   - If you want to create the service account under the default namespace, run:

   ```
   .\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
    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/.

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

Where to go next

- Install core components
- Install VDAs
- Create a site
- 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

May 5, 2025

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.)

If you plan to use MCS, do not disable the Datastore Browser feature in vCenter Server (described in https://kb.vmware.com/s/article/2101567). When you disable this feature, MCS does not work correctly.

Where to go next

- Install core components
- Install VDAs
- Create a site
- For creating and managing a connection in VMware environments, see Connection to VMware

More information

- Create and manage connections and resources
- Create machine catalogs

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

VMware cloud and partner solutions

September 6, 2025

Citrix Virtual Apps and Desktops™ supports the following VMware cloud and partner solutions:

- Azure VMware Solution (AVS)
- Google Cloud VMware Engine
- VMware Cloud on Amazon Web Services (AWS)

Azure VMware Solution (AVS) integration

Citrix Virtual Apps and Desktop service supports AVS. AVS provides cloud infrastructure containing vSphere clusters created by Azure infrastructure. Leverage the Citrix Virtual Apps and Desktop Service to use AVS for provisioning your VDA workload in the same way that you would using vSphere in on-premises enviornments.

Set up the AVS cluster

To enable the Citrix Virtual Apps™ and Desktop Service to use AVS, perform the following steps in Azure:

- Request a host quota
- Register the Microsoft.AVS resource provider
- Network Checklist
- Create an Azure VMware Solution private cloud
- Access an Azure VMware Solution private cloud
- Configure networking for your VMware private cloud in Azure
- Configure DHCP for Azure VMware Solution
- Add a network segment in Azure VMware Solution
- Verify Azure VMware Solution 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

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

- Problem type:Capacity Management Issues
- Problem subtype:Customer Request for Additional Host Quota/Capacity

In the **Description** of the support ticket, incldue the following information in the **Details** tab:

- POC or Production
- Region Name
- Number of hosts
- Any other details

> **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:

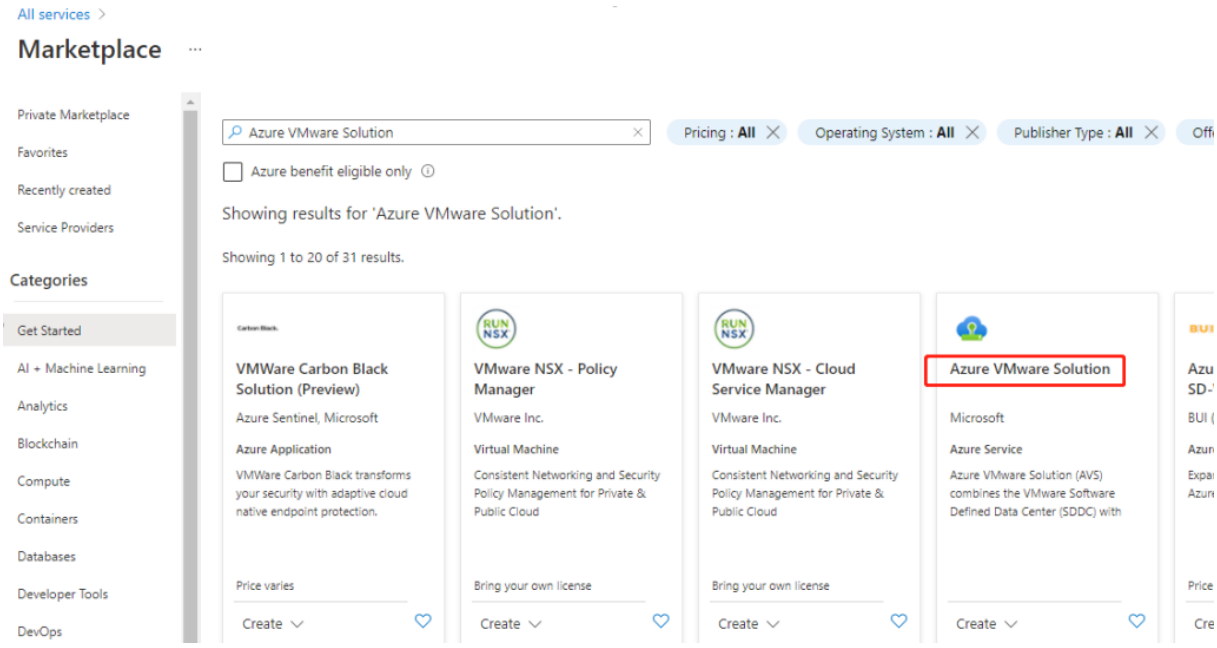
1. Sign in to the Azure portal.
2. On the Azure portal menu, select **All services**.
3. In the **All services** menu, enter the subscription, and select **Subscriptions**.
4. Select the subscription from the subscription list.
5. Select **Resource providers** and enter **Microsoft.AVS** in the search 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 Azure VMware Solution private cloud After conidering network requirements for your environment, create a 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.



image

In the **Azure VMware Solution** window:

1. Select **Create**.
2. Click the **Basics** tab.
3. Enter values for the fields, using the information in the table below:

Field	Value
Subscription	Select the subscription 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.
SKU	Select AV36.

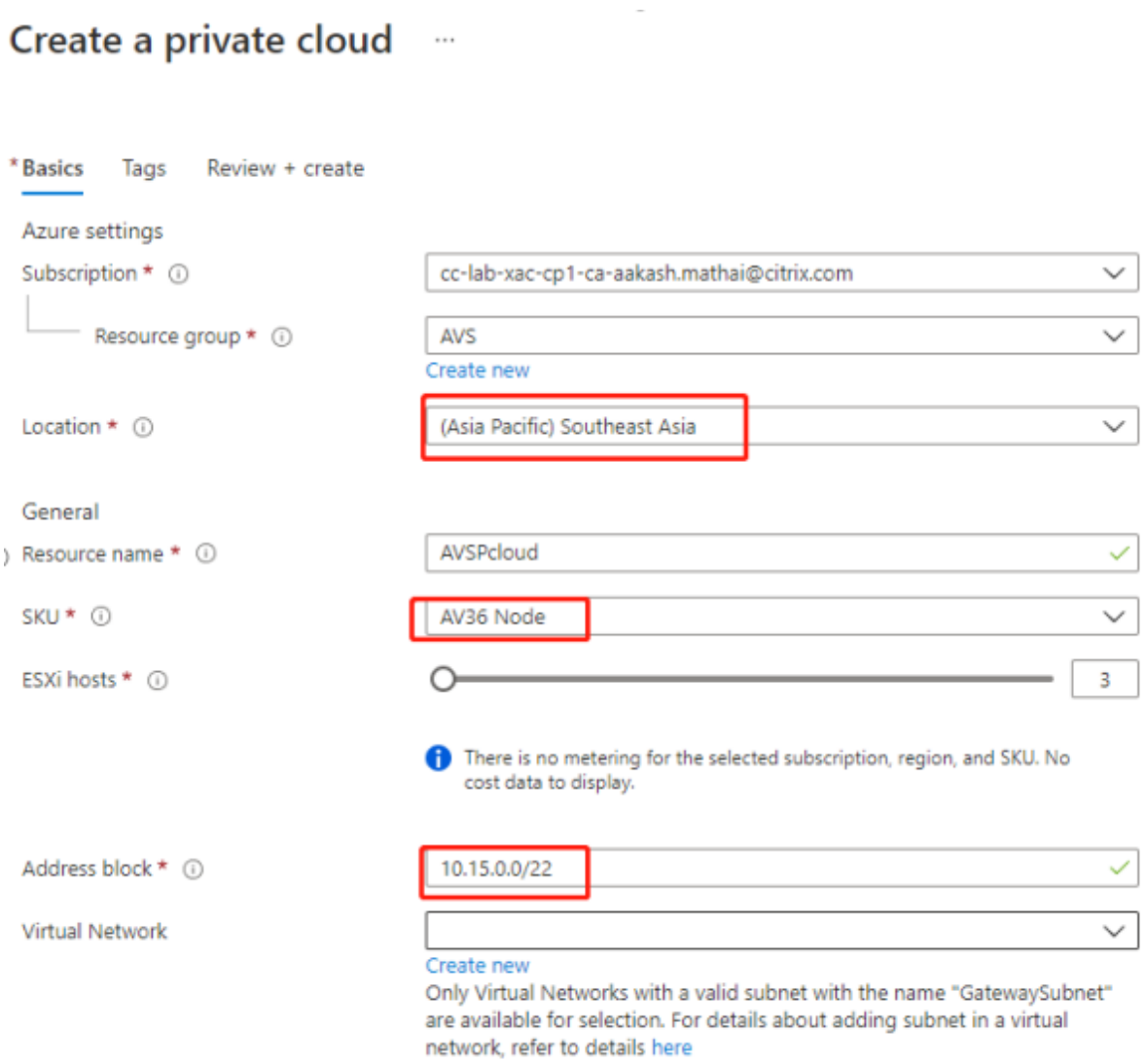
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Value
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	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 as well as with on-premises networks.
Virtual Network	Leave this blank because the Azure VMware Solution ExpressRoute circuit is established as a post-deployment step.

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 **SKU** field, select **AV36 Node**.
3. Specify an IP address in the **Address Block** field. For example, 10.15.0.0/22.
4. Select **Review + Create**.
5. After reviewing the information, click **Create**.

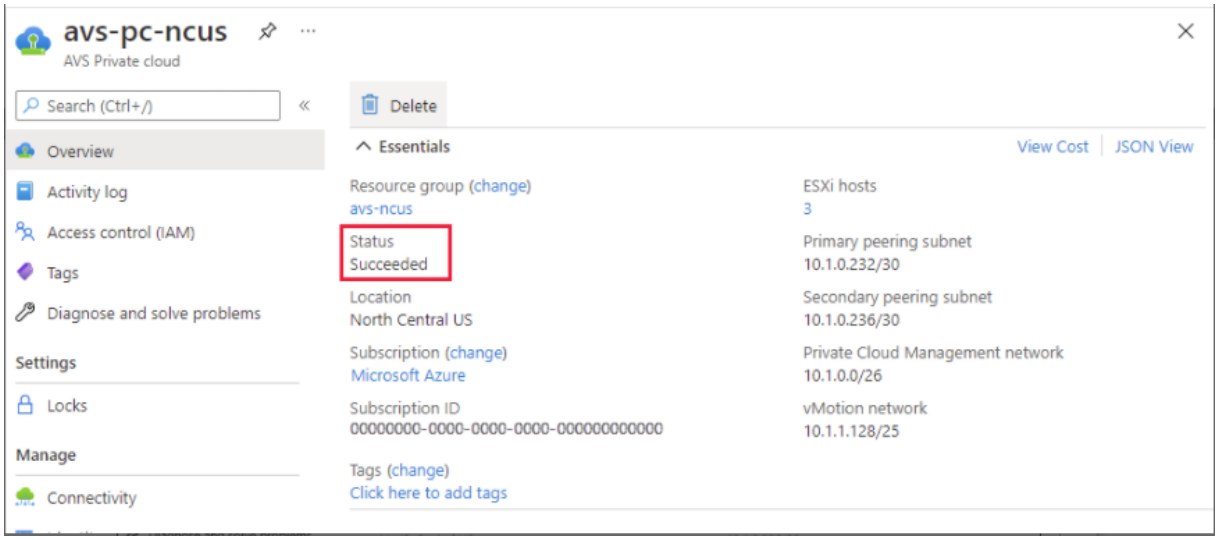
© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Tip:**
>
> Creating a private cloud can take 3-4 hours. Adding a single host to cluster can take 30-45 minutes.

Verify that the deployment was successful. Navigate to the resource group 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 an Azure VMware Solution private cloud Once you have created a private cloud, create a Windows VM and connect to the local vCenter of your private cloud.

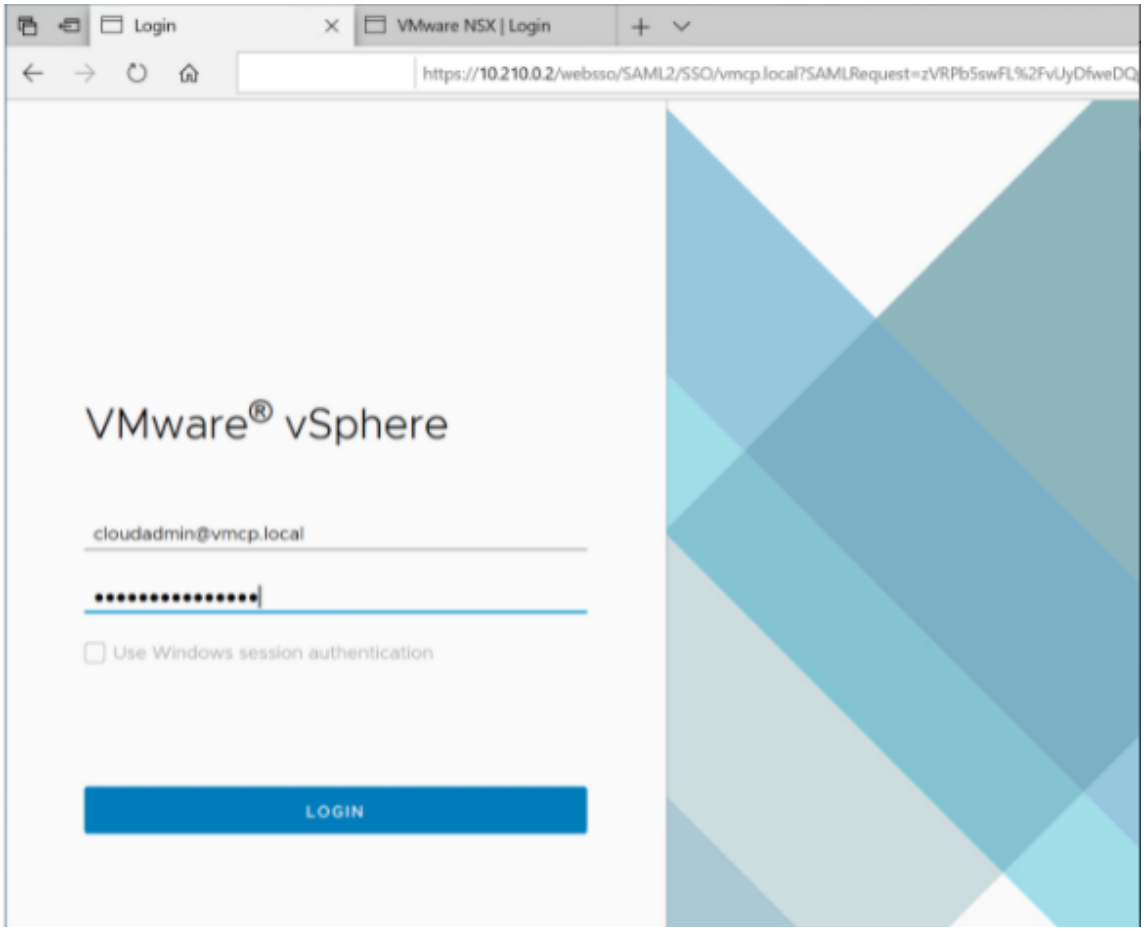
Create a new Windows virtual machine

1. In the resource group, select **+ Add** then search and select **Microsoft Windows 10/2016/2019**.
2. Click **Create**.
3. Enter the required information, then select **Review + Create**.
4. 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.

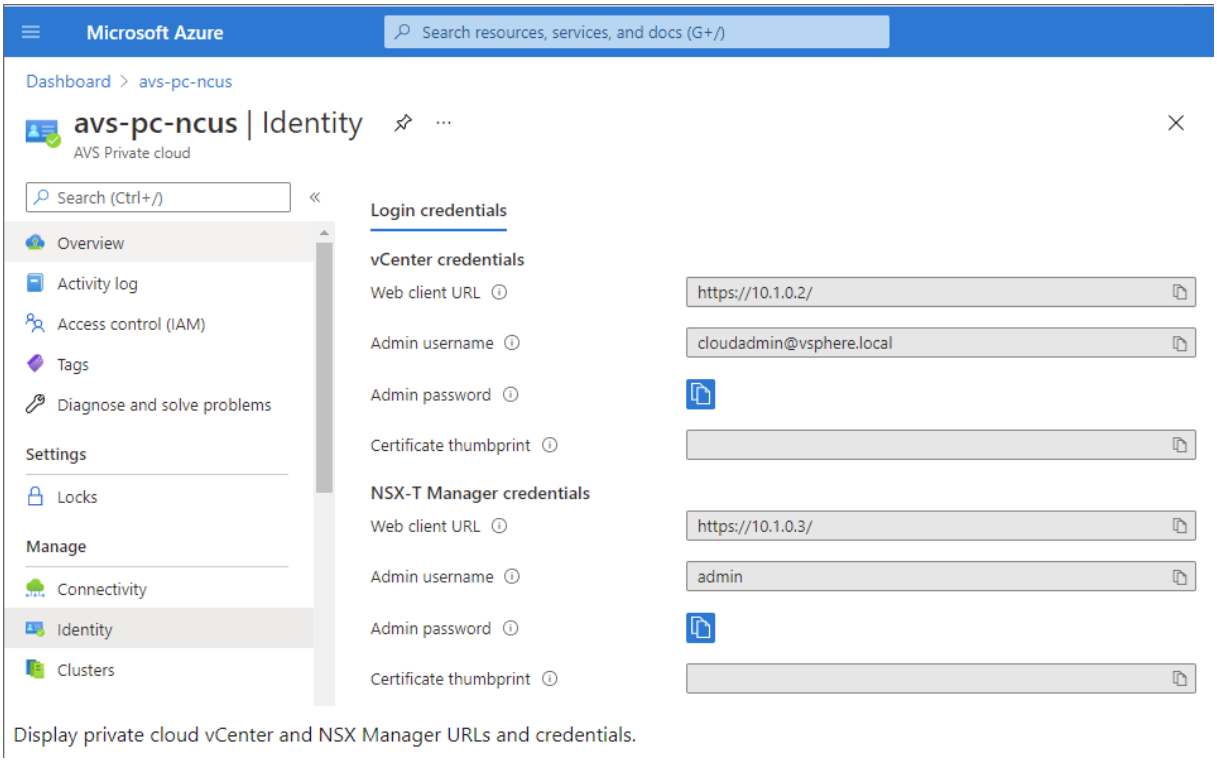
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.



Display private cloud vCenter and NSX Manager URLs and credentials.

After confirming URLs and user credentials:

1. Navigate to the VM 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 *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.

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

> **Important:**
>
> Use an address that does not overlap with the address space you used when you created your private cloud.

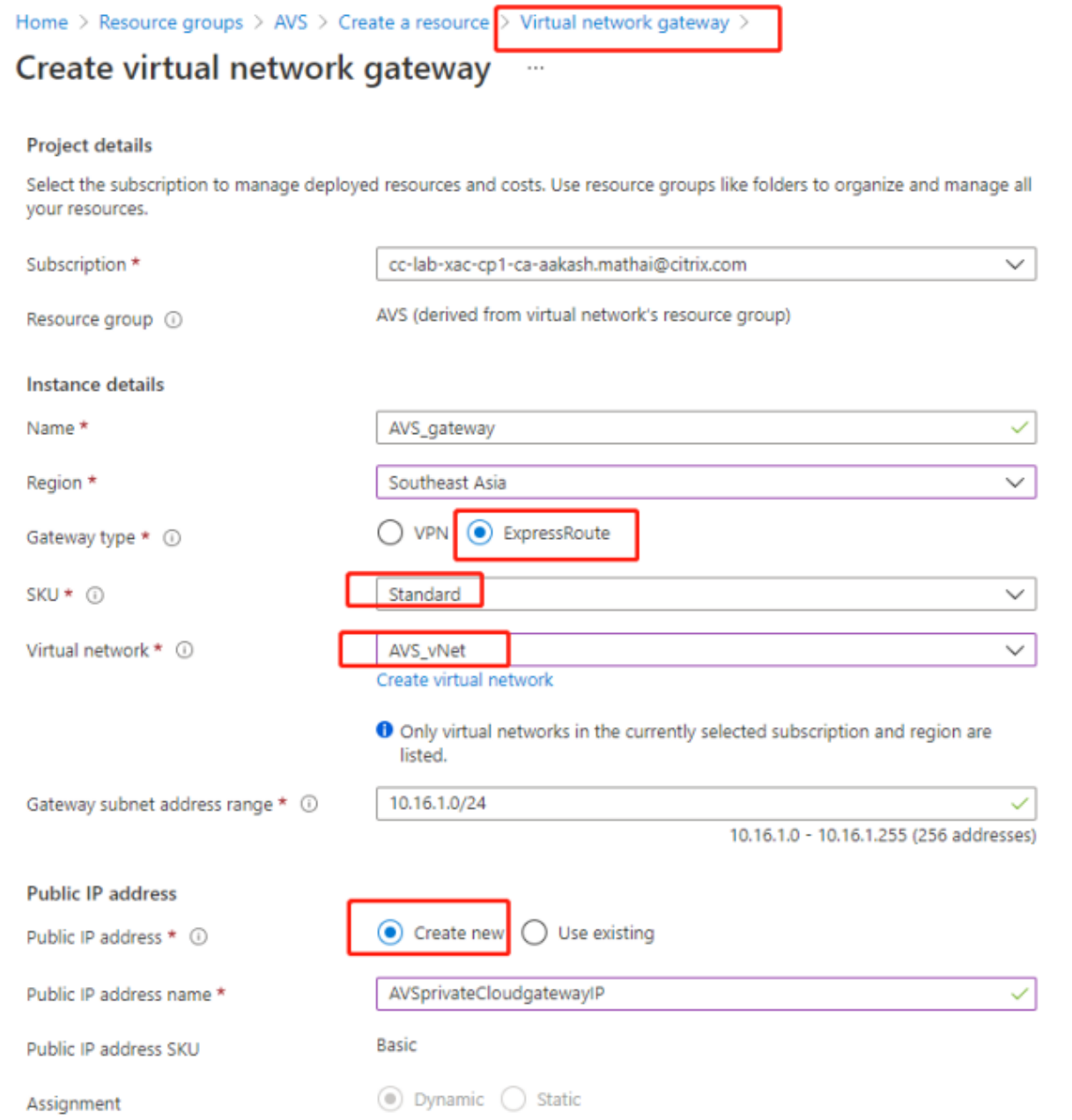
After entering the address space:

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.

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.

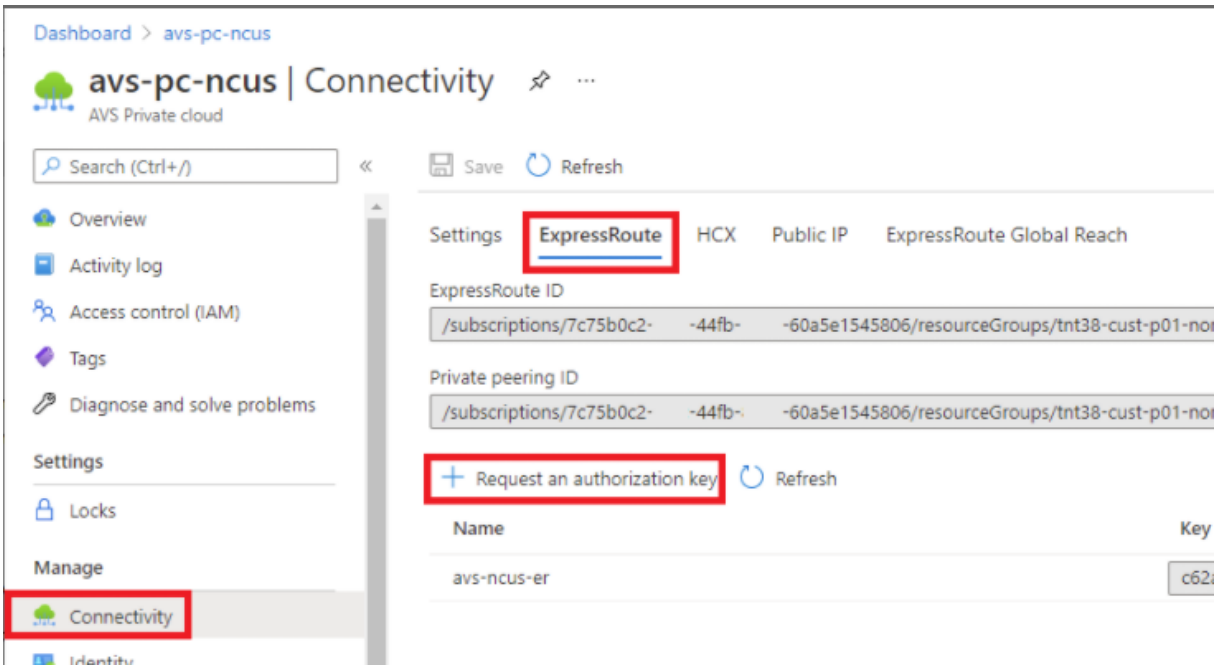
Once the deployment completes, connect your **ExpressRoute** connection to the virtual network gateway containing your Azure AVS private cloud.

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.

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

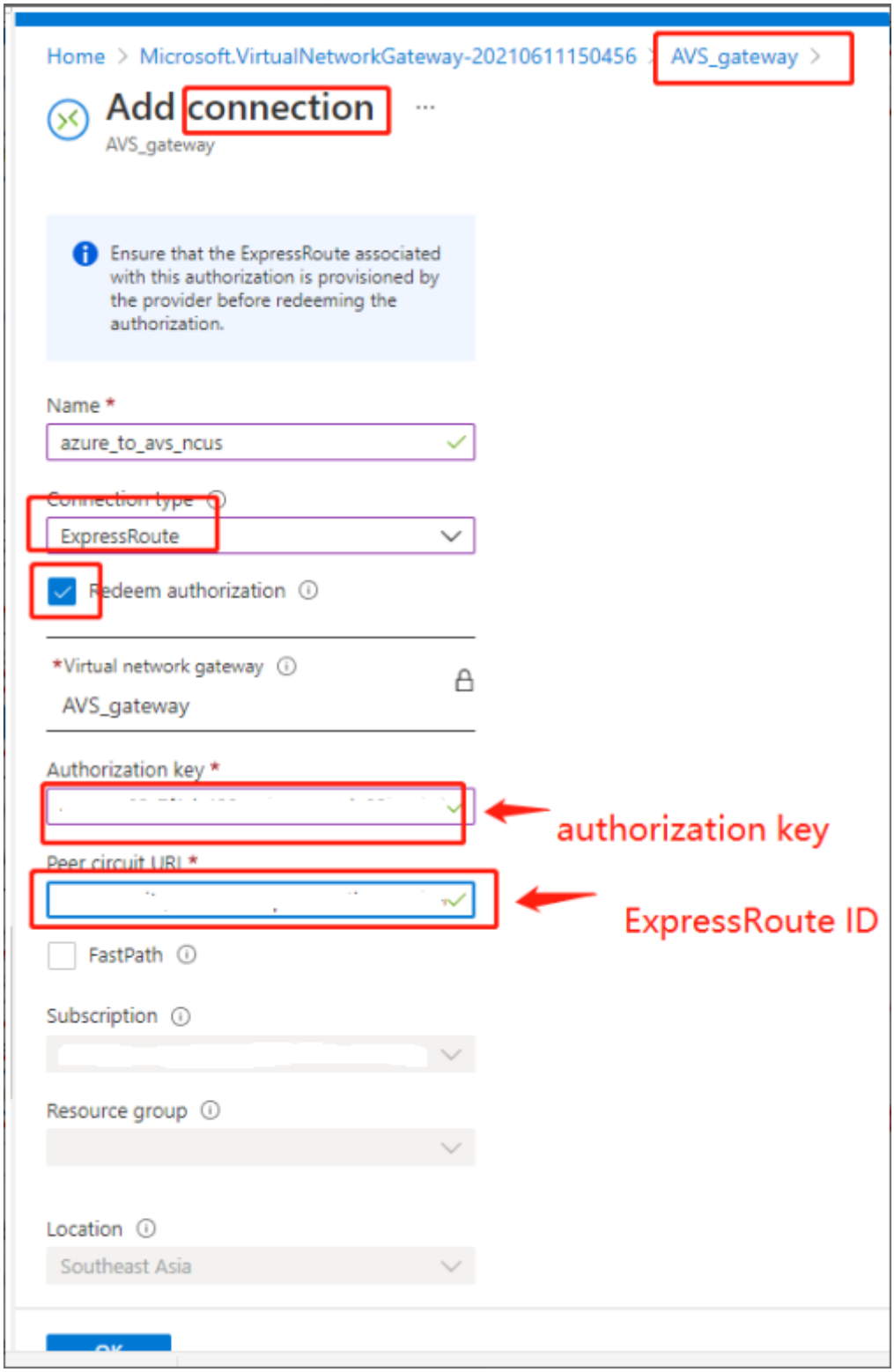
2. In the Azure portal, navigate to the **Azure VMware Solution private cloud**. Select **Manage> Connectivity > ExpressRoute** and then select **+ Request an authorization key.**



After requesting an authorization key:

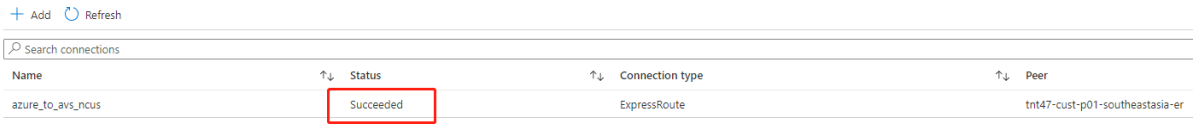
1. Enter a name for the key and click **Create**. It may take about 30 seconds to create the key. Once created, the new key appears in the list of authorization keys for the private cloud.
2. Copy the **authorization key** and **ExpressRoute ID**. You'll need them to complete the peering process. The authorization key disappears after some time, so copy it as soon as 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:

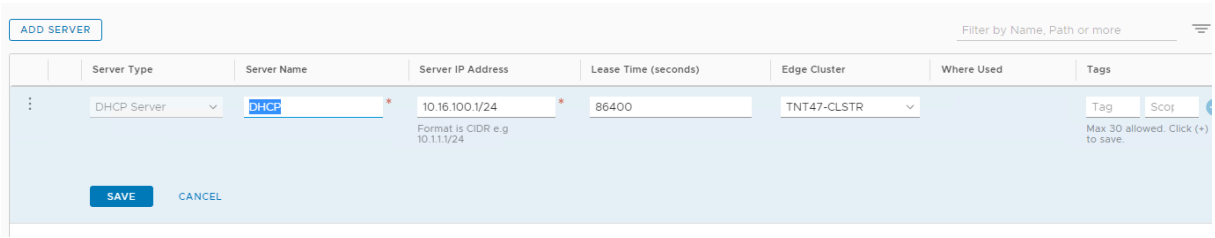
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure DHCP for Azure VMware Solution After connecting ExpressRoute to the virutal gateway, configure DHCP.

Use NSX-T to host your DHCP server In NSX-T Manager:

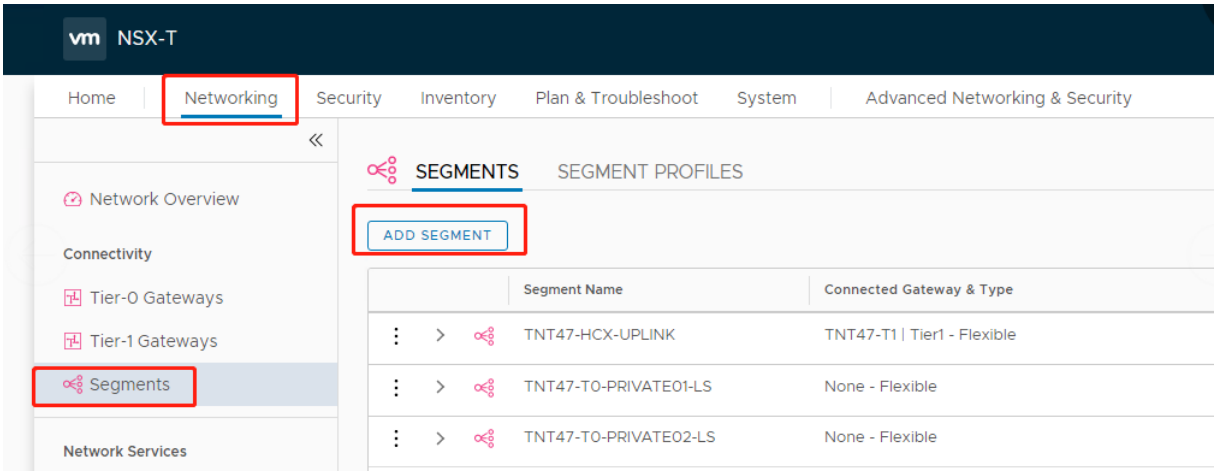
1. Select **Networking> DHCP**, and then select **Add Server**.
2. Select **DHCP** for the **Server Type**, provide the server name and IP address.
3. Click **Save**.
4. Select **Tier 1 Gateways**, select the vertical ellipsis on the Tier-1 gateway, and then select **Edit**.
5. Select **No IP Allocation 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 Azure VMware Solution After settnig up DHCP, add a network segment.

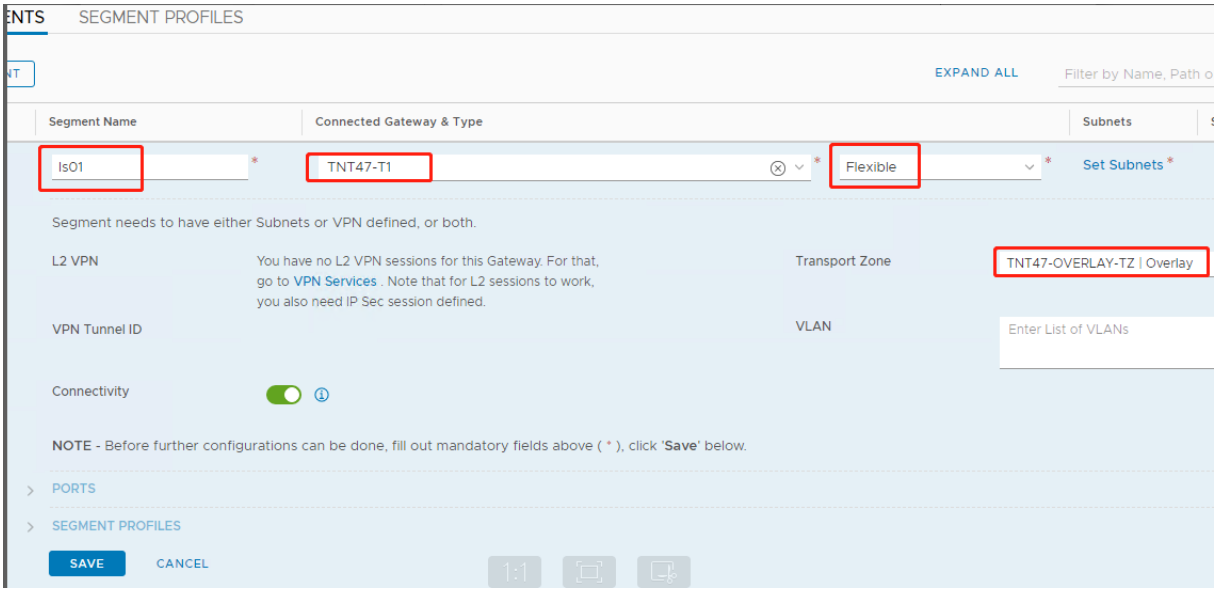
To add a network segment, in NSX-T Manager, select **Networking> Segments**, and then click **Add Segment**.

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



In the **Segments profile** screen:

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:

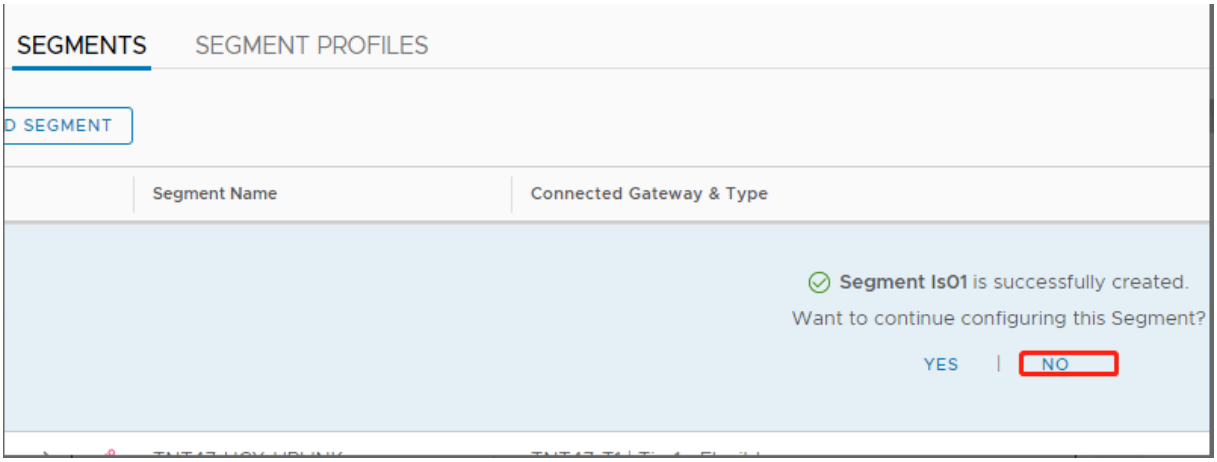
1. Enter the gateway IP address.
2. Select **Add**.

> **Important:**
>
> This segment IP address must belong to the Azure gateway IP address, 10.15.0.0/22.

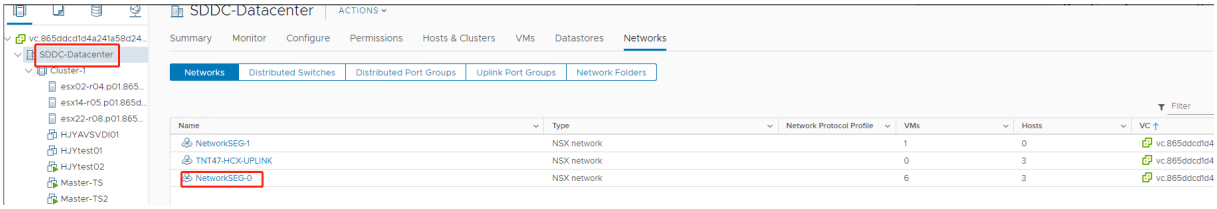
© 1997–2026 Citrix Systems, Inc. All rights reserved.

DHCP range should be belong to segment IP address:

Select **No** to decline the option to continue configuring the segment:

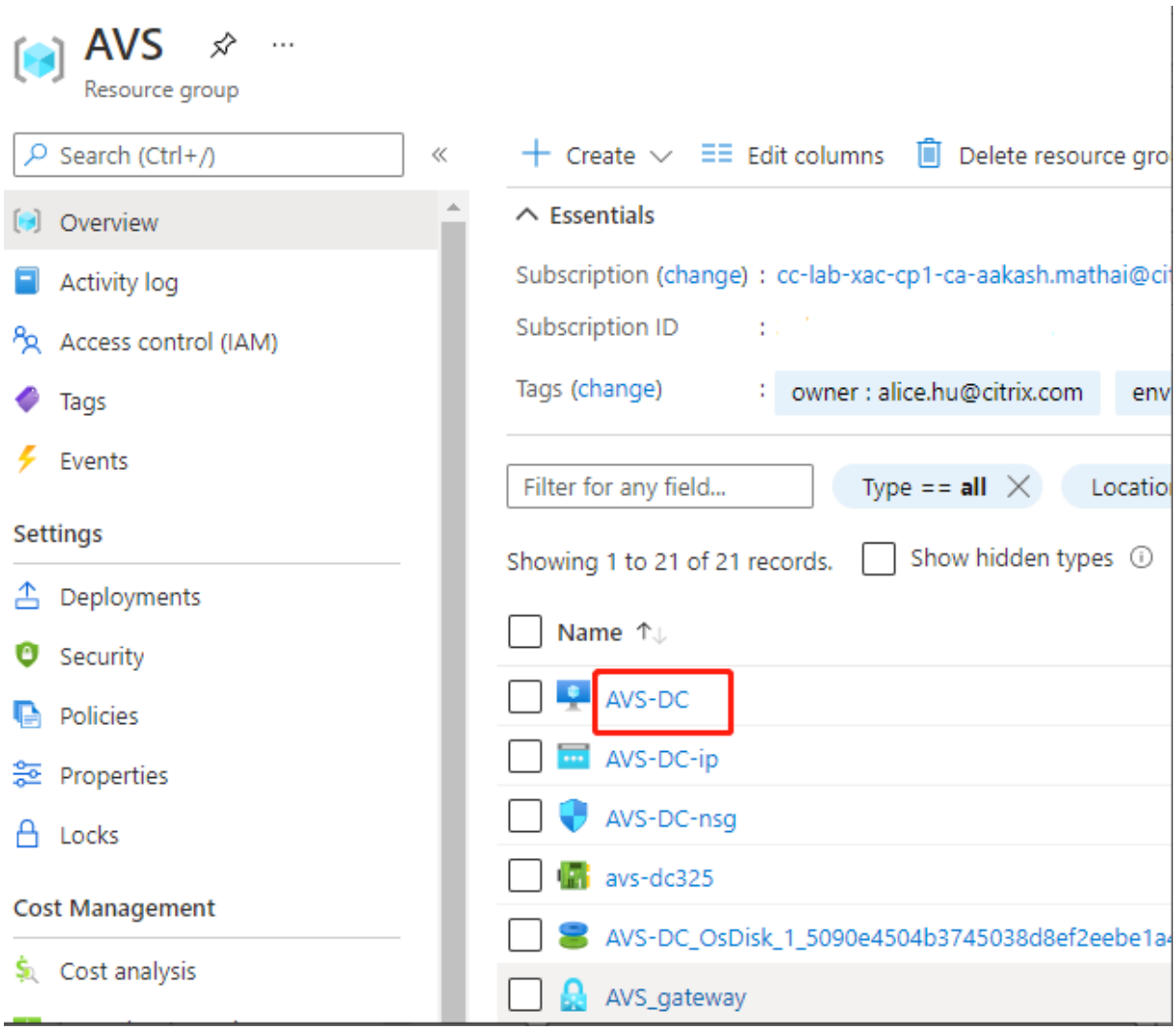


In vCenter, select **Networking > SDDC-Datacenter**:

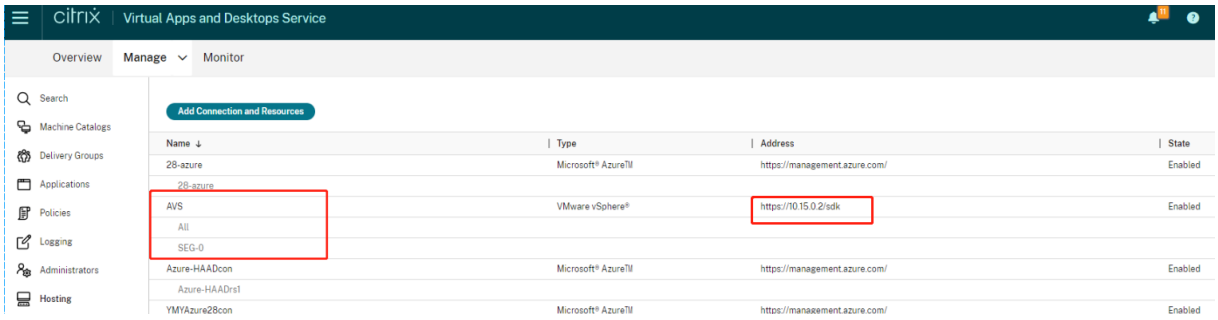


Verify the Azure AVS environment Setup a direct connection and connector in the Azure resource group:

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



Verify the connection with vCenter credentials:



Google Cloud VMware Engine

Citrix Virtual Apps and Desktops 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. Prepare 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.
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.

   > **Important:**
   >
   > The CIDR range must not overlap with any of your on-premises or cloud subnets. The CIDR range must be /27 or higher.

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.

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

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 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.

To deploy a VPN gateway:

1. In the **Google Cloud VMware Engine** portal, go to **Network > VPN Gateways**. Click **Create New VPN Gateway**.
2. Supply the name for the VPN gateway and the client subnet reserved during planning. 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.

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

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.

   > **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.

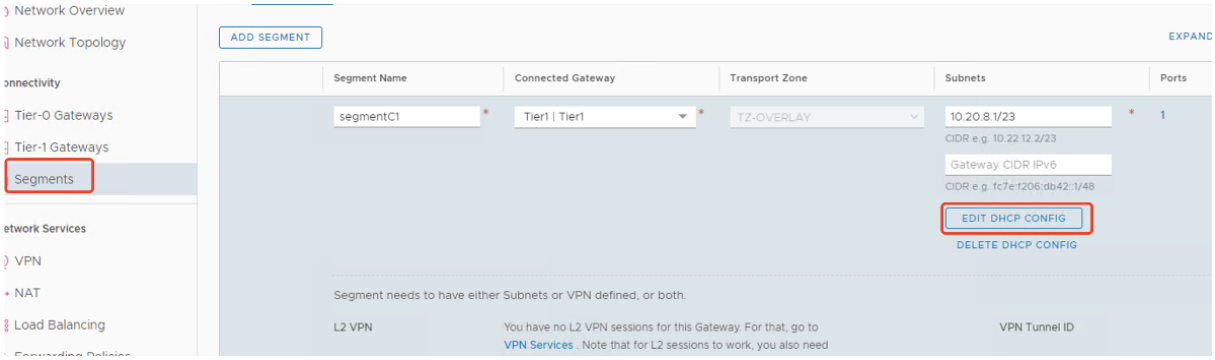
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a network segment in NSX-T For workload VMs, you create subnets as NSX-T network segments for your private cloud:

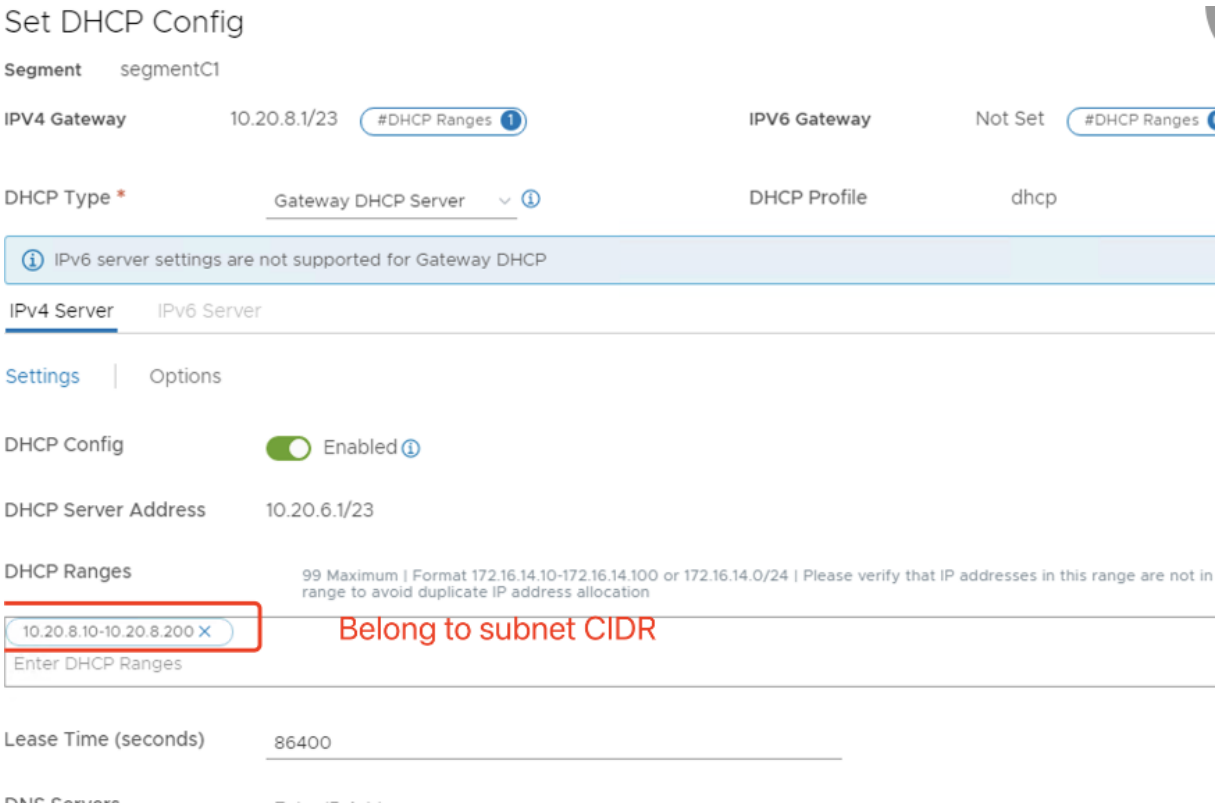
1. In NSX-T Manager, go to **Networking > Segments**.
2. Click **Add Segment**.
3. Enter a name for the segment.
4. Select the **Tier-1** as the **Connected Gateway** and leave the Type as **Flexible**.
5. Click **Set Subnets**.
6. Click **Add Subnets**.
7. Enter the subnet range in the **Gateway IP/Prefix 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.



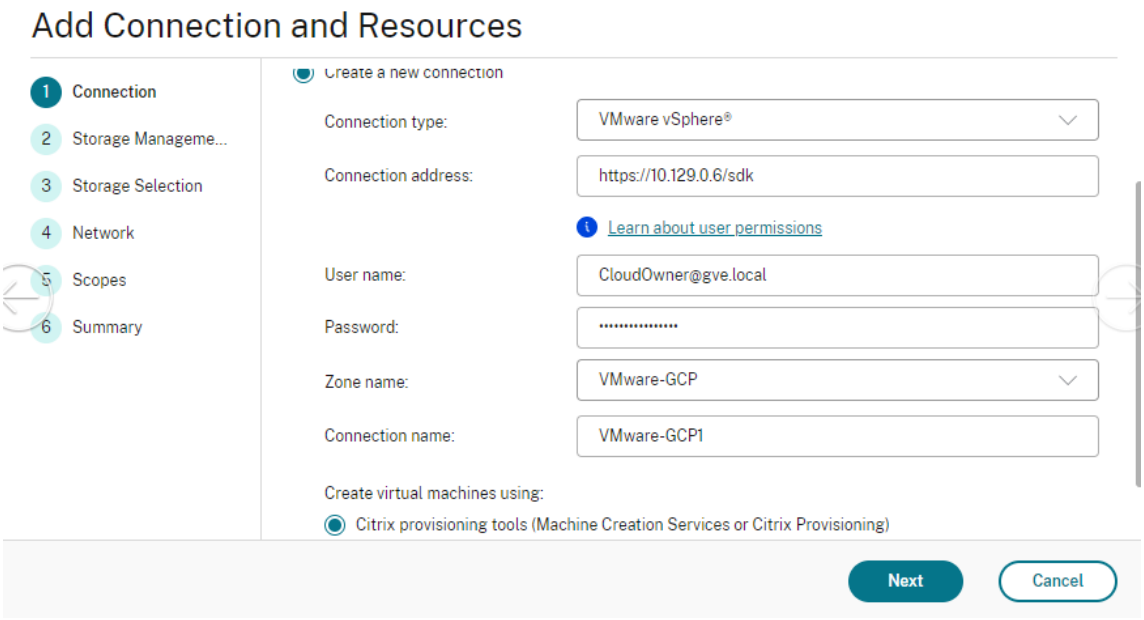
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create the Google Cloud VMware connection in Citrix Studio

1. Create a machine in vCenter.
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 NSX-T server.
6. Complete the wizard.

VMware cloud on Amazon Web Services (AWS)

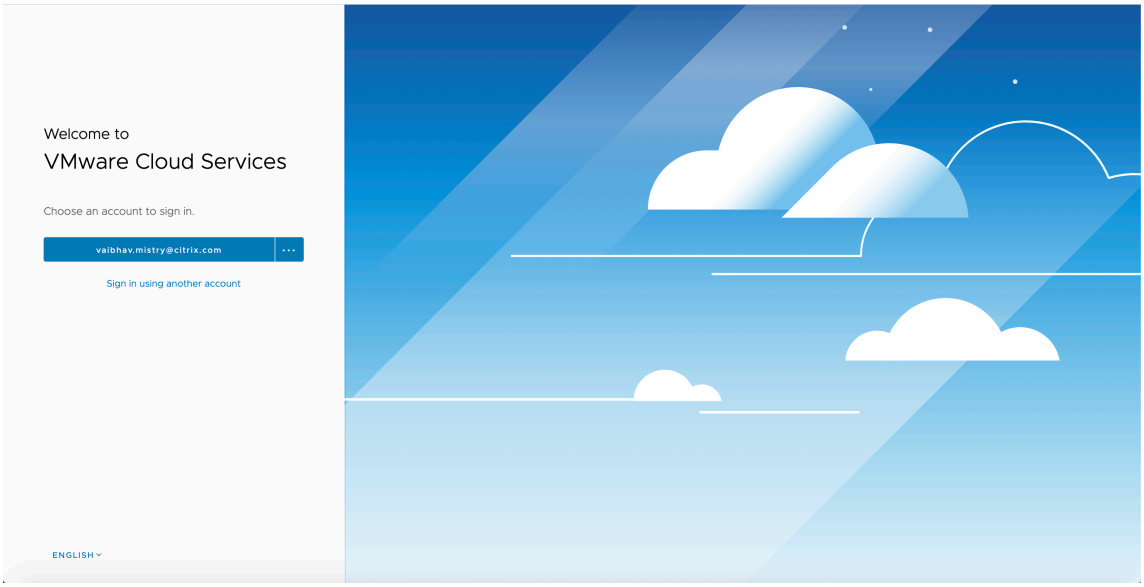
VMware cloud on Amazon Web Services (AWS) enables you to migrate VMware based on-premises Citrix workloads to AWS Cloud.

This article describes the procedure to set up a VMware cloud on AWS.

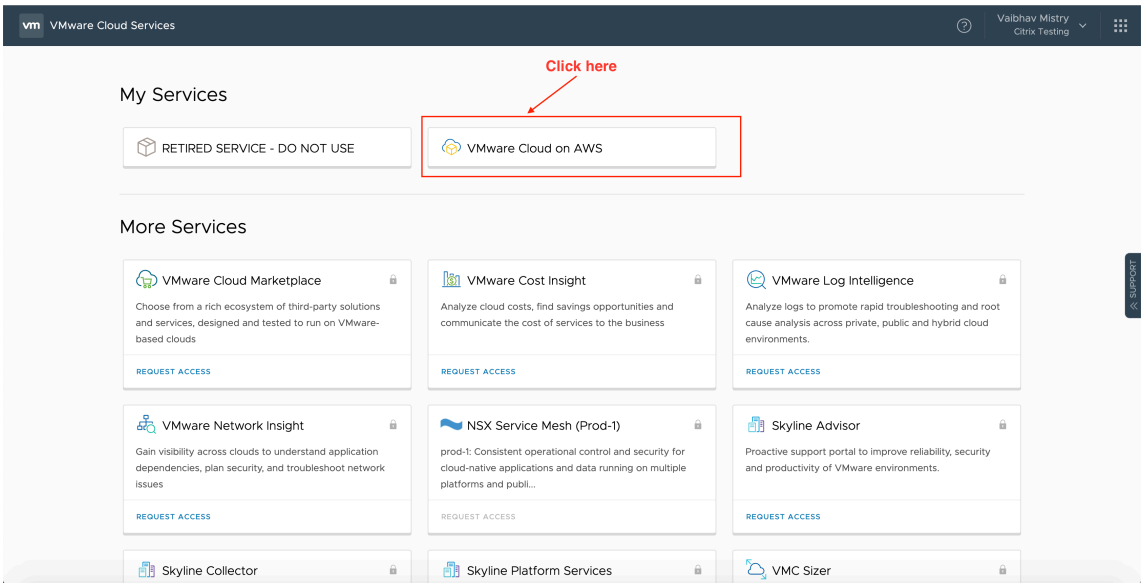
Access the VMware cloud environment

1. Log in to VMware cloud services using the URL https://console.cloud.vmware.com/.

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

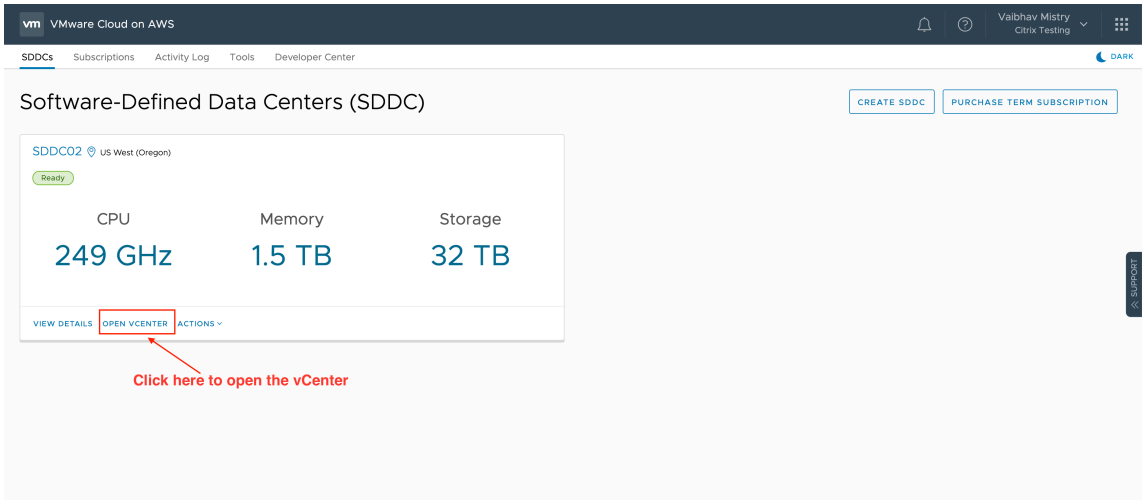


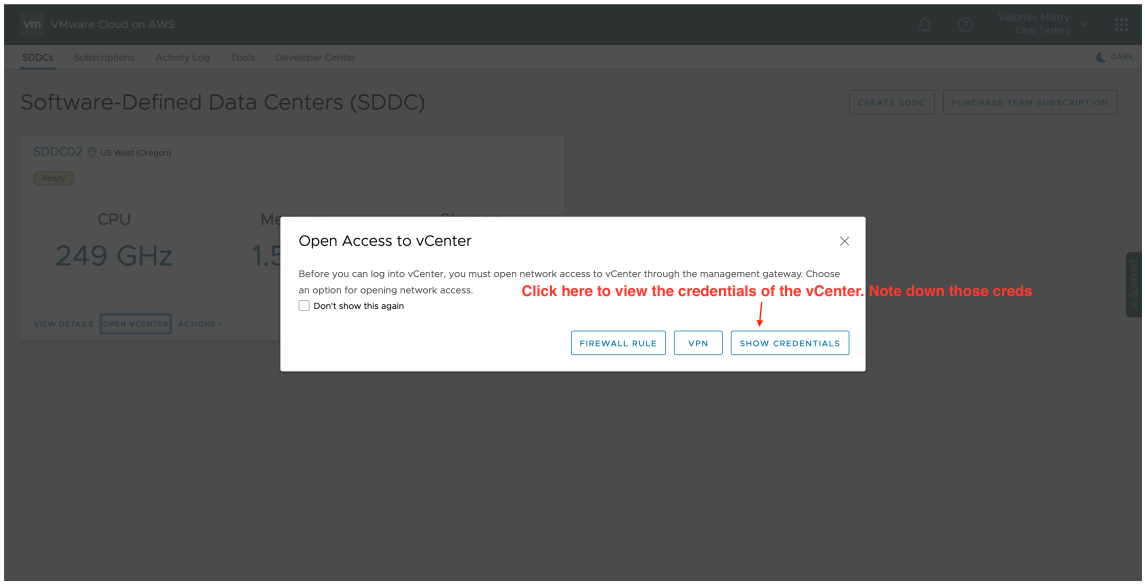
2. Click **VMware Cloud on AWS**. The page Software-Defined Data Centers (SDDC) appears.



3. Click **OPEN VCENTER**, and then click **SHOW CREDENTIALS**. Note the credentials for later use.

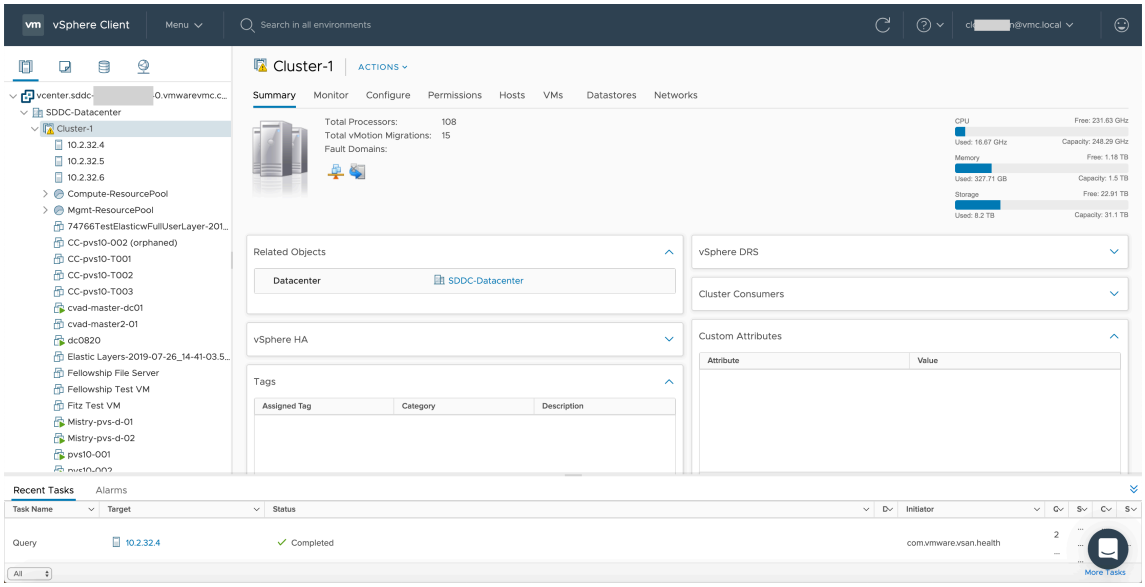
© 1997–2026 Citrix Systems, Inc. All rights reserved.





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.

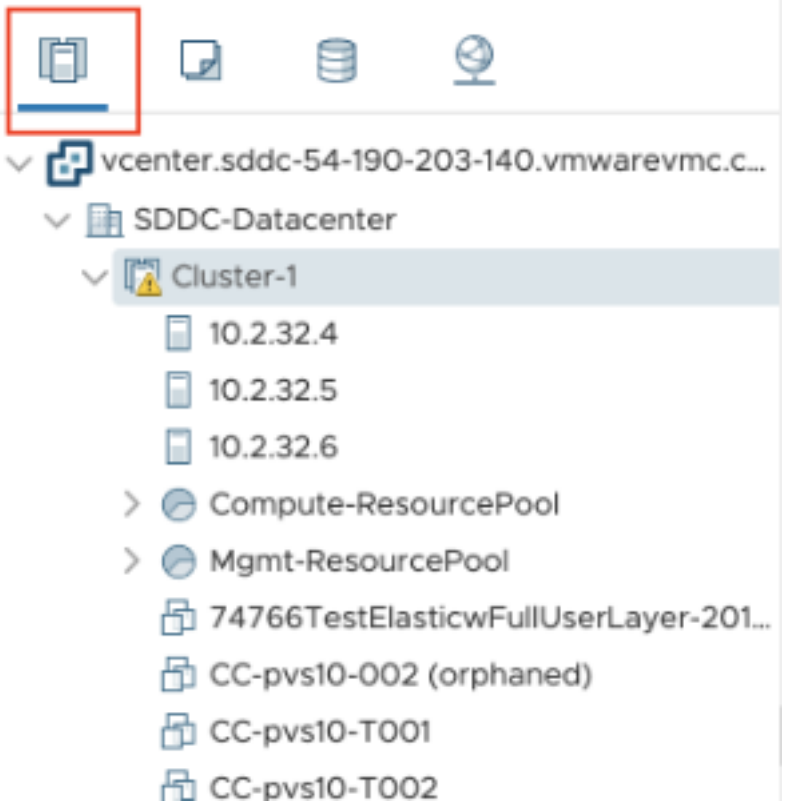
© 1997–2026 Citrix Systems, Inc. All rights reserved.



About VMware cloud environment

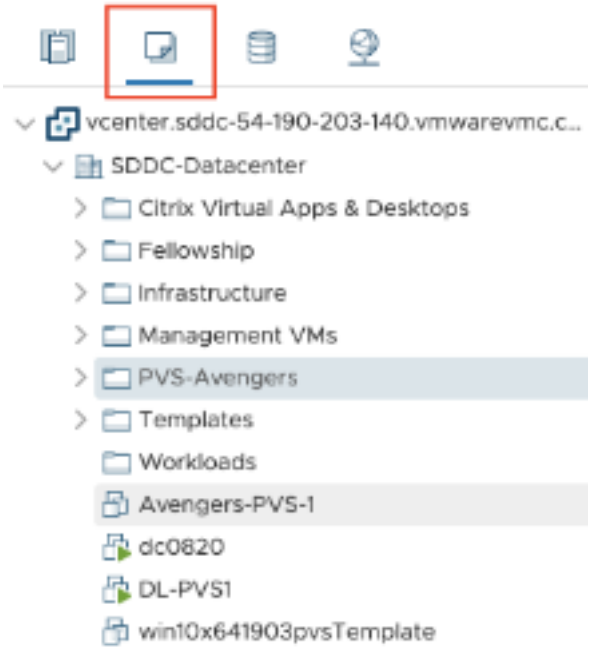
There are four views on the vSphere client webpage.

- Host and Cluster view: You cannot create a new Cluster, but the cloud admin can create multiple resource pools.



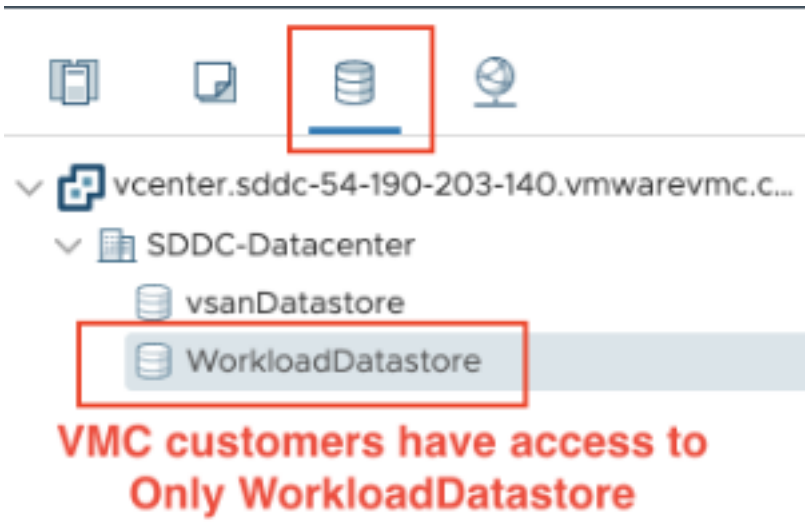
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VM and Template view: Cloud admin can create many folders.

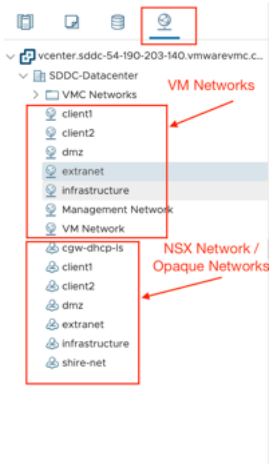


- Storage View: Select **WorkloadDatastore** storage when you add hosting unit in the Citrix Studio because you have access to only Workload Datastore.

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



- Network View: The icons are different for VMware cloud networks and opaque networks.



After you set up the cluster, refer to VMware virtualization environments for adding connections and resources.

Where to go next

- Install core components
- Install VDAs
- Create a site

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

- For creating and managing a connection, see Connection to VMware cloud and partner solutions

More information

- Create and manage connections and resources
- Create machine catalogs

Install core components

September 13, 2025

> **Important:**
>
> - Citrix collects basic licensing data as necessary for its legitimate interests, including license compliance. For more information, see Citrix Licensing Data.
> - Ensure the License Server is running a minimum of version 11.17.2 build 53100. Failure to meet this prerequisite will block the Citrix Virtual Apps and Desktops site upgrades and site creation.

The core components are the Citrix Delivery Controller™, Citrix Studio, Web Studio, Citrix Director, and Citrix License Server.

> **Note:**
>
> Citrix Studio is a Windows-based management console that lets you configure and manage your on-premises Citrix Virtual Apps and Desktops deployment. Web Studio is the next generation of Citrix Studio —a web-based management console offering full feature parity with Citrix Studio. For more information about Web Studio, see Install Web Studio.

(In versions before 2003, core components included Citrix StoreFront. You can still install StoreFront by clicking the **Citrix StoreFront** tile or running the command available on the installation media.)

Before you start an installation, review this article and Prepare to install.

This article describes the installation wizard sequence when installing core components. Command-line equivalents are provided. For more information, see Install using the command line.

Step 1. Download the product software and launch the wizard

Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops™ download page. Download the product ISO file.

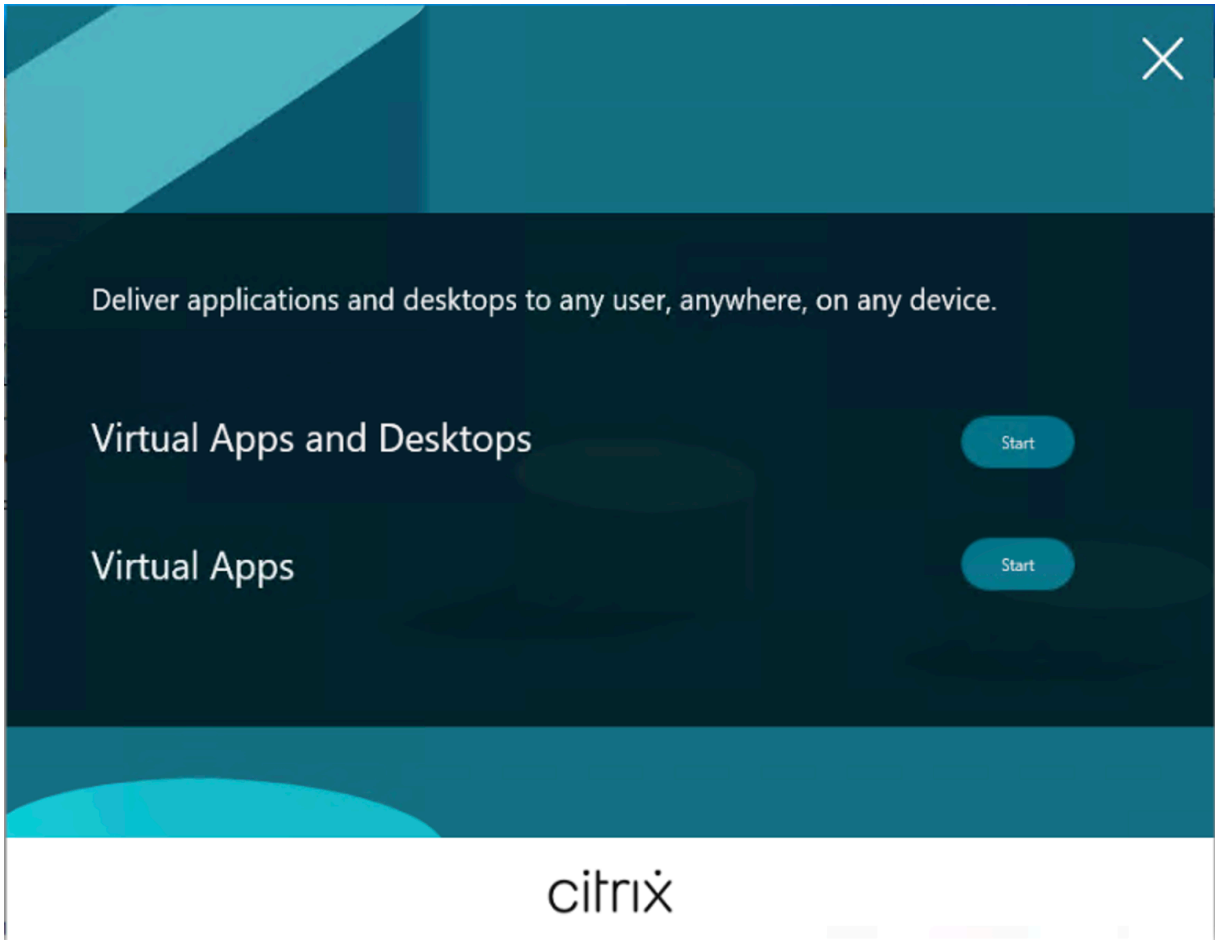
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unzip the file. Optionally, burn a DVD of the ISO file.

Log on to the machine where you are installing the core components, using a local administrator account.

Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the **AutoSelect** application or the mounted drive.

Step 2. Choose which product to install



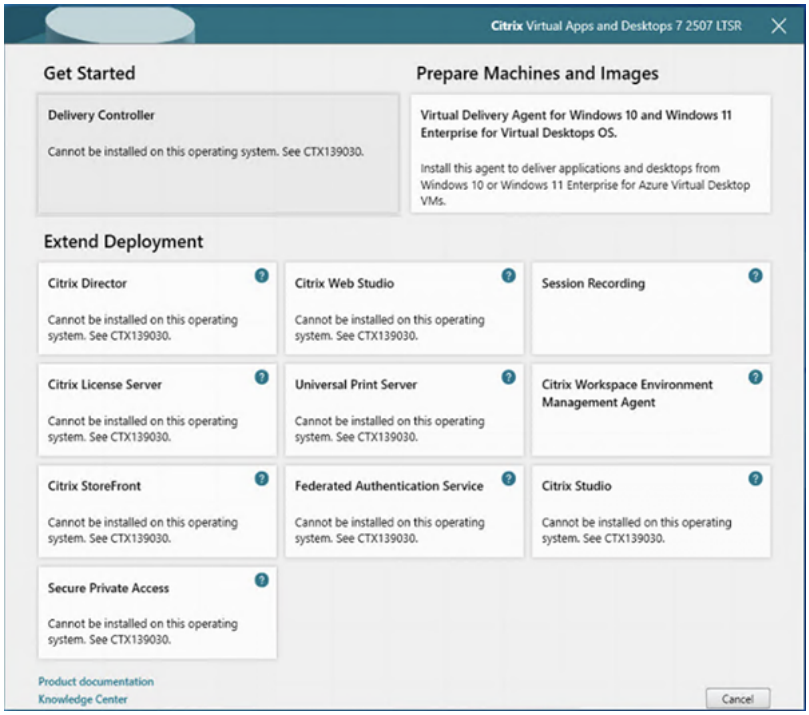
Click **Start** next to the product to install: Virtual Apps or Virtual Apps and Desktops.

(If the machine already has Citrix Virtual Apps and Desktops components installed on it, this page does not appear.)

Command-line option: `/xenapp` to install Citrix Virtual Apps. Citrix Virtual Apps and Desktops is installed if option is omitted.

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

Step 3. Choose what to install



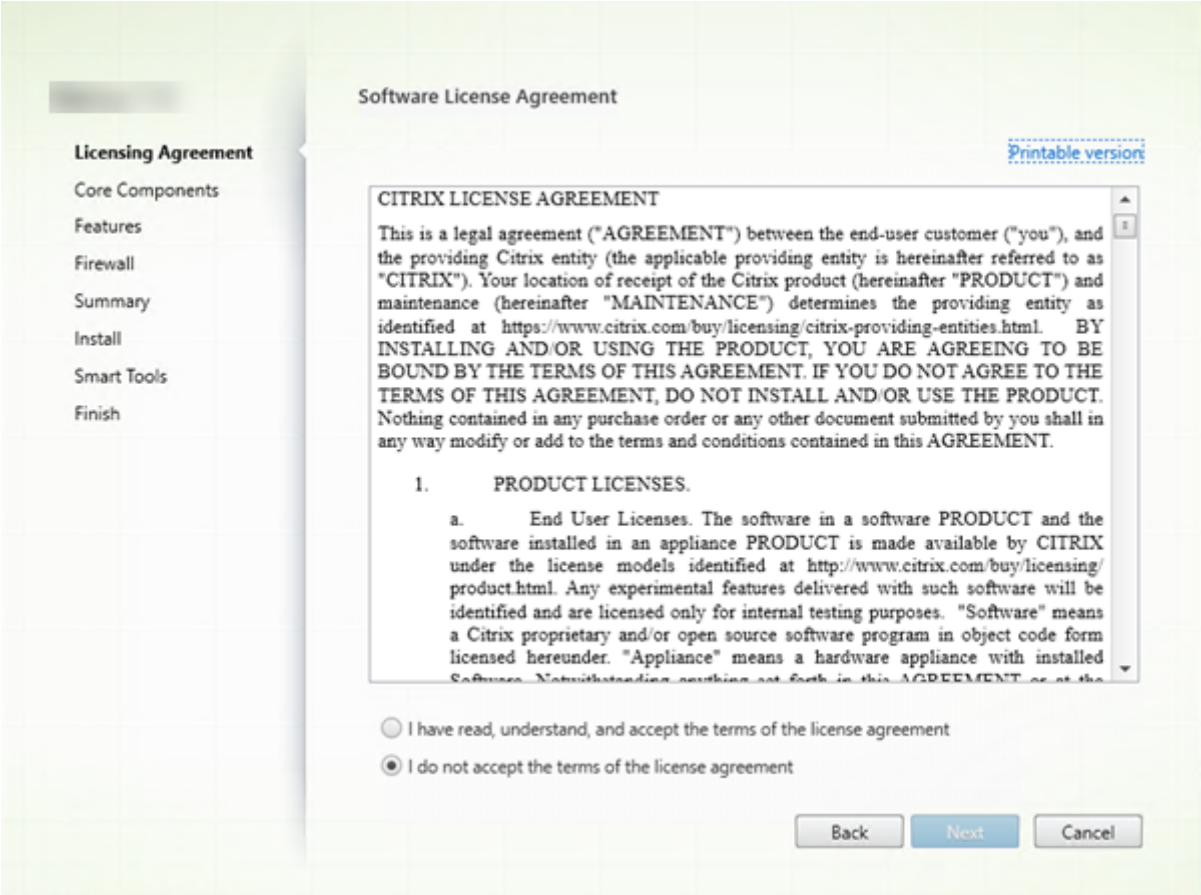
If you're just getting started, select **Delivery Controller**. (On a later page, you select the specific components to install on this machine.)

If you've already installed a Controller (on this machine or another) and want to install another component, select the component from the **Extend Deployment** section.

Command-line option: `/components`

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

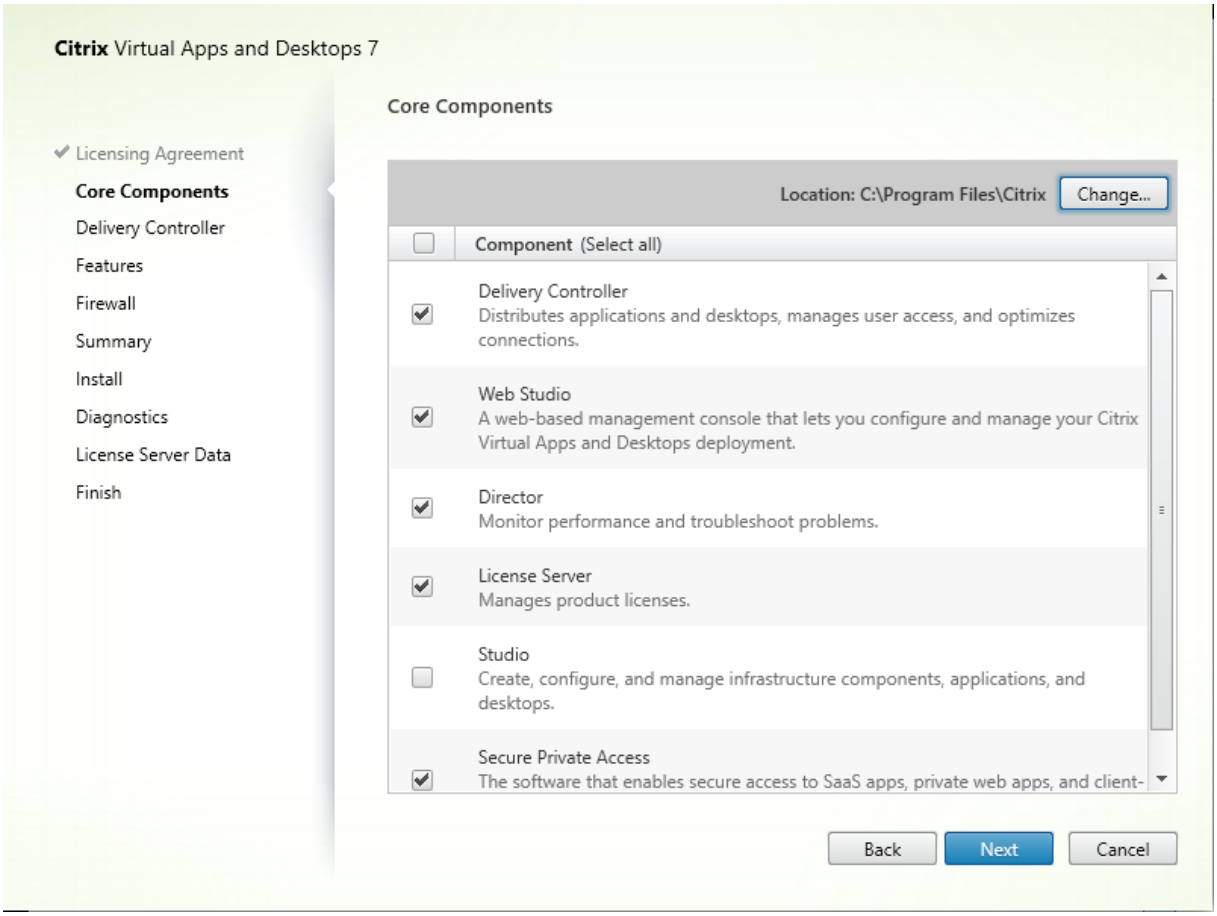
Step 4. Read and accept the license agreement



On the **Licensing Agreement** page, after you read the license agreement, indicate that you have read and accepted it. Then click **Next**.

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

Step 5. Select the components to install and the installation location



On the **Core components** page:

- **Location:** By default, components are installed in `C:\Program Files\Citrix`. The default is fine for most deployments. If you specify a different location, it must have execute permissions for the network service.
- **Components:** By default, the check boxes for all core components are selected. Installing all of the core components on one server is fine for proof of concept, test, or small production deployments. For larger production environments, Citrix recommends installing Director, StoreFront, Secure Private Access and the License Server on separate servers.

  > **Note:**
  >
  > If you're installing components on more than one server, install the Citrix License Server and licenses first, before installing other components on other servers. For guidance, see the Automatic installation section of the Licensing Guide for Citrix Virtual Apps and Desktops.

  An icon alerts you when you choose not to install a required core component on this machine.

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

That alert reminds you to install that component, although not necessarily on this machine.

Click **Next**.

Command-line options: `/installdir`, `/components`, `/exclude`

Hardware check

When you install or upgrade a Delivery Controller, the hardware is checked. The installer alerts you if the machine has less than the recommended amount of RAM (5 GB), which can affect site stability. For more information, see Hardware requirements.

Graphical interface: A dialog box appears.

- Recommended: Click **Cancel** to stop the installation. Add more RAM to the machine and then start the installation again.
- Alternatively, click **Next** to continue with the installation. The site might have stability issues.

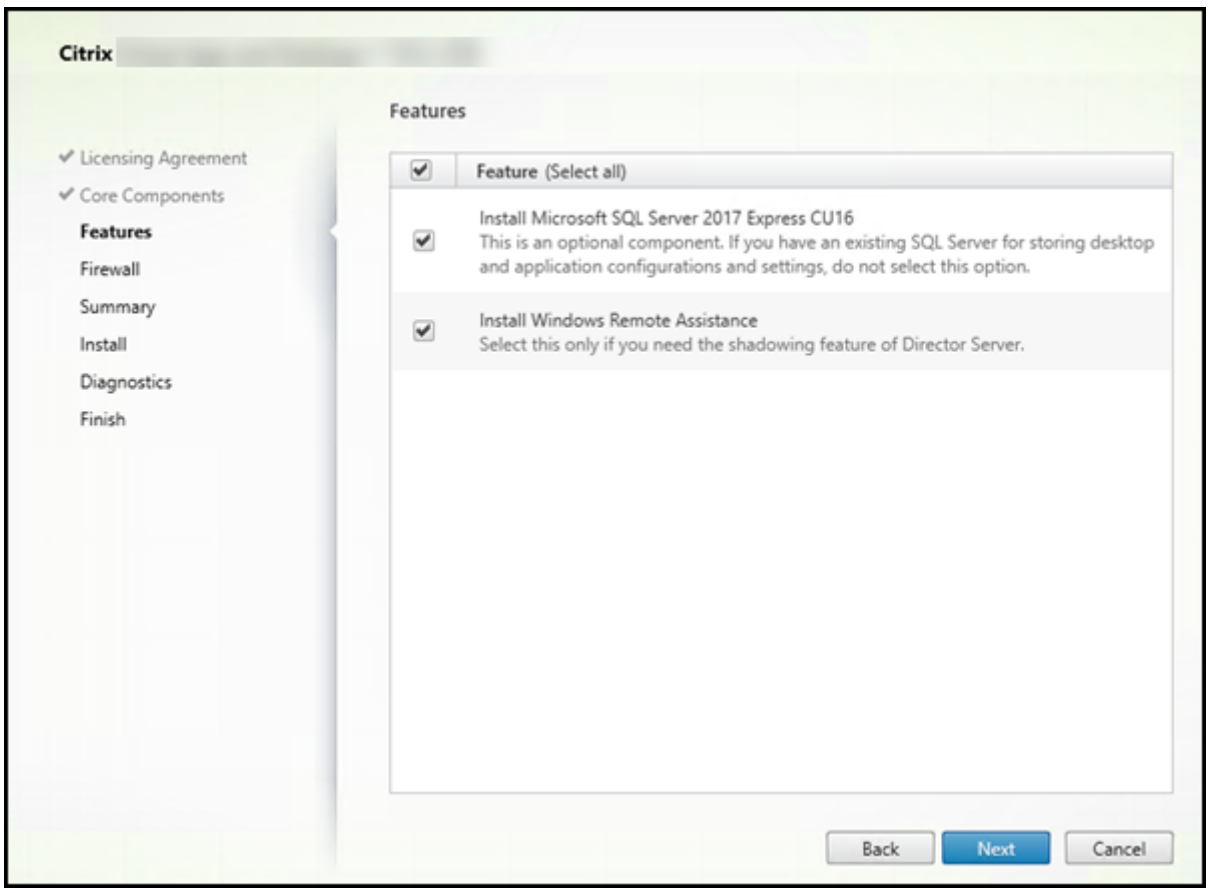
Command-line interface: The install/upgrade ends. The install logs contain a message that describes what was found and the available options.

- Recommended: Add more RAM to the machine and then run the command again.
- Alternatively, run the command again with the `/ignore_hw_check_failure` option to override the warning. Your site might have stability issues.

When upgrading, you're also notified if the OS or SQL Server version is no longer supported. See Upgrade a deployment.

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

Step 6. Enable or disable features



On the **Features** page:

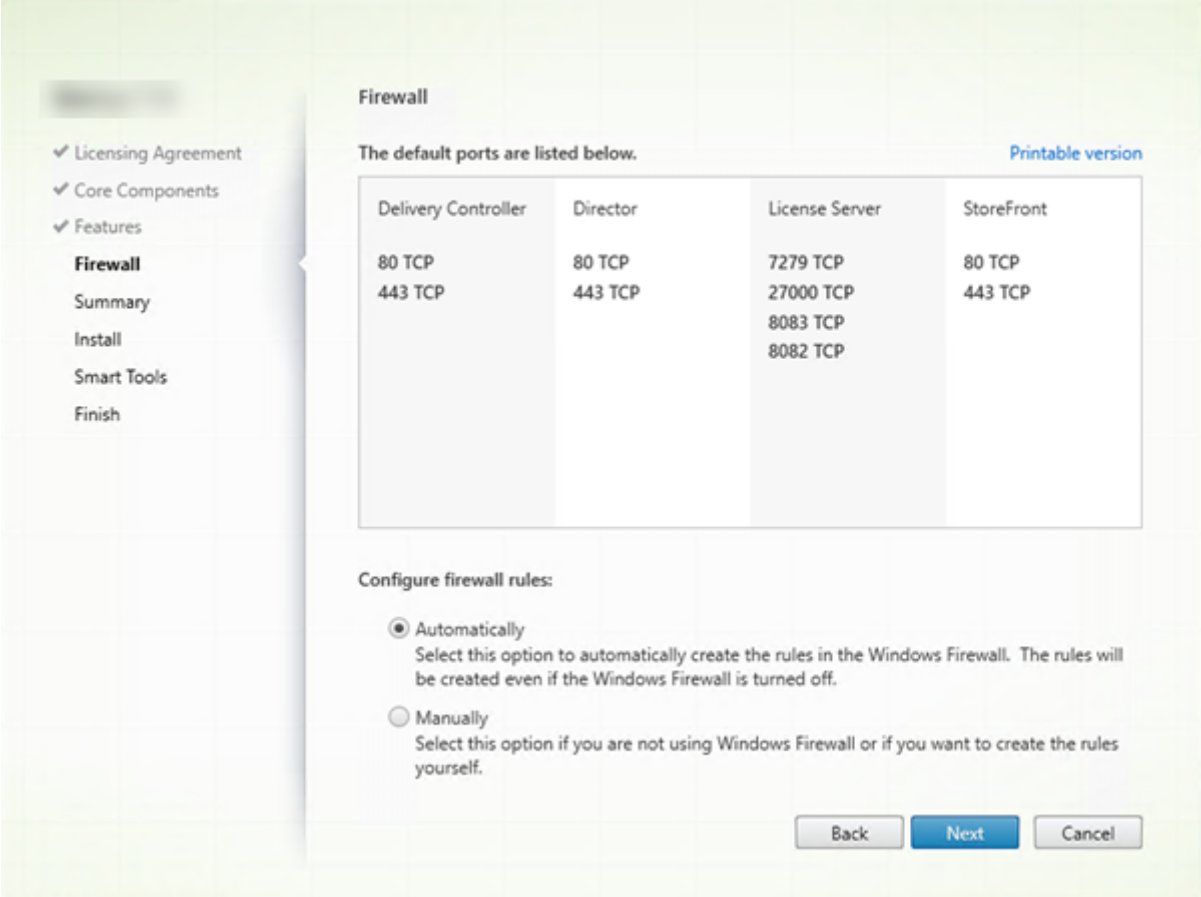
- Choose whether to install Microsoft SQL Server Express for use as the site database. By default, this selection is enabled. If you're not familiar with the Citrix Virtual Apps and Desktops databases, review Databases.
- When you install Director, Windows Remote Assistance is installed automatically. You choose whether to enable shadowing in Windows Remote Assistance for use with Director user shadowing. Enabling shadowing opens TCP port 3389. By default, this feature is enabled. The default setting is fine for most deployments. This feature appears only when you are installing Director.

Click **Next**.

Command-line options: `/nosql` (to prevent installation), `/no_remote_assistance` (to prevent enabling)

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

Step 7. Open Windows firewall ports



By default, the ports on the **Firewall** page are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. The default setting is fine for most deployments. For port information, see Network ports.

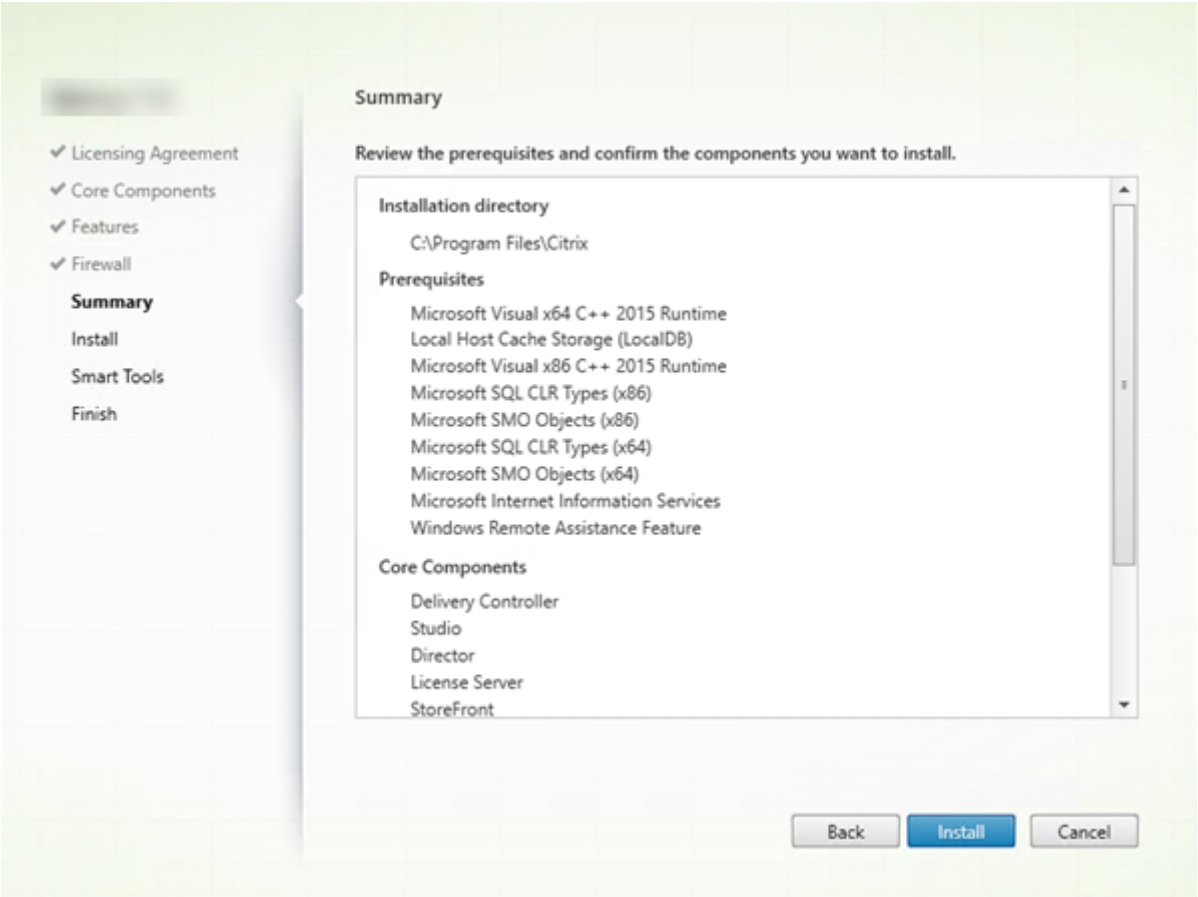
Click **Next**.

(The graphic shows the port lists when you install all the core components on this machine. That type of installation is usually for test deployments only.)

Command-line option: `/configure_firewall`

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

Step 8. Review prerequisites and confirm installation

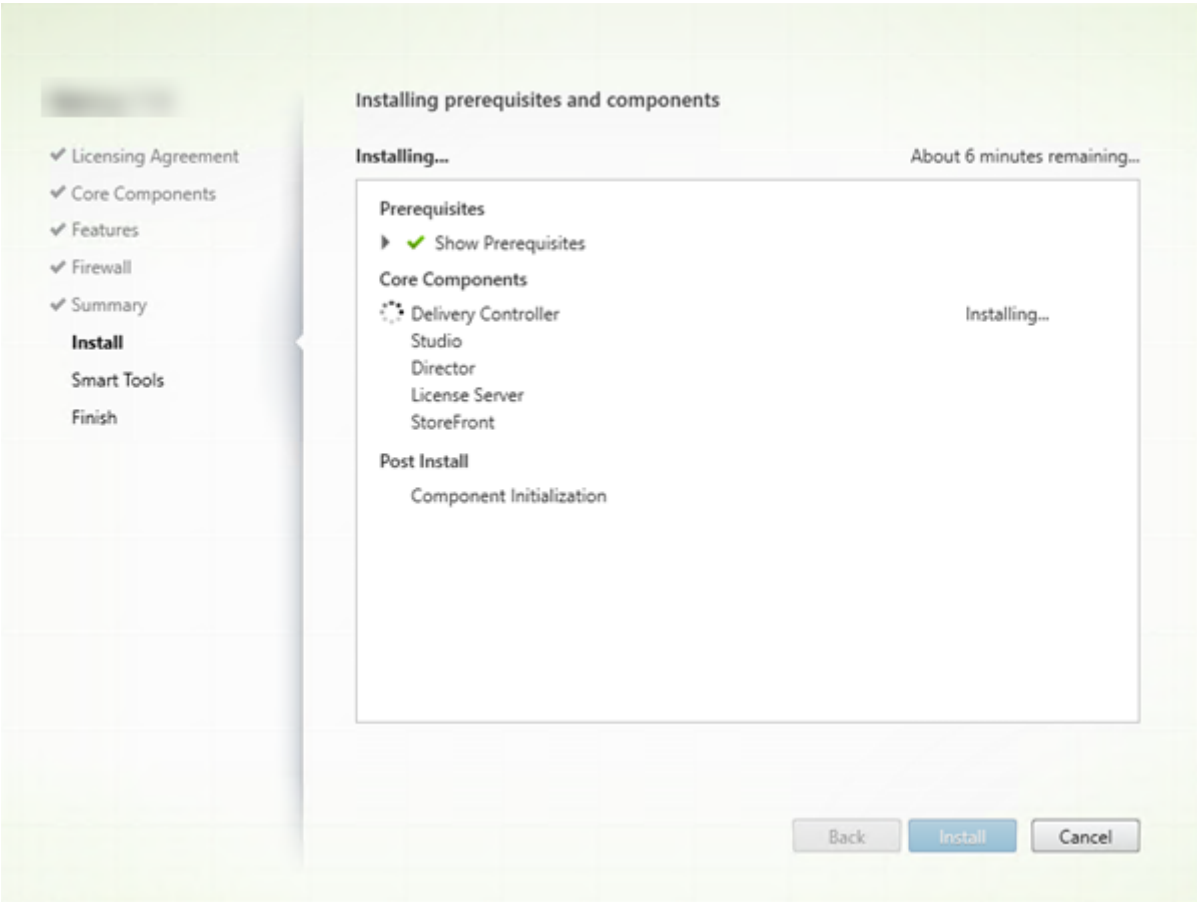


The **Summary** page lists what will be installed. Use the **Back** button to return to earlier wizard pages and change selections, if needed.

When you're ready, click **Install**.

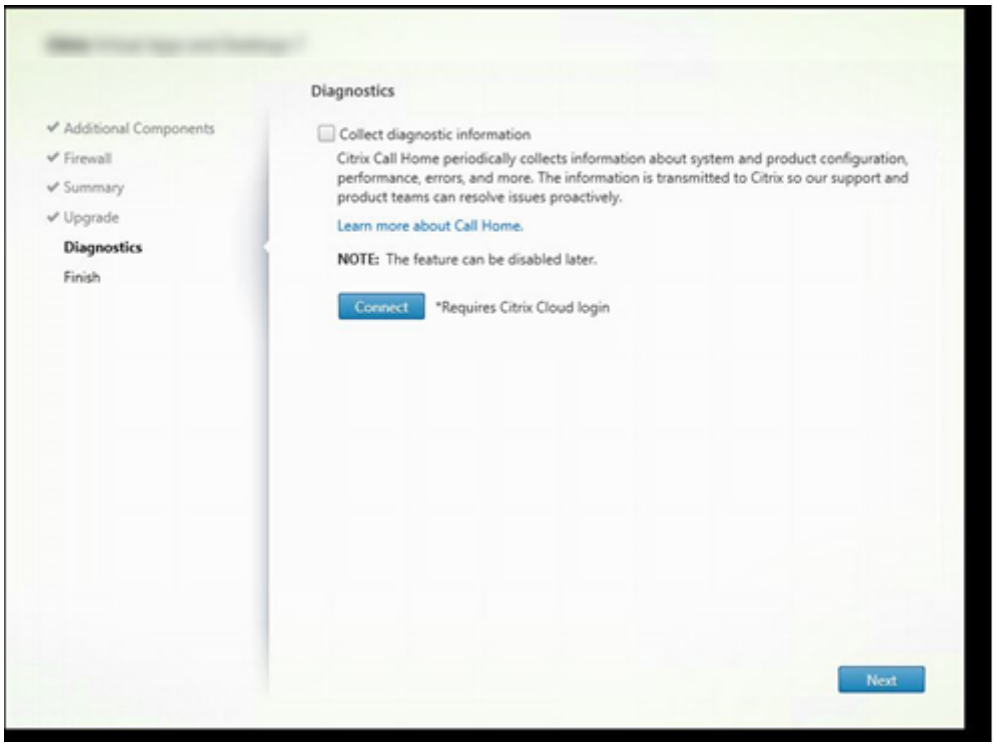
The display shows the progress of the installation:

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



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

Step 9. Sharing diagnostics information with Cloud Software Group



On the **Diagnostics** page, choose whether to participate in Citrix Call Home.

This page appears when installing a Delivery Controller using the graphical interface. When you install StoreFront (but not a Controller), the wizard displays this page. When you install other core components (but not a Controller or StoreFront), the wizard does not display this page.

During an upgrade, this page does not appear if Call Home is already enabled or if the installer encounters an error related to the Citrix Telemetry Service.

If you choose to participate (the default), click **Connect**. When prompted, enter your Citrix account credentials. You can change your enrollment choice later, after installation.

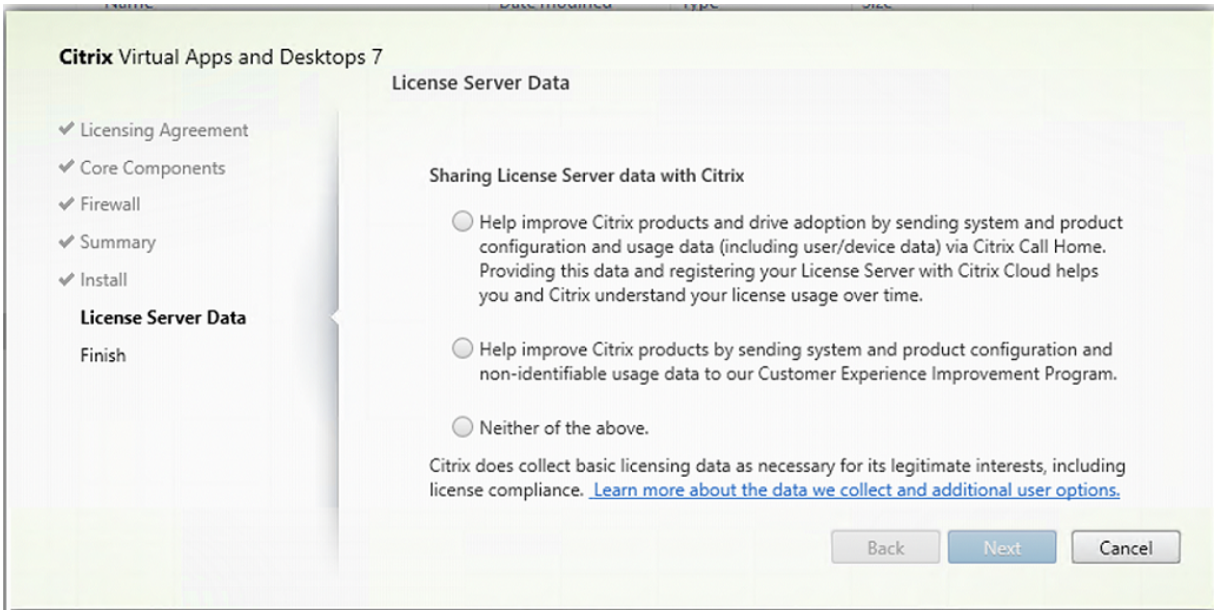
After your credentials are validated (or if you choose not to participate), click **Next**.

If you click **Connect** on the **Diagnostics** page without first selecting **Collect diagnostic information**, after you close the **Connect to Citrix Insight Services** dialog the **Next** button is disabled. You cannot move to the next page. To reenable the **Next** button, select and immediately deselect **Collect diagnostic information**.

For more information, see Call Home.

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

Step 10. Sharing License Server data with Cloud Software Group



On the **License Server Data** page, we request that you share either Call Home data or Customer Experience Improvement Program (CEIP) data to assist us. In addition, Cloud Software Group also requires the collection of basic licensing data, including license compliance, as necessary for its legitimate interests.

The **License Server Data** page appears when you have installed License Server:

- As a standalone.
- As a core component, during installation of a Delivery Controller.

During an upgrade, this page does not appear if the configuration is already set in the `/CITRIX.opt:` file.

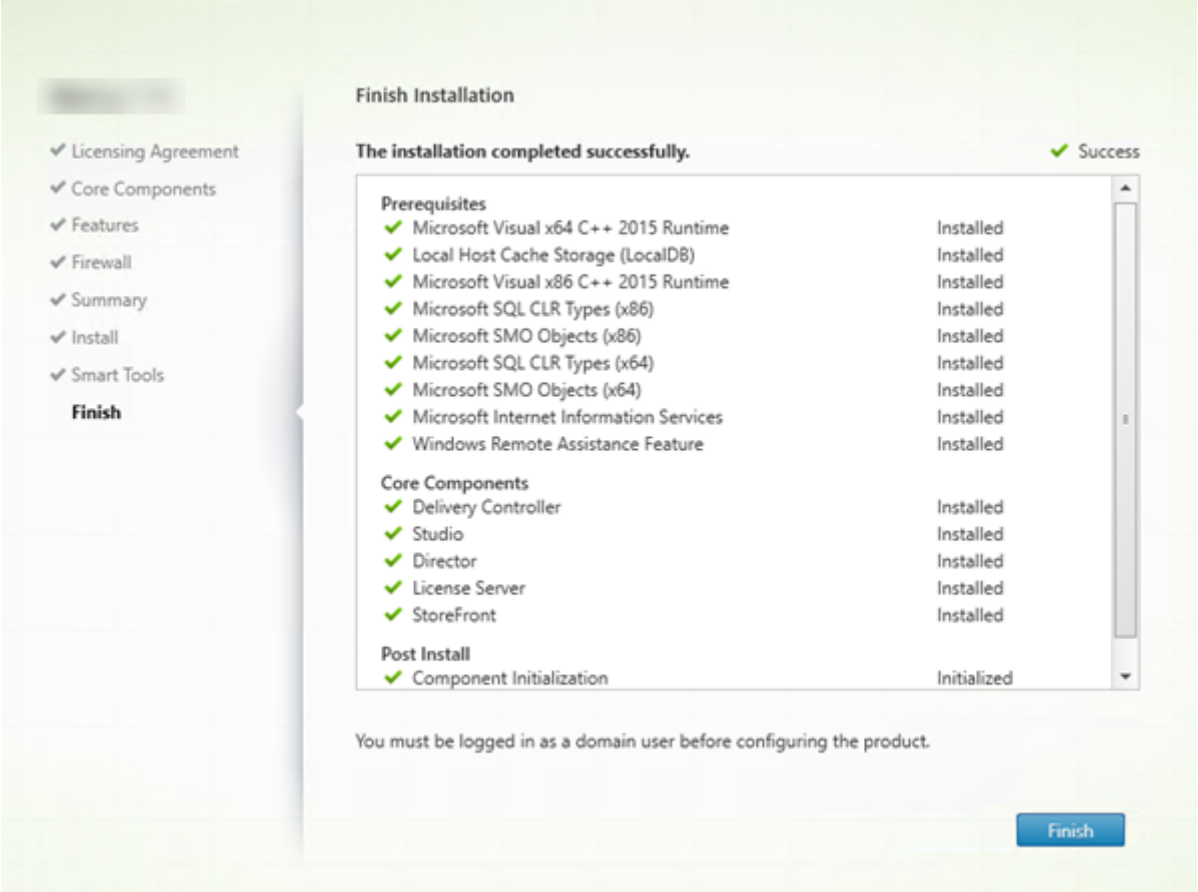
License Server monitors several types of user data, such as licensing data, Call Home data and CEIP data. To enable Call Home data and CEIP data collection, you must choose to participate (opt in).

For more information about how to enable Call Home and CEIP data collection when installing by using the command line, see Command line options for installing core components.

For more information about Cloud Software Group licensing data collection, see Citrix Licensing data collection programs.

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

Step 11. Finish this installation



The **Finish** page contains green check marks for all prerequisites and components that installed and initialized successfully.

Click **Finish**.

Step 12. Install remaining core components on other machines

If you installed all the core components on one machine, continue with Next steps. Otherwise, run the installer on other machines to install other components. You can also install more Controllers on other servers.

Next steps

After you install all the required components, use Studio to create a site.

After creating the site, install VDAs.

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

At any time, you can use the full-product installer to extend your deployment with the following components:

- **Universal Print Server server component:** Launch the installer on your print server.

  1. Select **Universal Print Server** in the **Extend Deployment** section.
  2. Accept the license agreement.
  3. On the **Firewall** page, by default, TCP ports 7229 and 8080 are opened in the firewall if the Windows Firewall Service is running, even if the firewall is not enabled. You can disable that default action if you want to open the ports manually.

  To install this component from the command line, see Command-line options for installing a Universal Print Server.

- Federated Authentication Service.
- Session Recording.
- Workspace Environment Management.

Install using the command line

January 12, 2026

> **Important:**
>
> - If you're upgrading, and your current version uses or has the Personal vDisk or AppDisks software installed, see Removing PvD, AppDisks, and unsupported hosts.
> - Citrix collects basic licensing data as necessary for its legitimate interests, including licensing compliance. For more information, see Citrix Licensing Data.

Introduction

This article applies to installing components on machines with Windows operating systems. For information about VDAs for Linux operating systems, see Linux Virtual Delivery Agents.

This article describes how to issue product installation commands. Before beginning any installation, review Prepare to install. That article includes descriptions of the available installers.

To see command execution progress and return values, you must be the original administrator or use **Run as administrator**. For more information, see the Microsoft command documentation.

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

As a complement to using the installation commands directly, sample scripts are provided on the product ISO that install, upgrade, or remove VDAs on machines in Active Directory. For details, see Install VDAs using scripts.

If you attempt to install or upgrade on a Windows OS version that is not supported for this Citrix Virtual Apps and Desktops version, a message guides you to information about your options. See Earlier operating systems.

For information about how Citrix reports the results of component installations, see Citrix installation return codes.

Use the full-product installer

To access the full product installer's command-line interface:

1. Download the product package from Citrix. Citrix account credentials are required to access the download site.
2. Unzip the file. Optionally, burn a DVD of the ISO file.
3. Log on to the server where you are installing the components, using a local administrator account.
4. Insert the DVD in the drive or mount the ISO file.
5. From the `\x64\XenDesktop Setup` directory on the media, run the appropriate command.

   To install core components: Run `XenDesktopServerSetup.exe`, with the options listed in Command-line options for installing core components.

   To install a VDA: Run `XenDesktopVDASetup.exe` with the options listed in Command-line options for installing a VDA.

   To install StoreFront: Run `CitrixStoreFront-x64.exe` in the `x64 > StoreFront` folder on the installation media.

   To install the Universal Print Server: Follow the guidance in Command-line options for installing a Universal Print Server.

   To install the Federated Authentication Service: Citrix recommends using the graphical interface.

   To install Session Recording: Follow the guidance in Session Recording.

   To install Workspace Environment Management: Follow the guidance in Workspace Environment Management.

   To install Secure Private Access: Run `XenDesktopSPASetup.exe` in the `x64 > XenDesktop` Setup folder on the installation media. Follow the guidance in Command-line options for installing a Secure Private Access.

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

Command-line options for installing core components

The following parameter options are valid when installing core components with the `XenDesktopServerSetup.exe` command. For more detail about options, see Install core components.

> **Note:**
>
> - Do not use `/exclude` while using command-line options for installing core components.
> - If you upgrade one component using `/components`, then other components might also be upgraded. This is to avoid potential compatibility issues between different components.
> - If you want to upgrade only one component, use the individual installer of that component. See Upgrade a deployment.

- **/ceipoptin** *ceipoptin* [,*ceipoptin*] …

  Enables collection of Call Home data and Customer Experience Improvement Program (CEIP) data. Valid values are:

  - `DIAGNOSTIC`: Choose this value to enable Citrix Licensing to collect Call Home data.
  - `ANONYMOUS`: Choose this value to enable Citrix Licensing to collect unidentified CEIP data (which does not identify users).
  - `NONE`: Choose this value to disable Citrix Licensing collection of CEIP data.

  For more information about Call Home data collection, see Citrix Licensing Call Home.

  For more details about CEIP data collection, see Citrix Licensing Customer Experience Improvement Program.

  For more details about CEIP data, see Citrix Licensing CEIP data elements.

  For more details about License Server licensing data, see Citrix Licensing Data.

- **/components** *component* [,*component*] …

  Comma-separated list of components to install or remove. Valid values are:

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio
  - `WEBSTUDIO`: Web Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix License Server
  - `SECUREPRIVATEACCESS`: Secure Private Access

To install only the VDA and exclude the installation of other Citrix components, specify /components vda.

This option is not valid when using the VDAWorkstationCoreSetup_xxxx.exe installer. That installer cannot install the Citrix Workspace app or other Citrix components.

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

If this option is omitted, all components are installed (or removed, if the /`remove` option is also specified).

(In releases before 2003, valid values included `STOREFRONT`. For version 2003 and later, use the dedicated StoreFront installation command mentioned in Use the full-product installer).

- **/onlyprereqs**

  Only the prerequisites for the selected components will be installed. No Citrix product components will be installed.

- **/configure_firewall**

  Opens all ports in the Windows firewall used by the components being installed, if the Windows Firewall Service is running, even if the firewall is not enabled. If you are using a third-party firewall or no firewall, you must manually open the ports.

- **/disableexperiencemetrics**

  Prevents automatic upload of analytics collected during installation, upgrade, or removal to Citrix.

- **/help** or **/h**

  Displays command help.

- **/ignore_hw_check_failure**

  Allows the Delivery Controller installation or upgrade to continue, even if the hardware checks fail (for example, due to insufficient RAM). For more information, see Hardware check.

- **/ignore_site_test_failure**

  Valid only during Controller upgrade. Usually, any site test failures are ignored and the upgrade proceeds. If omitted (or set to false), any site test failure causes the installer to fail, without performing the upgrade. Default = false

  During an upgrade, this option is ignored if an unsupported SQL Server version is detected. For details, see SQL Server version check.

- **/installdir *directory***

  Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.

- **/logpath *path***

  Log file location. The specified folder must exist. The installer does not create it. Default = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Valid only when installing the Director. Disables the user shadowing feature that uses Windows Remote Assistance.

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

- **/noreboot**

  Prevents a restart after installation. (For most core components, a restart is not enabled by default.)

- **/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.

- **/nosql**

  Prevents the installation of Microsoft SQL Server Express on the server where you are installing the Controller. If this option is omitted, SQL Server Express is installed for use as the site database.

  This option does not affect the installation of SQL Server Express LocalDB used for Local Host Cache.

- **/quiet** or **/passive**

  No user interface appears during the installation. The only evidence of the installation process is in Windows Task Manager. If this option is omitted, the graphical interface launches.

- **/remove**

  Removes the core components specified with the `/components` option.

- **/removeall**

  Removes all installed core components.

- **/sendexperiencemetrics**

  Automatically sends analytics collected during the installation, upgrade, or removal to Citrix. If this option is omitted (or `/disableexperiencemetrics` is specified), the analytics are collected locally, but not sent automatically.

- **/tempdir** *directory*

  Directory that holds temporary files during installation. Default = c:\Windows\Temp.

- **/xenapp**

  Installs Citrix Virtual Apps. If this option is omitted, Citrix Virtual Apps and Desktops™ is installed.

Examples of installing core components

The following command installs a Delivery Controller™, Studio, Citrix Licensing, and SQL Server Express on a server. Firewall ports required for component communications are opened automati-

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

cally.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller
,desktopstudio,licenseserver /configure_firewall
```

The following command installs a Citrix Virtual Apps™ Controller, Studio, and SQL Server Express on the server. Firewall ports required for component communication are opened automatically.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components
controller,desktopstudio /configure_firewall
```

The following command installs a Delivery Controller, Secure Private Access, and SQL Server Express on a server. Firewall ports required for component communication are opened automatically.

```
\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components
controller,secureprivateaccess /configure_firewall
```

If you upgrade from Citrix Virtual Apps and Desktops version 2407 to 2411 or later, or perform a fresh installation of version 2411 or later, update the License Server to the latest version (version 11.2.17 build 51000) as the first step. Then, upgrade the Delivery Controller. Failing to do so results in the failure of command-line installations and upgrade. Run the following commands to upgrade the License server and components such as Delivery controller, Web Studio, and Citrix Director (assuming you are inside the \x64 folder in the mounted ISO).

1. Run the following:

   ```
   1 \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   If you have copied the Licensing binaries to any of the local drives, then run the following command:

   ```
   1 \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. Run the following:

   ```
   1 \x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components "
       CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

Use a standalone VDA installer

Citrix account credentials are required to access the download site. You must either have elevated administrative privileges before starting the installation, or use **Run as administrator**.

1. Download the appropriate package from Citrix:

   - Multi-session OS Virtual Delivery Agent: `VDAServerSetup_xxxx.exe`
   - Single-session OS Virtual Delivery Agent: `VDAWorkstationSetup_xxxx.exe`

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

- Single-session OS Core Services Virtual Delivery Agent: `VDAWorkstationCoreSetup_xxxx.exe`

2. Either extract the files from the package to an existing directory first and then run the installation command, or simply run the package.

   To extract the files before installing them, use `/extract` with the absolute path, for example `C:\YourExtractFolder\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`

   To run the downloaded package, run its name: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, or `VDAWorkstationCoreSetup.exe`. Use the valid options listed in this article.

If you are familiar with the full product installer:

- Run the standalone `VDAServerSetup.exe` or `VDAWorkstationSetup.exe` installer as if it was the `XenDesktopVdaSetup.exe` command in everything except its name.
- The `VDAWorkstationCoreSetup.exe` installer is different, because it supports a subset of the options available to the other installers.

Comma-separated list of components to install or remove. Valid values are:

- `VDA`: Virtual Delivery Agent
- `CSA`: Citrix Secure Access™ Client
- `PLUGINS`: Citrix Workspace™ app for Windows
- `UPL`: Citrix User Personalization Layer

To install the VDA and Citrix Workspace app for Windows, specify /components vda,plugins or do not specify any components at all.

Starting with this version, Citrix Device Trust, Citrix uberAgent, and Citrix Workspace Environment Management™ (WEM) Agent are integrated into the default VDA installation. These components are silently installed as part of the VDA setup and are no longer managed as separate components.

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

> **Note:**
>
> If an existing standalone version of Citrix uberAgent® is detected in the environment, it will not be installed, upgraded, or uninstalled by the installer.

To install only the VDA and exclude the installation of other Citrix components, specify `/components vda`.

This option is not valid when using the VDAWorkstationCoreSetup_xxxx.exe installer. That installer cannot install the Citrix Workspace app or other Citrix components.

Command-line options for installing a VDA

The following options are valid with one or more of the following commands (installers): `VDAServerSetup_xxxx.exe`, `VDAWorkstationSetup_xxxx.exe`, and `VDAWorkstationCoreSetup.exe`.

For more details about options, see Install VDAs.

- **/components** *component*[,*component*]

  Comma-separated list of components to install or remove. Valid values are:

  - `VDA`: Virtual Delivery Agent
  - `PLUGINS`: Citrix Workspace app for Windows
  - `CSA`: Citrix Secure Access Client
  - `UPL`: Citrix User Personalization Layer

To install the VDA and Citrix Workspace app for Windows, specify `/components vda, plugins, CSA, UPL` or do not specify any components at all. If no components are specified, only the VDA will be installed by default.

To install only the VDA and exclude the installation of Citrix Workspace app, specify `/components vda`.

This option is not valid when using the `VDAWorkstationCoreSetup_xxxx.exe` installer. That installer cannot install the Citrix Workspace app.

- **/onlyprereqs**

  Only the prerequisites for the selected components will be installed. No Citrix product components will be installed.

- **/controllers** "*controller* [*controller*]"

  Space-separated FQDNs of Controllers with which the VDA can communicate, enclosed in straight quotation marks. Do not specify both the `/site_guid` and `/controllers` options.

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

- **/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 uses, specify the `/enable_hdx_udp_ports` option, in addition to this `/enable_hdx_ports` option.

- **/enable_hdx_udp_ports**

  Opens UDP ports in the Windows firewall that HDX adaptive transport uses, 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 extra ports that the VDA uses, specify the `/enable_hdx_ports` option, in addition to this `/enable_hdx_udp_ports` option.

- **/enable_hdx_tls_dtls**

  Opens TCP and UDP port 443 for HDX™ Direct V1.

- **/enable_real_time_transport**

  Enables or disables the use of UDP for audio packets (RealTime Audio Transport for audio). Enabling this feature can improve audio performance. Include the `/enable_hdx_ports` 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 Director. 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 retain the restore point, even though it was not used.

  For details, see Restore on install or upgrade failure.

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

- **/ENABLE_SECURE_DEFAULTS**

  Changes the default setting for various features from enabled to disabled for a more secure out-of-box configuration. The relevant features are: client drive redirection, special folder redirection, drag and drop, client TWAIN device redirection, Client USB Plug and Play device redirection, client printer redirection, client clipboard redirection, and client microphone redirection.

- **/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.

- **/SKIPHDXDRIVERCHECK**

  Skips the checking of the HDX™ Drivers to the VDA Meta-installer.

- **/exclude** "*component*"[,"*component*"]

  Prevents the installation of one or more comma-separated optional components, each enclosed in straight quotation marks. For example, installing or upgrading a VDA on an image that is not managed by MCS does not require the Machine Identity Service component. Valid values are as follows:

Multi-session OS	Single-session OS	Single-session OS Core Services
Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in
Citrix Backup and Restore	Citrix Backup and Restore	Citrix Browser Content Redirection
Citrix deviceTRUST	Citrix deviceTRUST	Citrix deviceTRUST
uberAgent	uberAgent	uberAgent
Citrix Secure Access Client	Citrix Secure Access Client	Citrix Secure Access Client
Citrix Workspace Environment Management Agent	Citrix Workspace Environment Management Agent	Citrix Workspace Environment Management Agent
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization **for** App-V - VDA

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

Multi-session OS	Single-session OS	Single-session OS Core Services
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Universal Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	
Machine Identity Service	Machine Identity Service	
Machine Management Provider	Machine Management Provider	
VDA Monitor Plug-in	User Personalization Layer	
VDA WMI Proxy Plug-in	VDA Monitor Plug-in	
	VDA WMI Proxy Plug-in	
Citrix App Protection Component	Citrix App Protection Component	Citrix App Protection Component

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

Multi-session OS	Single-session OS	Single-session OS Core Services
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`

Excluding Citrix Profile Management from the installation (`/exclude "Citrix Profile Management"`) affects monitoring and troubleshooting of VDAs with Citrix Director. 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 displays data only for machines that have Profile Management installed.

Even if you are using a third-party user 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 specify both `/exclude` and `/includeadditional` with the same component name, that component is not 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. This option can be helpful when you are creating a Remote PC Access deployment, and want to install other components that are not included by default. Valid values are as follows:

Multi-session OS	Single-session OS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`

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

Multi-session OS	Single-session OS
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

If you specify both `/exclude` and `/includeadditional` with the same component name, that component is not installed.

- **/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 is not available in the graphical interface.

- **/masterimage**

  Valid only when installing a VDA on a VM. Sets up the VDA as an image to be used to create other machines. This option is equivalent to `/mastermcsimage`.

  This option is not valid when using the `VDAWorkstationCoreSetup_xxxx.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) to provision VMs.

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

- **/websockettoken** *WebSocketToken*

  Creates a Web Socket VDA. The WebSocketToken is for the token that is required.

- **/websockettokenfile** *FileContainingWebSockToken*

  Creates a Web Socket VDA. The *FileContainingWebSockToken* is for the file that contains the token that is required.

- **/websockettokenstdin** <*WebSocketToken*

  Creates a Web Socket VDA. The <*WebSocketToken* is for the token that is required that is passed in by STDIN.

- **/no_mediafoundation_ack**

  Acknowledges that Microsoft Media Foundation is not installed, and several HDX multimedia features will not be installed and will not work. If this option is omitted and Media Foundation is not installed, the VDA installation exits since the pre-conditions are not met. Most supported Windows editions come with Media Foundation already installed, except N editions. If you enable Windows Features > Media Features *manually*, the registry key sought by the Citrix Meta Installer may not have a set value. Check the `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` registry key before starting the install process to confirm the value exists and is not empty.

- **/nodesktopexperience**

  The Enhanced Desktop Experience feature is no longer available. This option (and policy setting) is ignored, if specified.

  Valid only when installing a VDA for multi-session OS. Prevents enabling of the Enhanced Desktop Experience feature. This feature is also controlled with the Enhanced Desktop Experience Citrix policy setting.

- **/noreboot**

  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.

- **/physicalmachine**

  Use this argument along with `/remotepc` for RemotePC installation. Otherwise the VDA might not behave as expected in certain user scenarios.

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

- **/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*"

  If you plan to use the Rendezvous V2 protocol with services such as Gateway Service in your environment and have a non-transparent proxy in your network for outbound connections, specify the proxy here. Only HTTP proxies are supported. The address or PAC file path of the proxy for use with the Rendezvous protocol. This command line automatically installs the Citrix Rendezvous V2 as if /includeadditional "Citrix Rendezvous V2"was used. 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). Excludes installation of any additional components (see component lists with /exclude and /includeadditional options).

  This option is not valid when using the VDAWorkstationCoreSetup.exe installer. That installer automatically excludes installation of these components.

  /remotepc is not compatible with the /servervdi option.

- **/remove**

  Removes the components specified with the /components option.

- **/remove_appdisk_ack**

  Authorizes the VDA installer to uninstall the AppDisks™ VDA plug-in if it's installed.

- **/remove_pvd_ack**

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

Authorizes the VDA installer to uninstall Personal vDisk if it's installed.

- **/removeall**

  Removes the VDA. It does not remove the Citrix Workspace app (if installed).

- **/REMOVEALLWITHCWA**

  Removes CWA along with the VDA.

- **/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 VDA for single-session OS on a supported Windows multi-session machine. Omit this option when installing a VDA for multi-session OS on a Windows multi-session machine.

  Before using this option, see Server VDI.

  Use this option only with the full-product VDA installer.

- **/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.

Examples of installing a VDA

Install a VDA with the full-product installer:

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

The following command installs a VDA for single-session OS and Citrix Workspace app to the default location on a VM. This VDA will be used as an image and use MCS to provision VMs. The VDA will register initially with the Controller on the server named `Contr-Main` in the domain `mydomain`. The VDA will use user personalization layer and Windows Remote Assistance.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda
,plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports
 /includeadditional "user personalization layer"/mastermcsimage /
enable_remote_assistance
```

Install a single-session OS VDA with the VDAWorkstationCoreSetup standalone installer:

The following command installs a Core Services VDA on a single-session OS for use in a Remote PC Access or VDI deployment. Citrix Workspace app and other non-core services are not installed. The address of a Controller is specified, and ports in the Windows Firewall Service will be opened automatically. The administrator will handle restarts.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

Customize a VDA

After you install a VDA, you can customize several settings. From the `\x64\XenDesktop Setup` directory on the product media, run `XenDesktopVdaSetup.exe`, using one or more of the following options, which are described in Command-line options for installing a VDA.

- `/reconfigure` (required when customizing a VDA)
- `/h` or `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Troubleshoot VDAs

- In the Studio display for a delivery group, the **Installed VDA version** entry in the **Details** pane might not be the version installed on the machines. The machine's Windows Programs and Features display shows the actual VDA version.
- After a VDA is installed, it cannot deliver apps or a desktop to users until it registers with a Delivery Controller.

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

To learn about VDA registration methods and how to troubleshoot registration issues, see VDA registration.

Command-line options for installing a Universal Print Server

The following option is valid with the `XenDesktopPrintServerSetup.exe` command.

- **/enable_upsserver_port**

When this option is not specified, the installer displays the **Firewall** page from the graphical interface. Select **Automatically** to have the installer automatically add the Windows firewall rules, or **Manually** to let the administrator manually configure the firewall.

After installing the software on your print servers, configure the Universal Print Server using the guidance in Citrix Universal Print Server (UPS).

Command-line options for installing a Secure Private Access

The following options are valid with both:

1. CVAD installer: `XenDesktopSPASetup.exe`
2. SPA on-prem installer: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Opens ports in the Windows firewall required by the Secure Private Access, 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.

- **/nosql**

  Prevents the installation of Microsoft SQL Server Express on the server where you are installing the Secure Private Access. If this option is omitted, SQL Server Express is installed for use as the site database.

- **/help or /h or /?**

  Displays command help

- **/noreboot**

  Prevents a restart after installation. Secure Private Access cannot be used until after a restart.

- **/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.

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

- **/remove**

  Removes the Secure Private Access.

For more details about the options, see Secure Private Access installer.

More information

For information about how Citrix reports the result of component installations, see Citrix installation return codes.

Install Web Studio

March 16, 2026

Introduction

Citrix Studio is a Windows-based management console that lets you configure and manage your Citrix Virtual Apps and Desktops deployment. Web Studio is the next generation of Citrix Studio —a web-based management console offering full feature parity with Citrix Studio. With the same look and feel as the Citrix DaaS Studio interface, Web Studio modernizes your management experience by providing a native web experience.

You can deploy Web Studio to any Windows server with Internet Information Service (IIS) installed. There are two deployment options:

- Installed on a dedicated server:

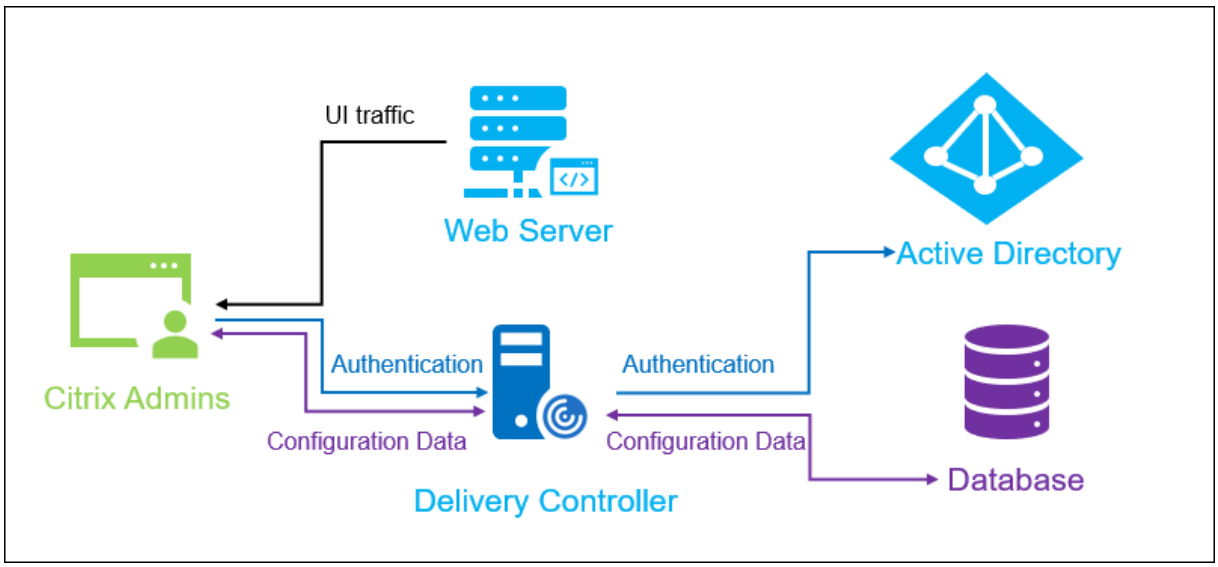
  For larger environments where performance and scalability are critical, we recommend installing Web Studio on a dedicated server. This server can optionally also host the Director.

- Integrated with a Delivery Controller™:

  For quick deployments and simpler environments, install Web Studio directly on a Delivery Controller. This approach is ideal for smaller deployments where minimizing administrative overhead is a priority.

The following diagram shows the Web Studio architecture:

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



A general workflow to get Web Studio up and running is as follows:

1. Install Web Studio.
2. Set up a site.
3. Add Delivery Controllers to Web Studio for management.
4. (Optional) Configure Web Studio as a proxy for Delivery Controllers
5. (Optional) Disable Pendo.
6. Sign in to Web Studio.

To set up a load-balanced Web Studio deployment, see this article.

New features available in Web Studio

See the What's new article.

System requirements

The following tables list the supported operating systems, browsers, display settings, and hardware requirements for installing and using Studio.

Supported operating systems

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

Operating system	Editions	Server Core support
Windows Server 2025	Standard, Datacenter	Yes
Windows Server 2022	Standard, Datacenter	Yes
Windows Server 2019	Standard, Datacenter	Yes
Windows Server 2016	Standard, Datacenter	Yes

Supported browsers

Browser	Minimum supported version
Microsoft Edge	92
Firefox ESR (Extended Support Release)	90
Google Chrome	92
Safari	14

Display requirements

Requirement	Value
Recommended screen resolution	1440 × 1024

Hardware requirements

Resource	Minimum requirement
Memory	1 GB RAM
Disk space	100 MB

Prerequisites

This release of Web Studio is compatible with Citrix Virtual Apps and Desktops™ 2212 deployments and later.

For deployments earlier than 2212, first upgrade to 2212 and then install Web Studio.

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

Known limitations

If you use Web Studio and Citrix Studio interchangeably, consider the following limitation: A template created in Web Studio is not shown in Citrix Studio, and vice versa. This is because Web Studio uses a database different from Citrix Studio to store templates. As a workaround, create a policy from a template in Web Studio and then create a template from this policy in Citrix Studio, and vice versa.

- To ensure a successful installation of Web Studio, do not change the default site name (**Default Web Site**) in Internet Information Services (IIS) Manager. Any changes to the default site name result in installation failures.

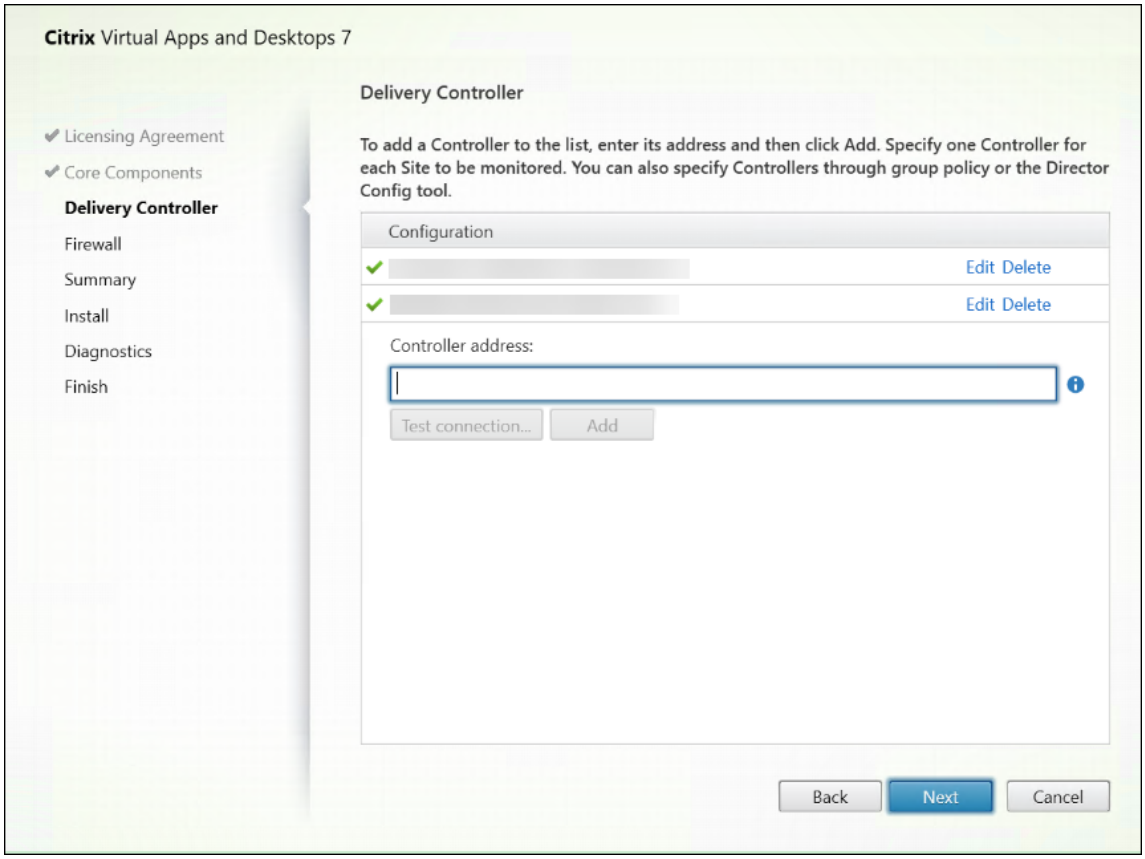
Install Web Studio

The following information is a supplement to the guidance in Install core components. To install Web Studio:

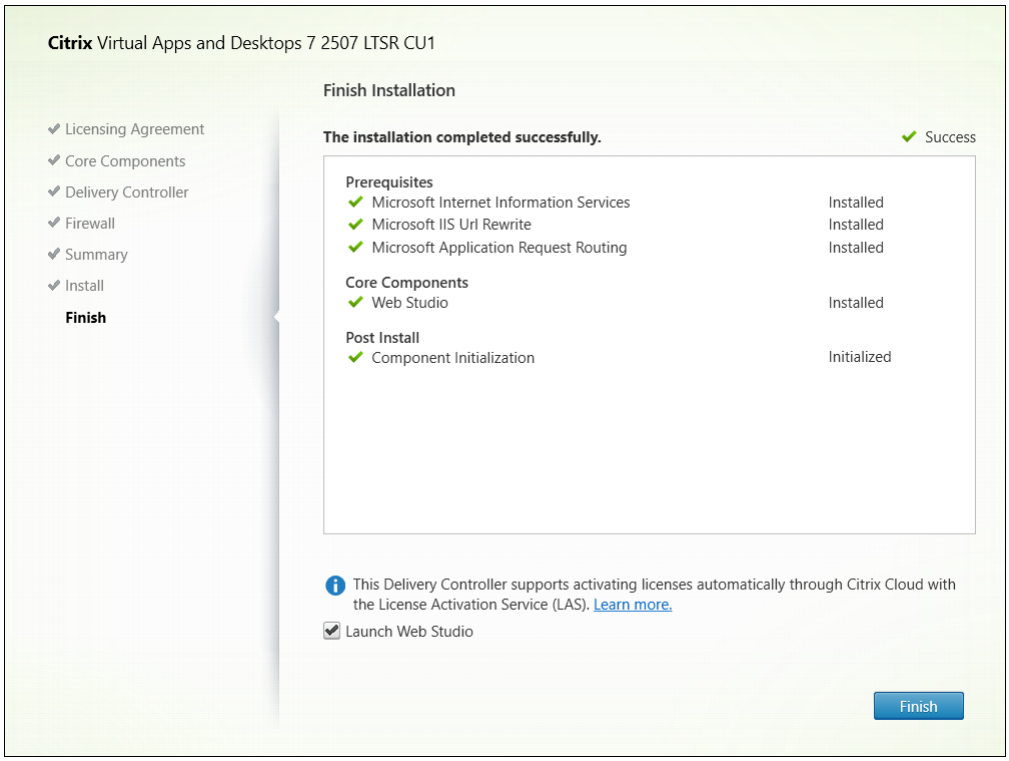
- Install Web Studio using the full product ISO installer for Citrix Virtual Apps and Desktops. The ISO installer checks for prerequisites, installs any missing components, sets up the Web Studio website (on the Delivery Controller if included in Delivery Controller installation), and performs basic configuration.
- If Web Studio was not included during installation, use the installer to add Web Studio.
- When installing Web Studio, you are prompted to type the FQDN of a Delivery Controller.

  > **Note:**
  >
  > - We recommend running Web Studio and Delivery Controllers on the same version to ensure full functionality.
  > - You can add more than one Delivery Controller. Web Studio attempts to connect to them in random order. If the Delivery Controller to which Web Studio is attempting to connect is unreachable, Web Studio automatically falls back to other Delivery Controllers.
  > - If Director was selected in **Core Components** and installed, the Delivery Controllers you add here are used for both Web Studio and Director.
  > - If the delivery controller is configured for TLS (recommended) then the entered FQDN must match the common name or a subject alternative name of the certificate installed on the delivery controller.

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



- On the **Finish** page, review the installed components and then click **Finish**.



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

> **Note:**
>
> You can also use the command line to install Web Studio. Example: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`. For more information, see Install using the command line.

Configure a certificate for TLS

By default, if IIS isn't already configured for HTTPS, the installer creates a self-signed certificate using the server's FQDN as the certificate's common name, and binds it to port 443. This behavior allows users to access Web Studio from the local machine, but users connecting from other machines see security warnings because the certificate isn't trusted. We recommend replacing this certificate with a certificate signed by an enterprise or public certificate authority (CA). For more information, see Enable TLS on web studio and Director. If a TLS certificate is already configured in IIS, the installer makes no changes.

> **Note:**
>
> To learn more about securing your Web Studio deployment, see Secure Web Studio deployment.

Set up a site

To set up your Citrix Virtual Apps and Desktops deployment (also known as a site), use the tool, Citrix Site Manager. The tool is installed automatically with a Delivery Controller.

To set up a site, follow these steps:

1. On a Delivery Controller, open the desktop Start menu, and then select **Citrix > Citrix Site Manager**.
2. In the Citrix Site Manager, select **Create a site**. The Site Setup wizard appears.
3. Create a site and configure its settings as follows:
   - On the **Introduction** page, type a name for the site.
   - The **Databases** page contains selections for setting up the site, monitoring, and configuration logging databases. For more information, see Step 3. Databases.
   - On the **Licensing** page, specify the License Server address and then indicate which license to use (install). For more information, see Step 4. Licensing.
4. On the **Summary** page, check all settings and click **Submit**.

   The IP address of this Controller is automatically added to the site.

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

> **Note:**
>
> The user who creates a site becomes a full administrator for it. For more information, see Delegated administration.

If you install a new Controller after creating a site, you must add the Controller to the site. Detailed steps are as follows:

1. Run Citrix Site Manager on this new Controller.
2. Select **Join an existing site**.
3. Type the address of a Controller that is already added to the site.
4. Click **Submit**.

Add Delivery Controllers to Web Studio for management

Use the Studio configuration tool to add the Delivery Controllers to Web Studio for management. This tool is available in the Web Studio installation folder.

By default, the tool is installed in the following default folder.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Suppose you want to configure the following two Delivery Controllers for the site that you want to manage with Web Studio: `ddc1.studio.local` and `ddc2.studio.local`. Run the following PowerShell command:

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **Note:**
>
> - The tool requires computer administrator permissions.
> - The Delivery Controller configuration changes might not take effect immediately due to cache settings on the IIS server. For immediate effect, go to the Web Studio server, open Internet Information Services (IIS) Manager, navigate to *Server_name* **> Sites > Default Web Site**, and select **Restart** in the Manage Website pane.
> - When you redeploy the Delivery Controllers with new FQDNs, update their FQDNs in Web Studio using `StudioConfig.exe` and in the `C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json` file. If you don't update the `manifest.json` file, the old FQDNs still appear in the Web Studio sign-in window. As a result, you must enter the new FQDNs as an alternative when signing in.
> - To view all supported parameters, run `StudioConfig.exe --help`.

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

(Optional) Configure Web Studio as a proxy for Delivery Controllers

By default, when you manage your deployment using the Web Studio console, you connect to both the Web Studio server and the Delivery Controllers through the web browser. We provide you with an option to configure the Web Studio server as a proxy for Delivery Controllers. As a result, you connect only to the Web Studio server when managing your deployment.

This section guides you to configure a Web Studio server as a proxy for Delivery Controllers. We assume that Web Studio and Delivery Controllers are installed on different servers.

Before you start, verify that you have all necessary core components installed in your deployment. For more information, see Install core components.

To enable proxy mode for Web Studio, follow these steps:

1. On the Web Studio server, run Windows PowerShell as an administrator.
2. Run the following command where you replace `fqdn_of_webstudio_machine` with the FQDN of your Web Studio server.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"--enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **Note:**
   >
   > If you have a load-balanced Web Studio deployment, replace `fqdn_of_webstudio_machine` with the FQDN of the load balancer server (also known as the virtual server). For more information, see Set up a load-balanced Web Studio deployment.

To disable proxy mode for Web Studio, run this PowerShell command:

```
1 & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --
     disableproxy
```

(Optional) Enable or disable Pendo

Starting with version 2411, Web Studio integrates Pendo, which is enabled by default. Pendo collects your usage data following the Citrix Privacy Policy. It also adds an icon in the bottom-right corner of Web Studio, providing you with contextual feature information and feedback options. If you prefer not to share your usage data, you can disable Pendo using the Studio configuration tool.

This tool is available in the Web Studio installation folder. By default, the tool is installed in the following folder: `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`.

To disable Pendo, follow these steps:

1. Sign in to Web Studio. If an icon appears in the bottom-right corner, Pendo is enabled.

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

2. On the Web Studio server, run Windows PowerShell as an administrator.
   Run this PowerShell command:

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --
    disablependo
```

To enable Pendo, run this command:

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --
    enablependo
```

Secure server configuration for Web Studio

Apply the following security configurations to the server hosting Web Studio for better security. These settings are applied at the server level, not in Web Studio itself.\

Disable medium-strength SSL ciphers (SWEET32)

The Web Studio server might use the medium-strength cipher `TLS_RSA_WITH_3DES_EDE_CBC_SHA`, which is vulnerable to the SWEET32 attack.

To disable the cipher, run the following PowerShell command on the Web Studio server:

```
Disable-TlsCipherSuite -Name TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Disable deprecated TLS 1.0 and 1.1 protocols

TLS 1.0 and TLS 1.1 are deprecated and cannot be enabled on the Web Studio server.

To disable them:

1. Open Registry Editor (`regedit.exe`).
2. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`.
3. Create the following subkeys if they don't exist:
   - `TLS 1.0\Client`
   - `TLS 1.0\Server`
   - `TLS 1.1\Client`
   - `TLS 1.1\Server`
4. In each `Client` and `Server` key, create the following `DWORD (32-bit)` values:
   - `Enabled` = `0`

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

- `DisabledByDefault` = 1 (optional but recommended)

5. Restart the server to apply changes.

Sign in to Web Studio

1. Access Web Studio at `https://<address of the server hosting Web Studio>/Citrix/Studio` if the default port number 443 is used. If a different port is configured, use `https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio`.

   The Sign-in page appears if you've added Delivery Controllers to Web Studio and they are reachable.

   > **Note:**
   >
   > The **Unable to sign in** page appears in the following cases:
   >
   > - No Delivery Controllers have been specified for the site. You are prompted to add one to connect.
   > - The specified Delivery Controllers are unreachable. Click **Test** to check connectivity. Or, enter an alternate Delivery Controller and click **Connect**.

2. Enter **User name**, **Password**, and **Domain**.
3. Click **Sign in**.

Next steps

1. Install VDAs
2. Use Web Studio to deliver virtual apps and desktops to your users by:
   a) Creating a machine catalog
   b) Creating a delivery group
   c) Creating an application group (optional)

Install VDAs

January 23, 2026

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

> **Important:**
>
> - If you're upgrading and your current version has the Personal vDisk or AppDisks software installed, see Removing PvD, AppDisks, and unsupported hosts.
> - Binaries distributed by Citrix® are now signed. Signed binaries indicate that they are validated by either Citrix-generated certificates or authentic third-party certificates.

There are two types of VDAs for Windows machines: VDA for multi-session OS and VDA for single-session OS. (For information about VDAs for Linux machines, see the Linux Virtual Delivery Agent documentation.)

Before starting an installation, review Prepare to install and complete all preparation tasks.

Before installing VDAs, install the core components. You can also create the site before installing VDAs.

This article describes the installation wizard sequence when installing a VDA. Command-line equivalents are provided. For details, see Install using the command line.

Step 1. Download the product software and launch the wizard

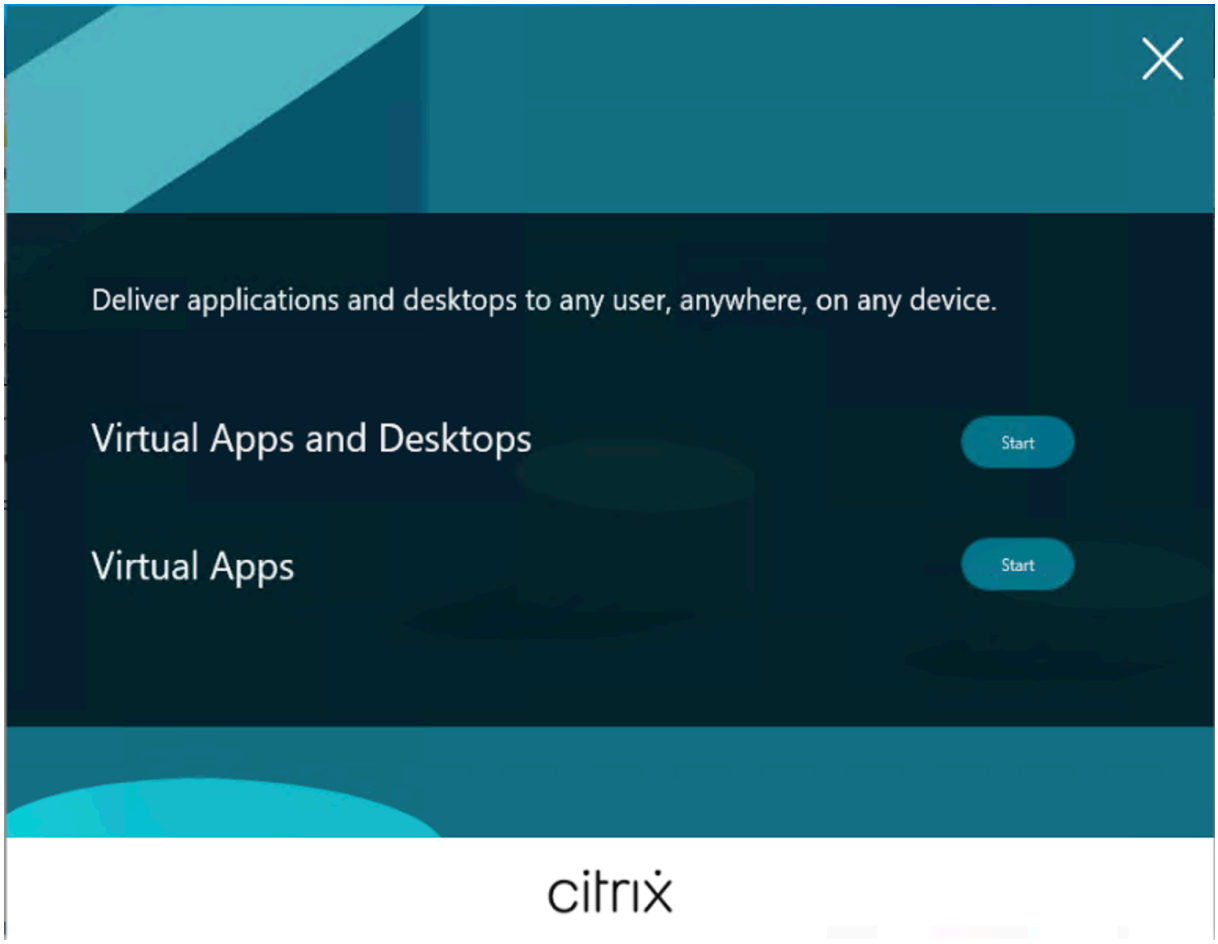
If you're using the full-product installer:

1. If you haven't downloaded the product ISO yet:
   - Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops™ download page. Download the product ISO file.
   - Unzip the file. Optionally, burn a DVD of the ISO file.
2. Use a local administrator account on the image or machine where you're installing the VDA. Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the **AutoSelect** application on the mounted drive.

   The installation wizard launches.

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

Step 2. Choose which product to install

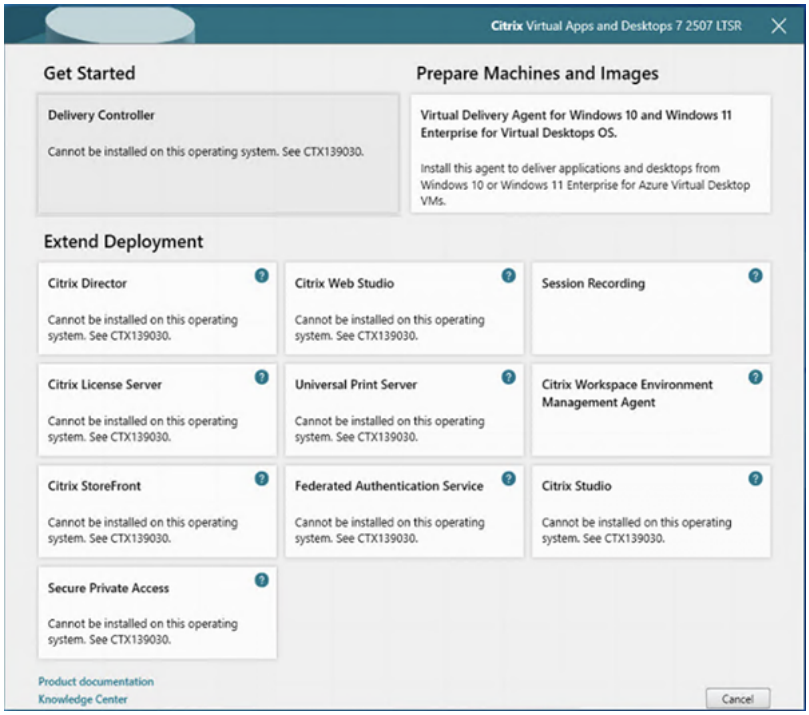


Click **Start** next to the product to install: Citrix Virtual Apps or Citrix Virtual Desktops. (If the machine already has a Citrix Virtual Apps or Citrix Virtual Desktops component installed, this page does not appear.)

Command-line option: `/xenapp` to install Citrix Virtual Apps. Citrix Virtual Desktops is installed if this option is omitted.

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

Step 3. Select the VDA



Select the **Virtual Delivery Agent** entry. The installer knows whether it's running on a single-session or multi-session OS, so it offers only the appropriate VDA type.

For example, when you run the installer on a Windows Server 2019 machine, the VDA for multi-session OS option is available. The VDA for single-session OS option is not offered.

If you try to install (or upgrade to) a Windows VDA on an OS that is not supported for this Citrix Virtual Apps and Desktops version, a message guides you to information about options.

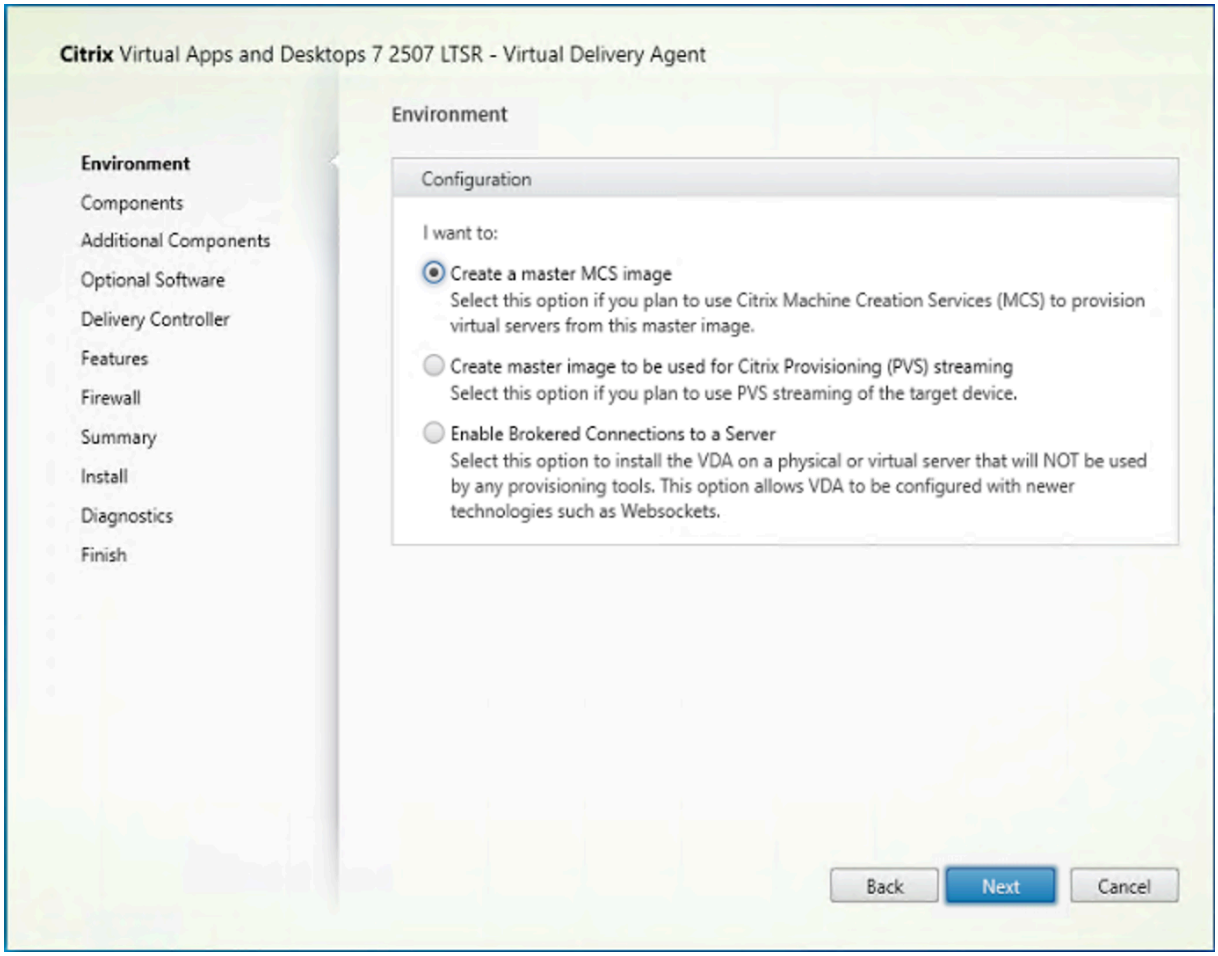
If you're using a standalone package:

1. Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page. Download the appropriate package:
   - `VDAServerSetup_2507.exe`: Multi-session OS VDA *version*
   - `VDAWorkstationSetup_2507.exe`: Single-session OS VDA *version*
   - `VDAWorkstationCoreSetup_2507.exe`: Single-session OS Core Services VDA *version*
   - `VDASingleSessionCoreSetup_2507.exe`: New Single-session OS Core Services VDA version (for 2507 CU1 and later)
2. Right-click the package and choose **Run as administrator.**

   The installation wizard launches.

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

Step 4. Specify how the VDA will be used



On the **Environment** page, specify how you plan to use the VDA, indicating whether you use this machine as an image to provision more machines.

The option you choose affects which Citrix Provisioning™ tools are installed automatically (if any), and the default values on the Additional Components page of the VDA installer.

Several MSIs (provisioning and other) are installed automatically when you install a VDA. The only way to prevent their installation is with the `/exclude` option in a command-line installation.

Choose one of the following:

- **Create a master MCS image:** Select this option to install a VDA on a VM image, if you plan to use Machine Creation Services™ to provision VMs. This option installs the Machine Identity Service. This is the default option.

  Command-line option: `/mastermcsimage` or `/masterimage`

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

> **Important:**
>
> The installation media or ISO image must be mounted locally. Mounting an ISO image off a network drive for the purposes of installing software is not supported.

- **Create a master image using Citrix Provisioning or third-party provisioning tools:** Select this option to install a VDA on a VM image, if you plan to use either Citrix Provisioning or third-party provisioning tools (such as Microsoft System Center Configuration Manager) to provision VMs.

  Command-line option: `/masterpvsimage`

- (Appears only on multi-session OS machines) **Enable brokered connections to a server:** Select this option to install a VDA on a physical or virtual machine that will not be used as an image to provision other machines.

  Command-line option: `/remotepc`

- (Appears only on single-session OS machines) **Enable Remote PC Access:** Select this option to install a VDA on a physical machine for use with Remote PC Access.

  Command-line option: `/remotepc`

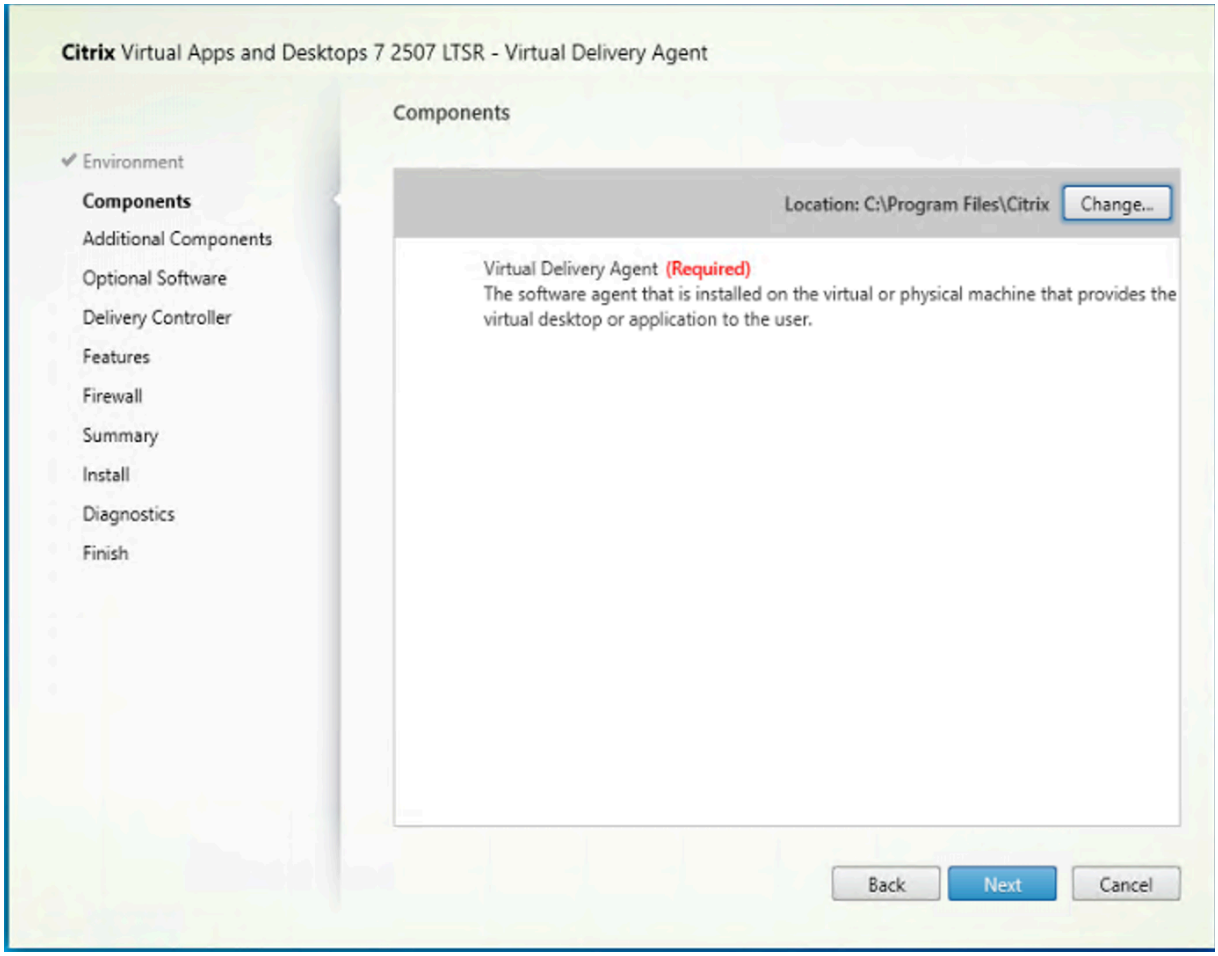
Click **Next**.

This page does not appear:

- If you're upgrading a VDA
- If you are using the `VDAWorkstationCoreSetup_2507.exe`, `VDAServerSetup_2507.exe`, or `VDAWorkstationSetup_2507.exe` installer

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

Step 5. Select the location to install VDA



> **Note:**
>
> CWA and CSA have moved from the Component page to the new Optional Software page.

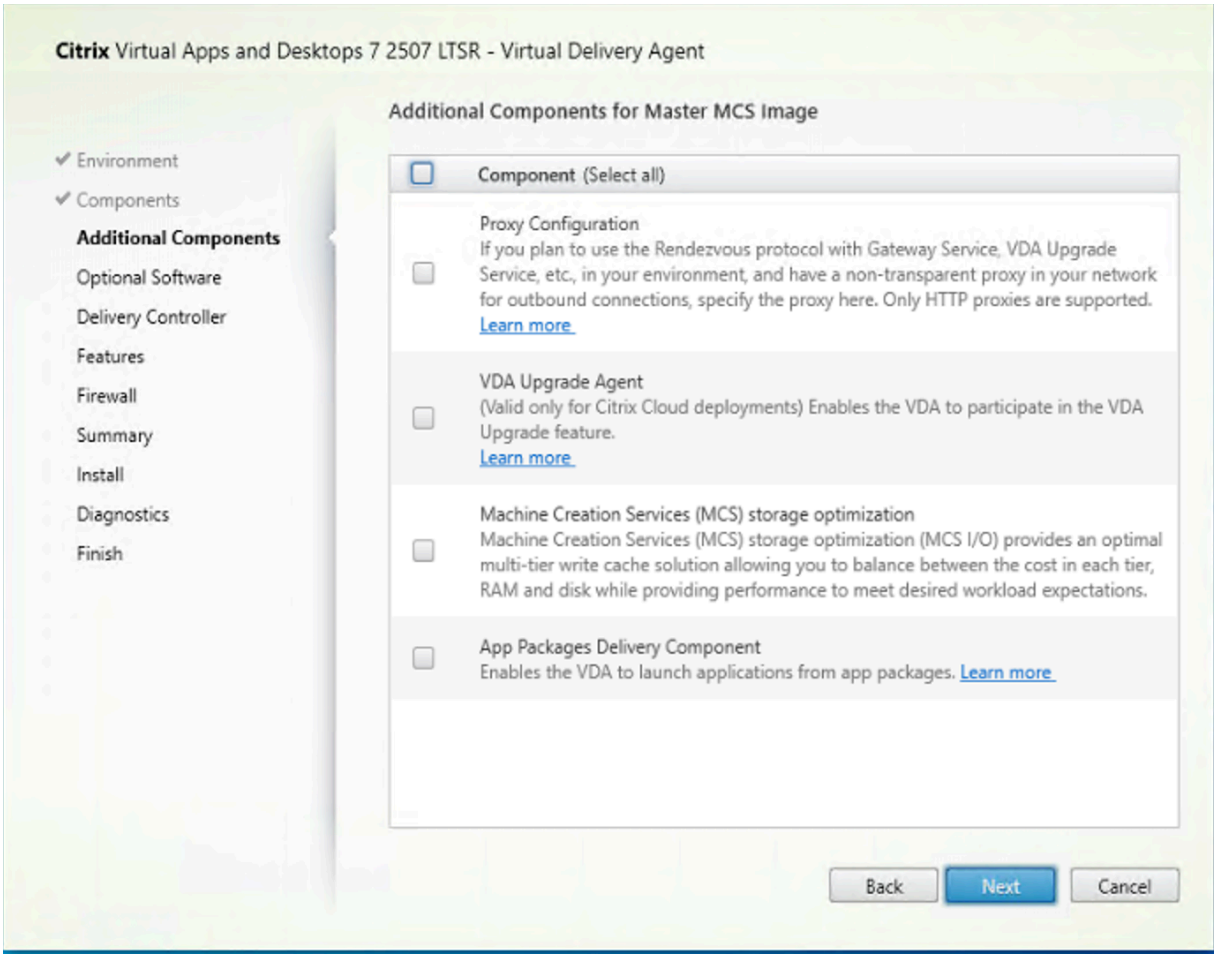
On the **Components** page:

- **Location:** By default, VDA is installed in `C:\Program Files\Citrix`. This default is fine for most deployments. If you specify a different location, that location must have `execute` permissions for network service.

Click **Next**.

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

Step 6. Install additional components



The **Additional Components** page contains checkboxes to enable or disable installation of other features and technologies with the VDA. In a command-line installation, you can use the `/exclude` or `/includeadditional` option to expressly omit or include one or more available components:

- **/includeadditional** "*component*"[,"*component*"] …
- **/exclude** "*component*"[,"*component*"] …

The following table indicates the default setting of items on this page. The default setting depends on the option that you selected on the **Environment** page.

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

Additional Components page	Environment page: “Master image with MCS”or “Master image with Citrix Provisioning” selected	Environment page: “Enable brokered connections to server”(for multi-session OS) or “Remote PC Access”(for single-session OS) selected
App Packages Delivery Component	Not selected	Not selected
Citrix VDA Upgrade Agent	Not selected	Not selected
Citrix Backup and Restore	Not selected	Not selected
Citrix MCS IODriver	Not selected	Not selected
Citrix Rendezvous V2	Not selected	Not selected

This page does not appear if:

- You are using the `VDAWorkstationCoreSetup.exe` installer. Also, the command-line options for the additional components are not valid with that installer.
- You are upgrading a VDA and all the additional components are already installed. If some of the additional components are already installed, the page lists only components that are not installed.

Select or clear the following checkboxes. (The components might appear in a different order in the installer.)

- **App Packages Delivery Component:** Install this component if you use applications from Microsoft App-V packages. For details, see Deploy and deliver App-V applications.

  Command-line option: `/includeadditional "App Packages Delivery Component"` to enable component installation, `/exclude "App Packages Delivery Component"` to prevent component installation.

- **Citrix Profile Management:** This component manages user personalization settings in user profiles. For details, see Profile Management.

  Excluding Citrix Profile Management from the installation affects the monitoring and troubleshooting of VDAs with Citrix Director. On the **User details** and **End Point** 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 user profile management solution, Citrix recommends that you install and run the Citrix Profile Management Service. Enabling the Citrix Profile Management Service is not required.

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

Command-line option: `/includeadditional "Citrix Profile Management"` to enable component installation, `/exclude "Citrix Profile Management"` to prevent component installation.

- **Citrix Profile Management WMI Plug-in:** This plug-in provides Profile Management runtime information in WMI (Windows Management Instrumentation) objects (for example, profile provider, profile type, size, and disk usage). WMI objects provide session information to Director.

  Command-line option: `/includeadditional "Citrix Profile Management WMI Plug-in"` to enable component installation, `/exclude "Citrix Profile Management WMI Plug-in"` to prevent component installation.

> **Note:**
>
> Starting with this version, **Citrix Profile Management** and **Citrix Profile Management WMI Plug-in** are now part of the VDA and are installed automatically for **Master Image/MCS/PVS** use cases. These components are **not installed by default** for the **Remote PC** use case. In all instances, installed components are automatically upgraded. The command-line behavior remains unchanged from previous releases.

- **VDA Upgrade Agent:** Applicable only to Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments. Enables the VDA to participate in the VDA Upgrade feature. You can use that feature to upgrade a catalog's VDAs from the management console, immediately or at a scheduled time. If this agent is not installed, you can upgrade a VDA by running the VDA installer on the machine.

  Command-line options: `/includeadditional "Citrix VDA Upgrade Agent"` to enable component installation, `/exclude "Citrix VDA Upgrade Agent"` to prevent component installation.

- **MCSIO write cache for storage optimization:** Installs the Citrix MCS I/O driver. For more information, see Storage shared by hypervisors and Configure cache for temporary data.

  Command-line options: `/includeadditional "Citrix MCS IODriver"` to enable component installation, `/exclude "Citrix MCS IODriver"` to prevent component installation.

- **Proxy Configuration:** Install this component if you plan to use the Rendezvous protocol with the Gateway Service, VDA Upgrade Service, and so on, in your environment, and you have a non-transparent proxy in your network for outbound connections, specify the proxy here. Only HTTP proxies are supported.

  If you install this component, specify the address of the proxy or PAC file path on the **Rendezvous Proxy Configuration** page. For feature details, see Rendezvous protocol.

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

Command-line option: `/includeadditional "Citrix Rendezvous V2"` to enable component installation, `/exclude "Citrix Rendezvous V2"` to prevent component installation.

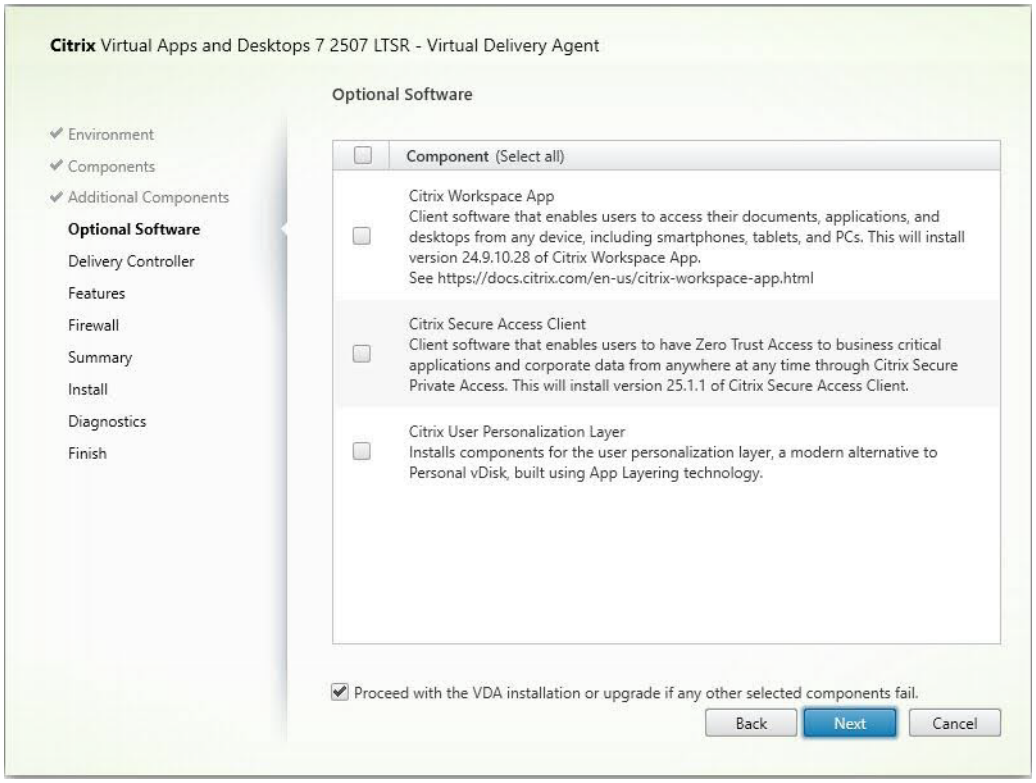
- **Citrix Backup and Restore:** If a VDA installation or upgrade fails, then this component can return the machine to a backup that was done before the installation or upgrade.

  Make sure that the Microsoft prerequisites are met as mentioned in Prepare to install.

  Command-line option: `/includeadditional "Citrix Backup and Restore"` to enable component installation, `/exclude "Citrix Backup and Restore"` to prevent component installation.

  > **Note:**
  >
  > If the MCS storage optimization is enabled, then the backup or restore for Windows server or desktop Operating System can fail. To resolve this, disable the MCS storage optimization option in the meta installer.

Step 7. Install optional software



> **Note:**
>
> The Optional Software page is a new addition starting Citrix Virtual Apps and Desktops 2503, pro-

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

> viding customers with more flexibility to install additional Citrix software on the VDA.
>
> The Citrix Workspace™ App and Citrix Secure Access™ Client have been moved from the Component page to the Optional Software page.
>
> The User Personalization Layer has also been moved from the Additional Component page to the Optional Software page. Its selection logic remains the same as when it was on the Additional Component page. That is, if the User Personalization Layer is already installed, it is selected as **Required** and the component is upgraded.

On the **Optional Software** page:

- **Location**: By default, components are installed in `C:\Program Files\Citrix`. This default is fine for most deployments. If you specify a different location, that location must have `execute` permissions for network service.
- **Components**: By default, Citrix Workspace app for Windows is not installed with the VDA. If you are using the `VDAWorkstationCoreSetup.exe` installer, Citrix Workspace app for Windows is never installed, so this checkbox is not displayed.

Click **Next**.

Command-line options: `'/installdir "C:\Program Files\VDA" /components "VDA","CSA","PLUGINS"`.to install the Virtual Delivery Agent, Citrix Secure Access Client, Citrix deviceTRUST, Citrix uberAgent, and the Citrix Workspace app into the specified directory.

> **Note:**
>
> You can choose to install, upgrade, or uninstall the Citrix Workspace app and other components during a VDA installation, upgrade, or uninstallation in the following scenarios:
>
> - During VDA installation and upgrade to 2507 LTSR, you can choose to include or exclude components and CWA plug-ins.
>   - By default, **Citrix Workspace app (CWA)**, **Citrix Secure Access Client (CSA)**, and **Citrix User Personalization Layer (UPL)** are not installed. You can select them during installation if needed.
>   - **Citrix Device Trust**, **Citrix uberAgent**, and **Citrix Workspace Environment Management™ agent** are now integrated with the VDA and are always installed. These components cannot be deselected when installing using the GUI.
>   - By default, the **Citrix Workspace Environment Management™ agent** runs in **Basic deployment**, a single-machine mode with limited functionality that doesn't connect to a WEM infrastructure. To enable full WEM capabilities by connecting the agent to the WEM service in Citrix Cloud or an on-premises deployment, configure the settings through group policies. For more information, see this WEM article.

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

- **Command-line changes**

  /components VDA CSA : The command installs **VDA** and **CSA** (selected), and also **Citrix Device Trust**, **Citrix uberAgent**, and **Citrix Workspace Environment Management agent** (default integrated).

  /components VDA : The command installs **VDA**, and also **Citrix Device Trust**, **Citrix uberAgent**, and **Citrix Workspace Environment Management agent** as these are now integrated into the VDA itself. If you specify Citrix Device Trust, Citrix uberAgent, and Citrix Workspace Environment Management agent as arguments alongside the "/components"option, the VDA Meta-installer logs a notification indicating the removal of these arguments from the "/components"option. Subsequently, the VDA Meta-installer proceeds with the installation or upgrade of the VDA.

  /components : The command is an invalid command and it must always include VDA. Additional components can be added for installation as required.

  Using `/exclude` command for default integrated components : In Citrix Virtual Apps and Desktops 2507 LTSR, the `/exclude` option always takes precedence. It can be used to prevent installation of default integrated components. Example: `/exclude` "Citrix Device Trust","Citrix Universal Print Client". The command installs VDA with Citrix Workspace Environment Management agent, but does not install Citrix Device Trust and Citrix Universal Print Client.

- During a VDA upgrade, if Citrix Workspace app, Citrix Secure Access Client and Citrix User Personalization Layer are not already installed in the VDA, you can choose to install them.
- During a VDA upgrade, if the version of Citrix Workspace app, and other installed plug-ins can be upgraded, then the option to upgrade them is displayed.
- During installation or upgrade, if the Citrix Workspace app (CWA) plug-in or any components fail to install or upgrade, you can override the failure and continue installing the core VDA by selecting the checkbox '**Proceed with VDA upgrade or installation if selected components fail.**'
- During a VDA uninstallation, you can choose whether to uninstall the Citrix Workspace app (CWA) and any other installed components. By default, all components except CWA are uninstalled automatically. CWA is treated differently and is not removed unless explicitly selected.

- **Citrix User Personalization Layer:** Installs the MSI for the user personalization layer. For details, see User personalization layer.

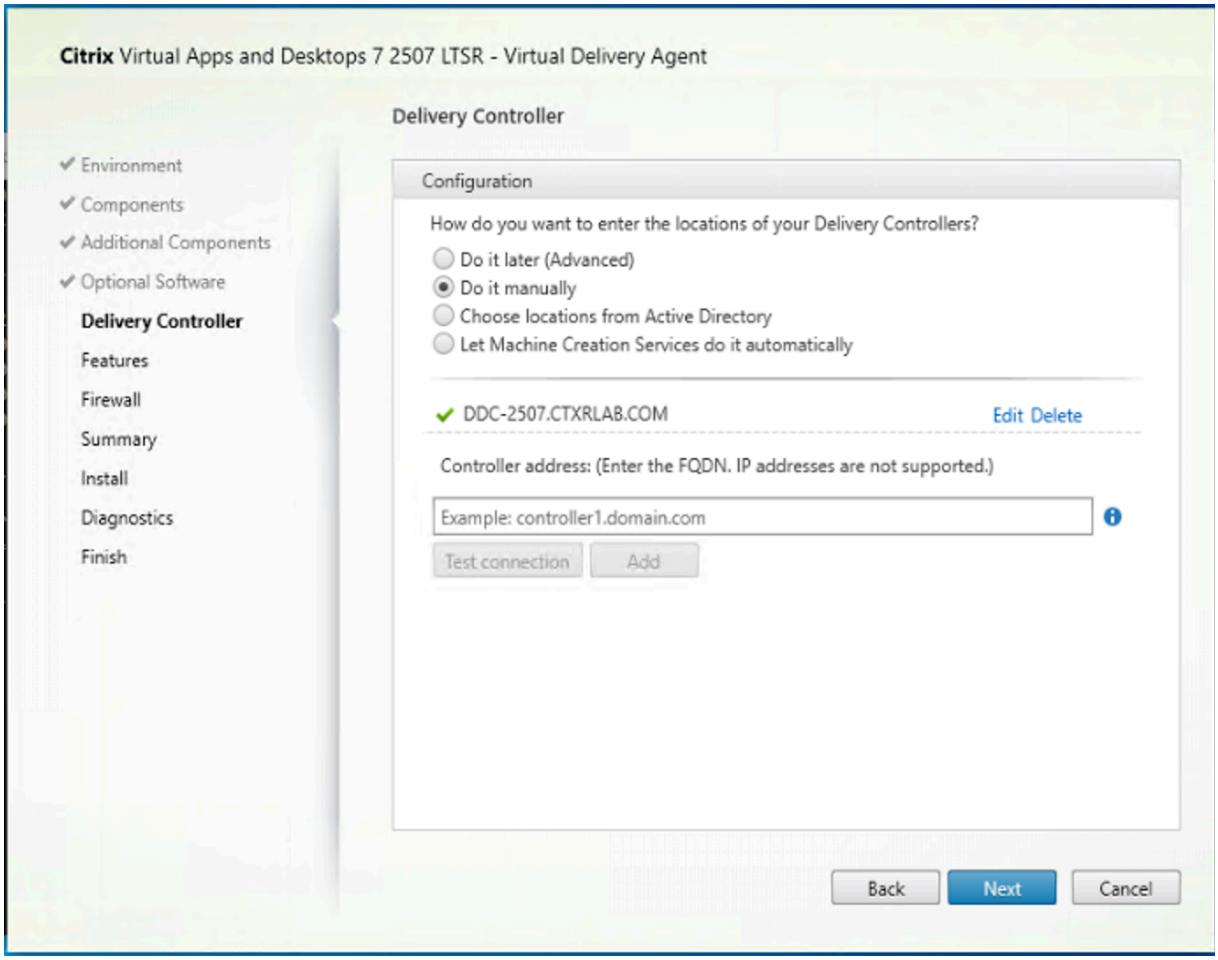
  This component appears only when installing a VDA on a single-session Windows 10 machine.

  Command-line option: `/includeadditional "User Personalization Layer"` to enable component installation, `/exclude "User Personalization Layer"` to

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

prevent component installation.

Step 8. Delivery Controller™ addresses



On the **Delivery Controller** page, choose how you want to enter the addresses of installed Controllers. Citrix recommends that you specify the addresses while you're installing the VDA (**Do it manually**). The VDA cannot register with a Controller until it has this information. If a VDA cannot register, users cannot access applications and desktops on that VDA.

- **Do it manually:** (default) Enter the FQDN of an installed Controller and then click **Add**. If you've installed more Controllers, add their addresses.
- **Do it later (Advanced):** If you choose this option, the wizard asks you to confirm that's what you want to do before continuing. To specify addresses later, you can either rerun the installer or use Citrix Group Policy. The wizard also reminds you on the **Summary** page.
- **Choose locations from Active Directory:** Valid only when the machine is joined to a domain and the user is a domain user.
- **Use WebSocket Token:** Creates a WebSocket VDA. The WebSocketToken is for the token that is

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

required.

- **Let Machine Creation Services do it automatically:** Valid only when using MCS to provision machines.

Click **Next**. If you selected **Do it later (Advanced)**, you are prompted to confirm that you will specify Controller addresses later.

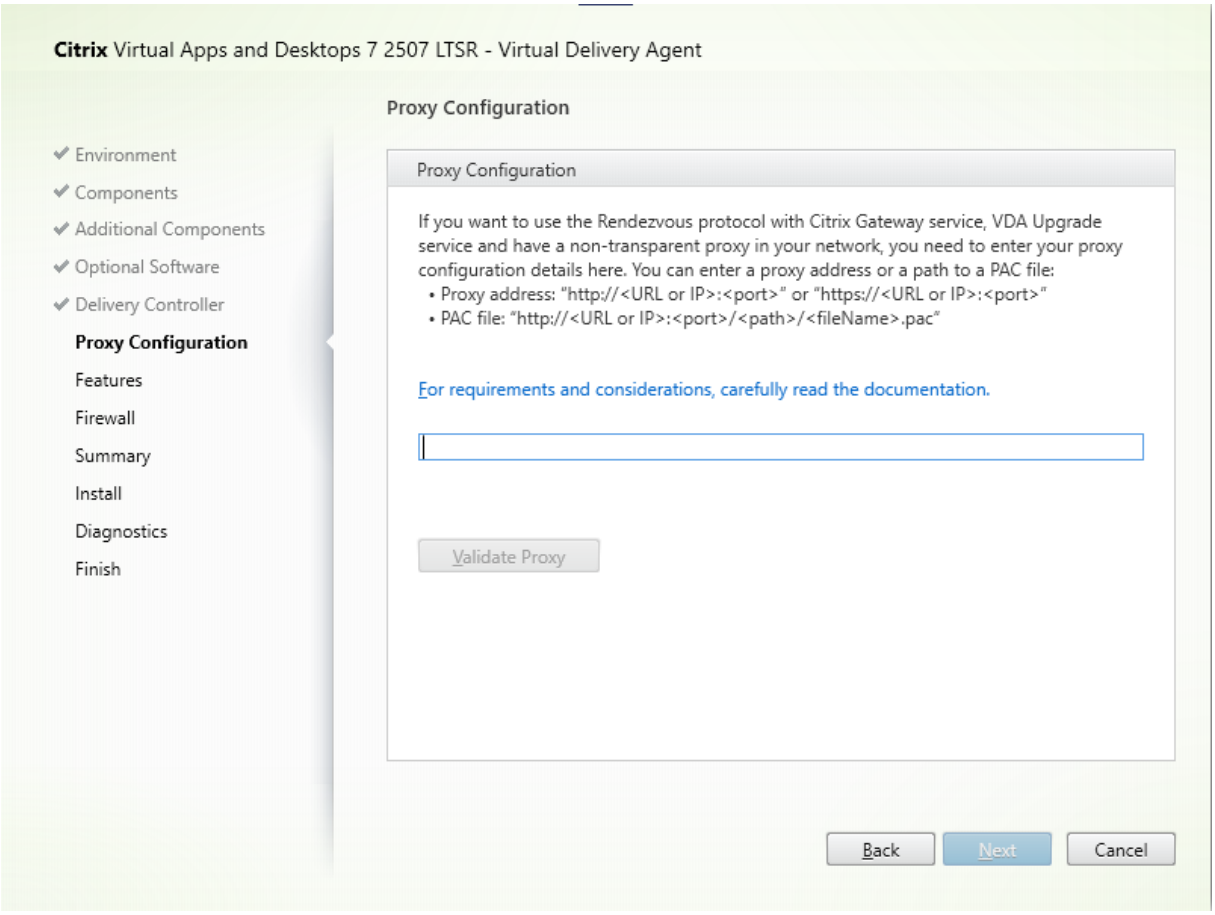
Other considerations:

- The address cannot contain non-alphanumeric characters.
- If you specify addresses during VDA installation and in Group Policy, the policy settings override settings provided during installation.
- Successful VDA registration requires that the firewall ports used to communicate with the Controller are open. That action is enabled by default on the **Firewall** page of the wizard.
- After you specify Controller locations (during or after VDA installation), you can use the auto-update feature to update the VDAs when Controllers are added or removed. For details about how VDAs discover and register with Controllers, see VDA registration.

Command-line option: `/controllers`

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

Step 9. Proxy Configuration



The **Proxy Configuration** page appears only if you enabled the **Proxy Configuration** check box on the **Additional Components** page.

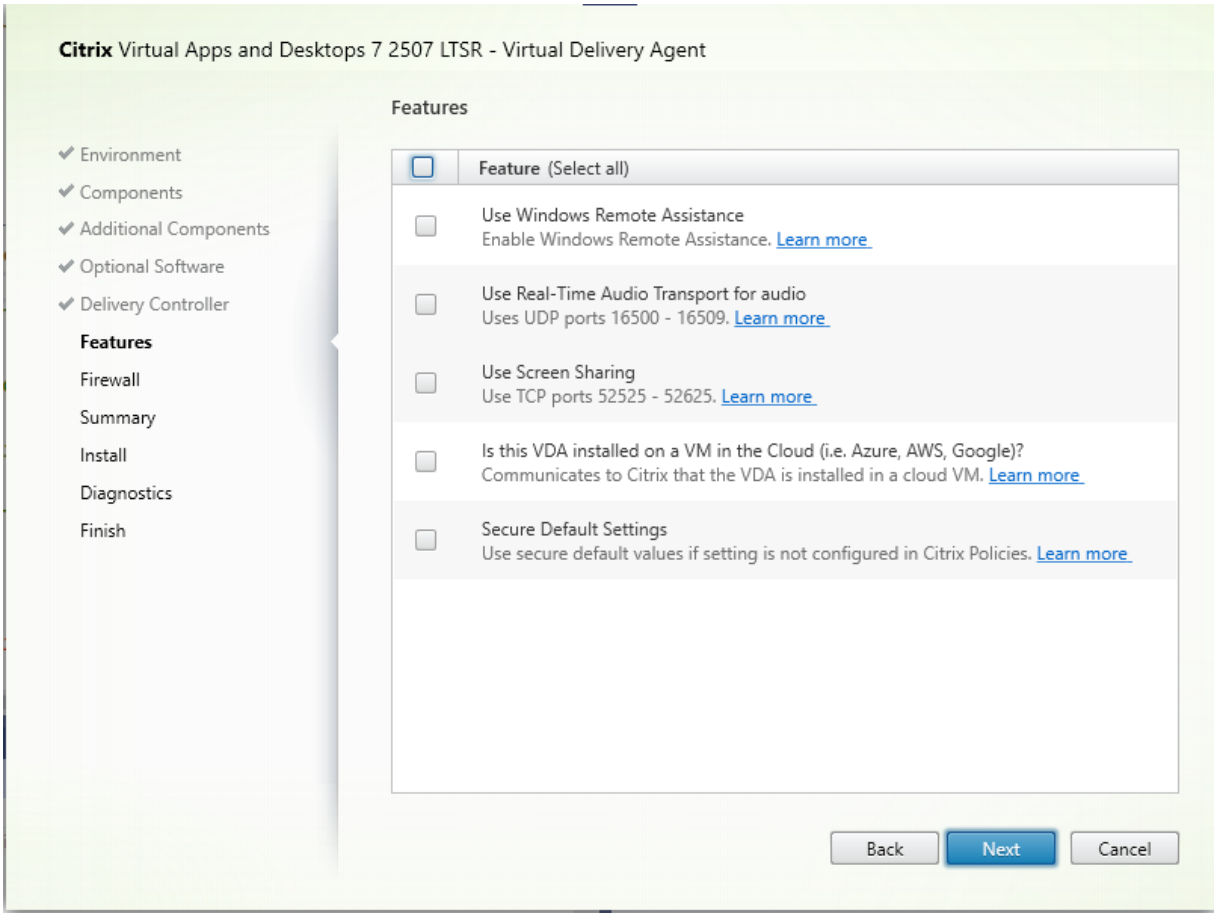
1. Select whether you will specify the proxy source by proxy address or PAC file path.
2. Specify the proxy address or PAC file path.
   - Proxy address format: `http://<url-or-ip>:<port>`
   - PAC file format: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

The firewall for the proxy port must be open for the connection test to succeed. If a connection cannot be made to the proxy, you can choose whether to continue with the VDA installation.

Command-line option: `/proxyconfig`

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

Step 10. Enable or disable features



On the **Features** page, use the check boxes to enable or disable the features you want to use.

- **Use Windows Remote Assistance:** When this feature is enabled, Windows Remote Assistance is used with the user shadowing feature of Director. Windows Remote Assistance opens the dynamic ports in the firewall. (Default = disabled)

  Command-line option: `/enable_remote_assistance`

- **Use Real-Time Audio Transport for audio:** Enable this feature if voice-over-IP is widely used in your network. The feature reduces latency and improves audio resilience over lossy networks. It allows audio data to be transmitted using RTP over UDP transport. (Default = disabled)

  Command-line option: `/enable_real_time_transport`

- **Use screen sharing:** When enabled, ports used by screen sharing are opened in the Windows firewall. (Default = disabled)

  Command-line option: `/enable_ss_ports`

- **Is this VDA installed on a VM in a cloud:** This setting helps Citrix to correctly identify resource locations for on-premises and service (Citrix Cloud™) VDA deployments for telemetry purposes.

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

This feature has no impact on customer-side utilization. Enable this setting if your deployment uses Citrix DaaS (Default = disabled).

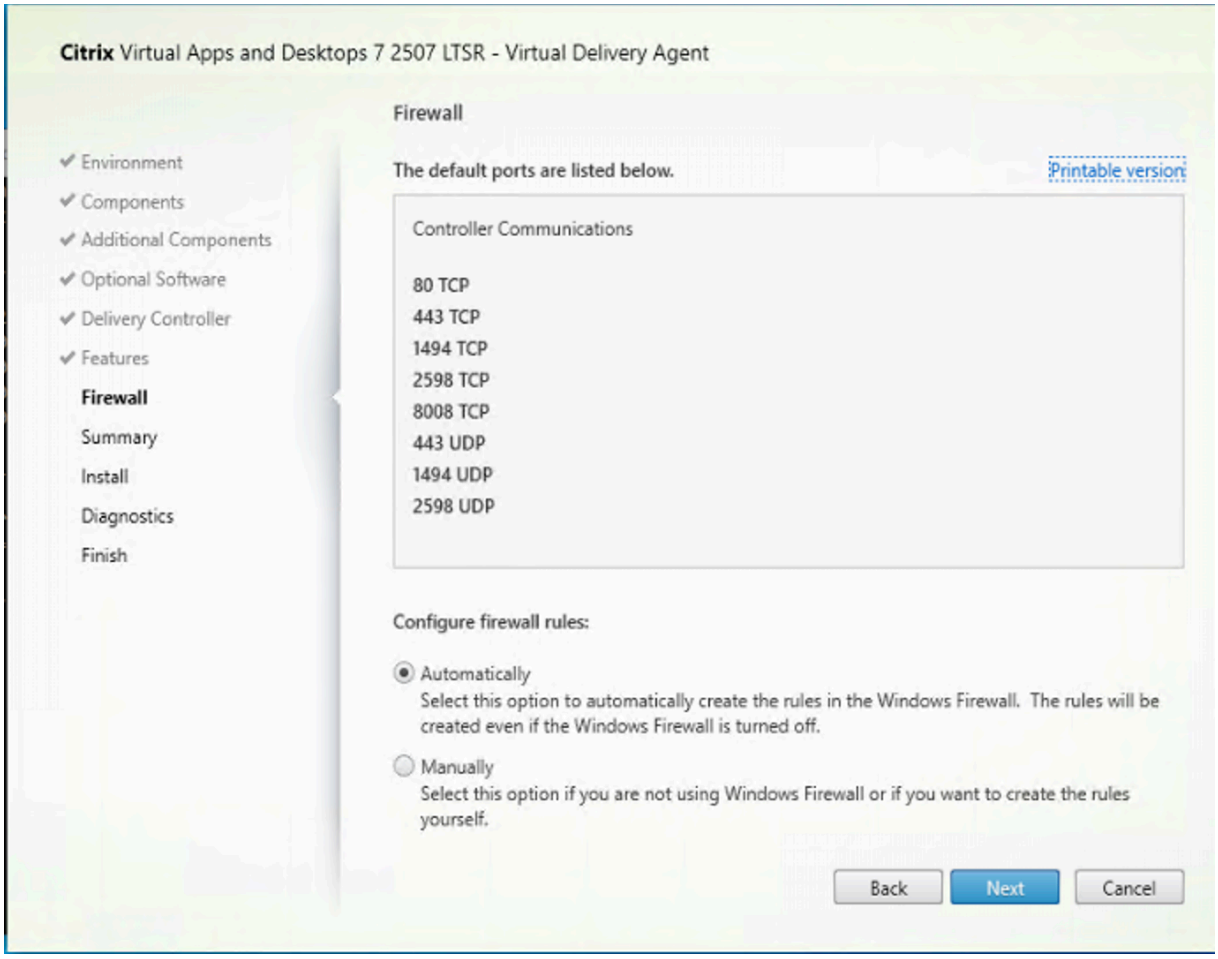
Command-line option: /xendesktopcloud

- **Secure Default Settings:** This option changes the default setting for various features from enabled to disabled for a more secure out-of-box configuration. The relevant features are: client drive redirection, special folder redirection, drag and drop, client TWAIN device redirection, Client USB Plug and Play device redirection, client printer redirection, client clipboard redirection, and client microphone redirection.

Command-line option: /ENABLE_SECURE_DEFAULTS

Click **Next**.

Step 11. Firewall ports



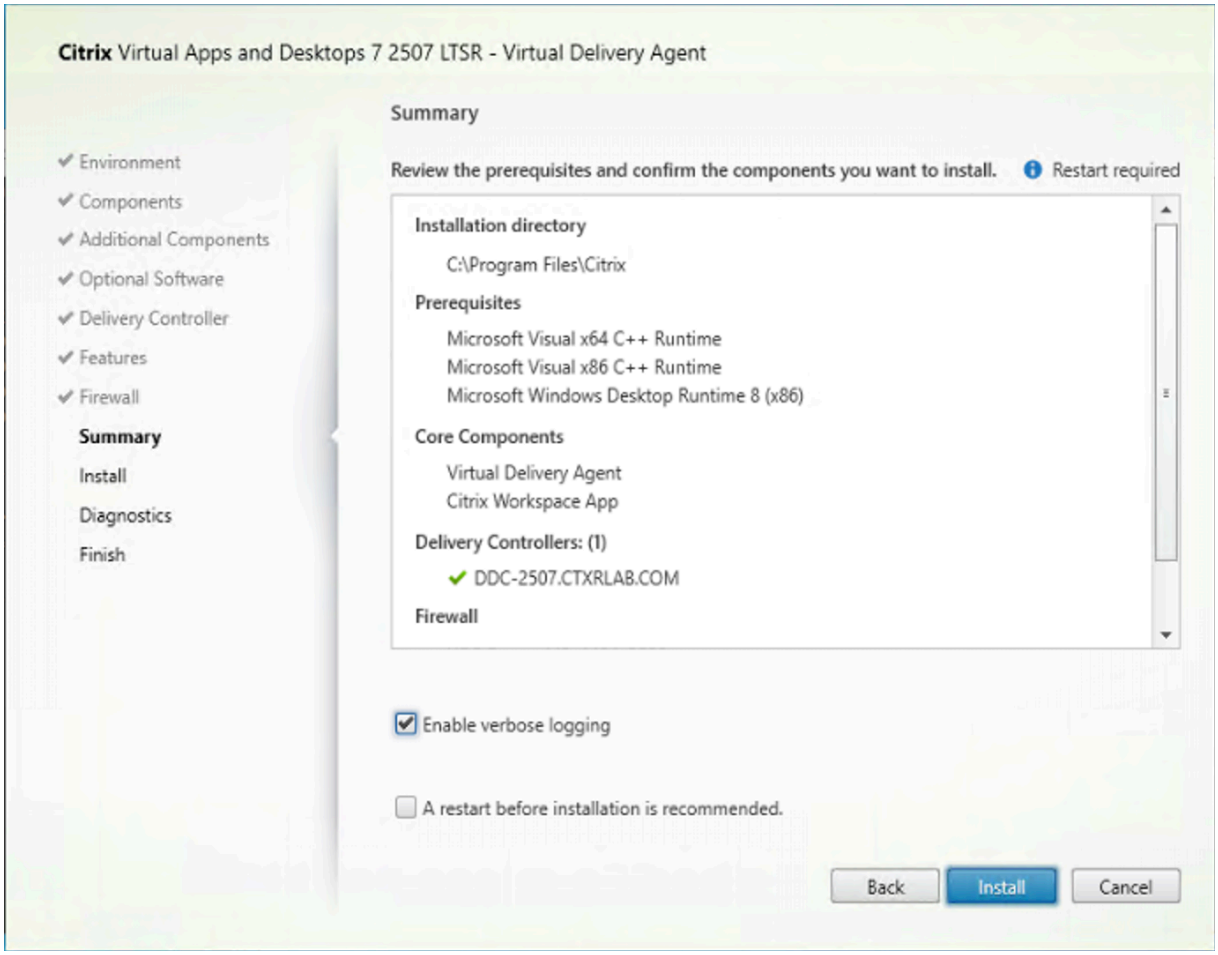
On the **Firewall** page, by default, the ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. This default setting is fine for most deployments. For port information, see Network ports.

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

Click **Next**.

Command-line option: `/enable_hdx_ports`

Step 12. Review prerequisites and confirm installation



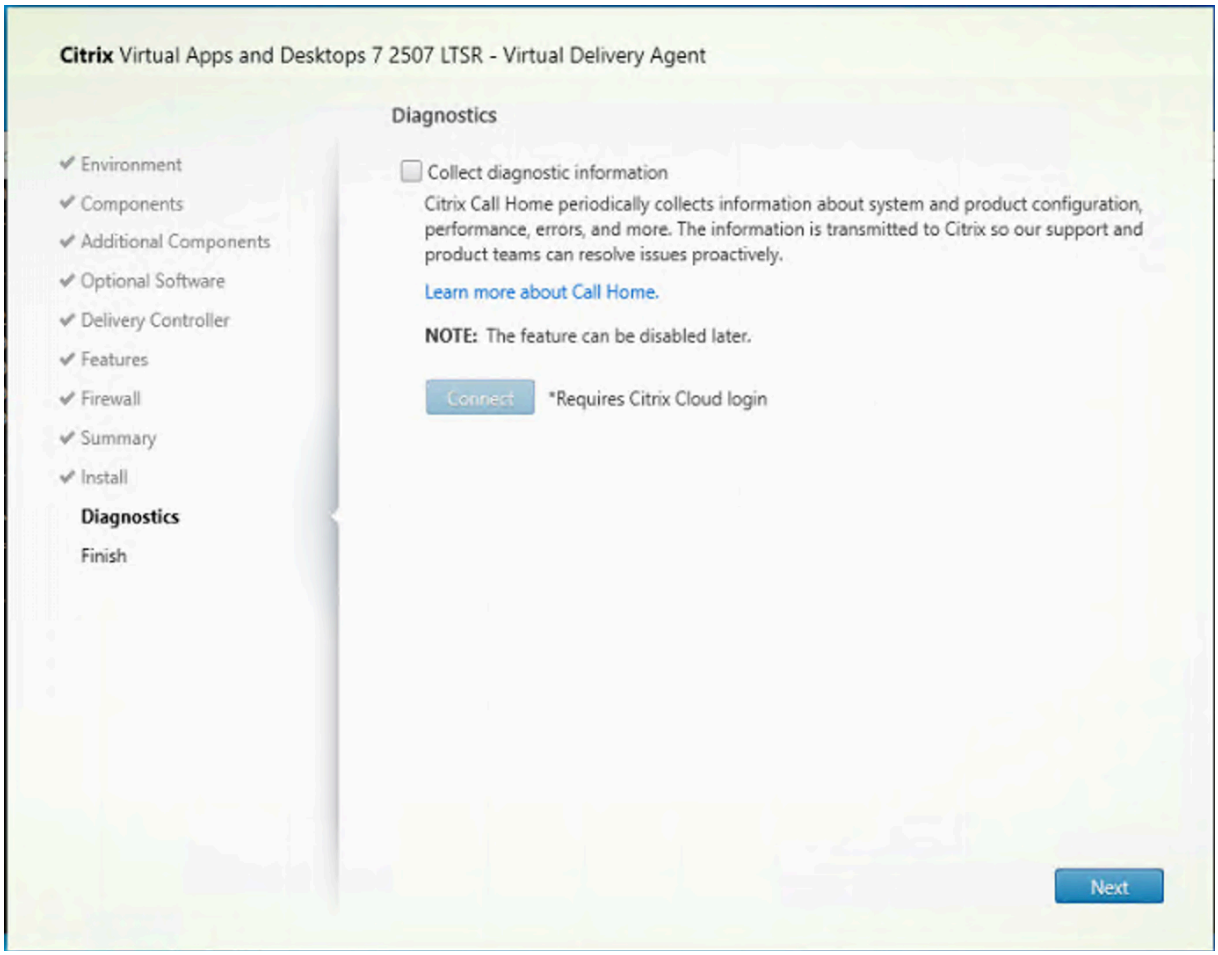
The **Summary** page lists what will be installed. Use the **Back** button to return to earlier wizard pages and change selections.

When you're ready, click **Install**.

If prerequisites aren't already installed or enabled, the machine might restart once or more times. See Prepare to install.

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

Step 13. Diagnostics



On the **Diagnostics** page, choose whether to participate in Citrix Call Home. If you choose to participate (the default), click **Connect**. When prompted, enter your Citrix account credentials.

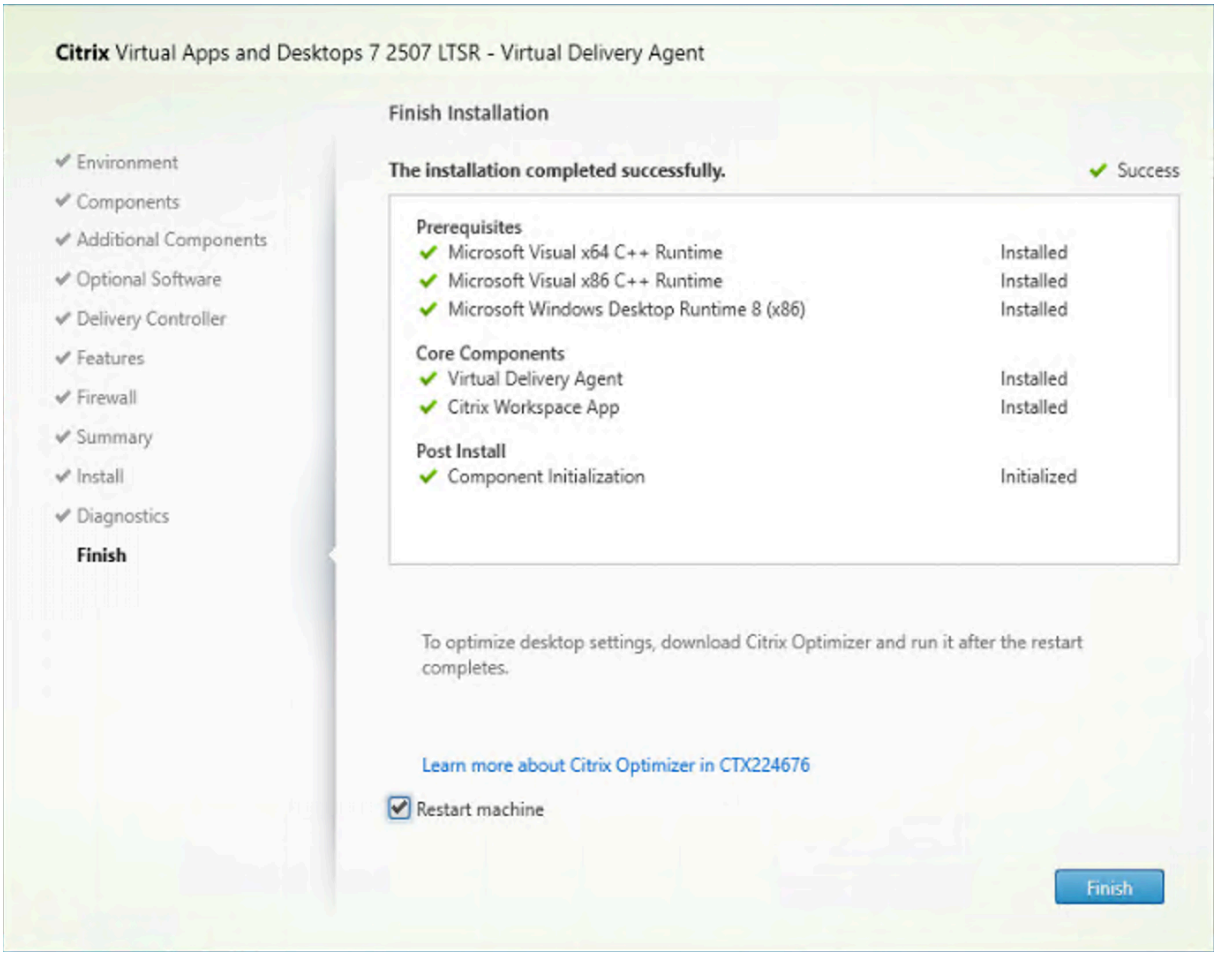
After your credentials are validated (or if you choose not to participate), click **Next**.

When using the full product installer, if you click **Connect** on the **Diagnostics** page without first selecting **Collect diagnostic information**, after you close the **Connect to Citrix Insight Services** dialog the **Next** button is disabled. You cannot move to the next page. To reenable the **Next** button, select and immediately deselect **Collect diagnostic information**.

For more information, see Call Home.

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

Step 14. Complete this installation



The **Finish** page contains green check marks for all prerequisites and components that installed and initialized successfully.

Click **Finish**. By default, the machine restarts automatically. Although you can disable this automatic restart, the VDA cannot be used until the machine restarts.

Next steps

Repeat the procedure above to install VDAs on other machines or images, if needed.

After you install all VDAs, launch Studio. If you haven't created a site yet, Studio automatically guides you to that task. After that's done, Studio guides you to create a machine catalog and then a delivery group. See:

- Create a site
- Create machine catalogs
- Create delivery groups

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

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

To customize 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, you can change:
    - Controller addresses
    - TCP/IP port to register with the Controller (default = 80)
    - Whether to open Windows Firewall ports automatically

Troubleshoot

- For information about how Citrix reports the results of component installations, see Citrix installation return codes.
- In the Studio display for a delivery group, the **Installed VDA version** entry in the **Details** pane might not be the version installed on the machines. The machine's Windows Programs and Features display shows the actual VDA version.
- After a VDA is installed, it cannot deliver apps or a desktop to users until it registers with a Delivery Controller.

  To learn about VDA registration methods and how to troubleshoot registration issues, see VDA registration.

Known limitation

When you use Citrix Workspace app for Windows version 1912 or earlier, the session drops after a while. This issue is fixed in the newer LTSR and CR versions of Citrix Workspace app.
For more information on the supported release versions, see Citrix Workspace app for Windows / Citrix Receiver for Windows Long Term Service Releases.

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

Configure Windows Defender Access Control related to VDA Installation

September 6, 2025

Customers configure Windows Defender Access Control (WDAC) settings to prohibit loading of unsigned binaries. The unsigned binaries distributed through VDA installers are thus prohibited which restricts the VDA installation.

Citrix® now signs all Citrix-generated binaries with a Citrix code signing certificate. Additionally, Citrix also signs the third-party binaries which are distributed along with our product with a certificate that authenticates those third-party binaries as trusted binaries.

> **Important:**
>
> Upgrading from an older VDA with unsigned third-party binaries to a newer VDA version with signed binaries may not always place the signed binaries on the upgraded machine.
> This is due to a mechanism within the OS where upgrade of the system does not replace binaries with the same version.
> Although the third-party binaries have been signed, their versions, which are controlled by third parties, are not able to be updated by Citrix, resulting in these binaries not being updated. To avoid this limitation:
>
> 1. Include the binaries in an allow list. This eliminates the need for signing the binaries.
> 2. Uninstall the older VDA and install the new VDA. This resembles a fresh VDA install and the signed versions will be installed.

Create a new Base Policy with the Wizard

The WDAC allows you to add trusted binaries to run on your system. After the installation of WDAC, the **Windows Defender Application Control Policy Wizard** opens automatically.

To add the binaries, a new base WDAC policy must be created. Citrix-recommended guidelines for creating a base policy are provided in this section.

- Select **Signed and Reputable Mode** as the base template because it authorizes Windows operating components, apps installed from the Microsoft Store, all Microsoft-signed software, and third-party Windows hardware-compatible drivers.
- **Enable Audit Mode** because it allows you to test new Windows Defender Application Control policies before you enforce them.
- Add **Custom Rule** for **File Rules** to specify the level at which applications are identified and trusted and provide a reference file. By selecting "Publisher"as the rule type, a reference file that is signed by one of the Citrix certificates can be selected.

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

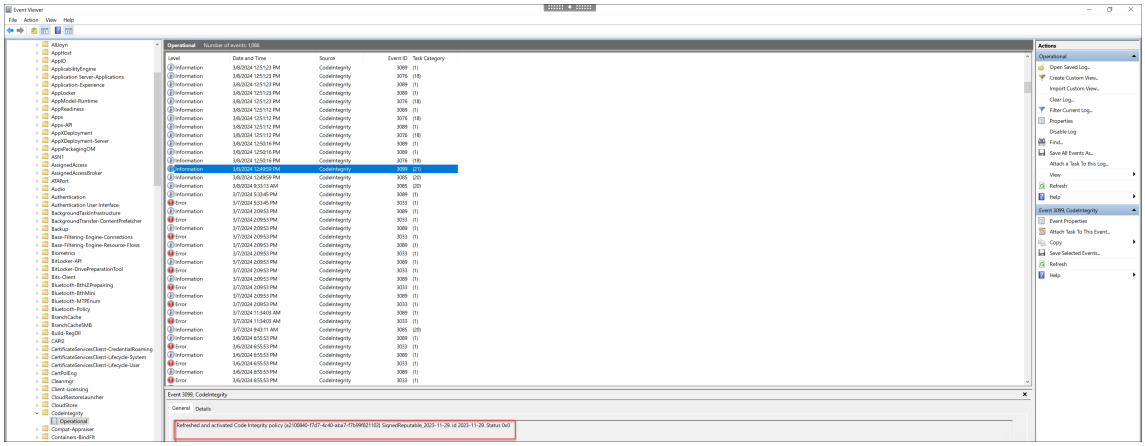
- After the rules are added, navigate to the folder where `.XML` and `.CIP` files are saved. The `.XML` file has all the rules defined in the policy. It can be configured to change, add, or remove any rules.
- Before deploying the WDAC policies, the `.XML` file must be converted to its binary form. The WDAC file converts the `.XML` file to `.CIP` file.
- Copy and paste the `.CIP` file to: C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active and reboot the machine. The generated policy will be applied in audit mode.
- For a step-by-step process to create a base policy, see Creating a new Base Policy with the Wizard.

When this policy is applied, WDAC does not give warnings about any Citrix files that are signed by the specified publisher/CA authority.

Similarly, we can create a publisher-level rule for the files that have been signed by the third party.

Verify the applied policy

1. After the machine has been rebooted, open the **Event Viewer** and go to **Applications and Services Logs > Microsoft > Windows > CodeIntegrity > Operational**.
2. Make sure the applied policy is activated.



3. Look for logs that have violated the policy and check the properties of that file. First, confirm it has been signed. If not and this machine has gone through a VDA upgrade, this most likely is the case described in the limitation above. If signed, this file is potentially signed with the alternate certificate, as described previously.

An example of a Citrix-generated file signed with a Citrix certificate is `C:\Windows\System32\drivers\picadm.sys`.
An example of a third-party binary signed with the Citrix third-party certificate is `C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`.

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

Precheck for VDA install and upgrade

May 5, 2025

Introducing a decoupled pre-flight check for VDA installation and upgrades, enabling customers to proactively identify potential issues before proceeding. This check validates all dependencies and prerequisites, providing a clear pass/fail status for each condition. If any failures occur, detailed remediation guidance with specific recommendations is provided. The actual installation or upgrade process remains separate and must be initiated manually after the pre-check is completed.

This article outlines the steps to perform the precheck for VDA installation and upgrade.

Step 1. Run Command Line

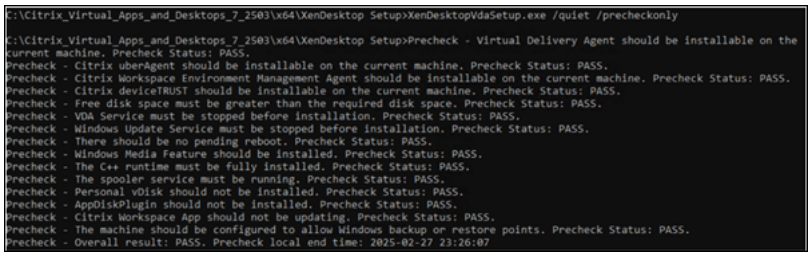
> **Note:**
>
> - The pre-check is supported only in command-line mode.
> - The installation or upgrade is not initiated when running this command.

To perform a precheck, add the `/precheckonly` option to your frequently used command for installation or upgrade. All the precheck conditions for your VDA installation or upgrade will be checked.

Perform precheck for default install and upgrade

Run the following command to perform a precheck and ensure that the machine status is in acceptable state:

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly
```

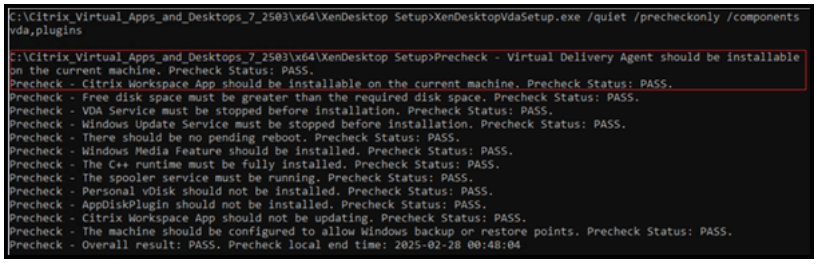


Perform precheck for install and upgrade of specified components

To check prerequisites for specific components before installation or upgrade, add `/precheckonly` to your command.

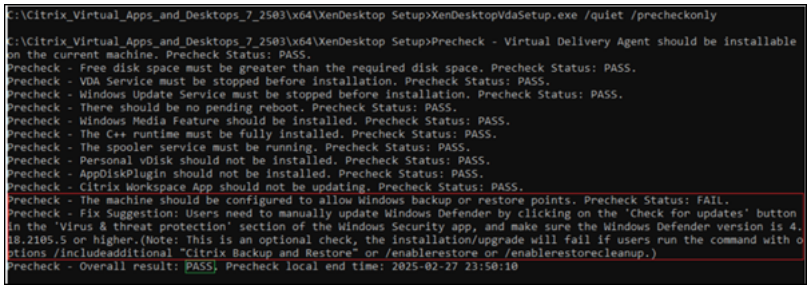
```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /
components vda,plugins
```

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



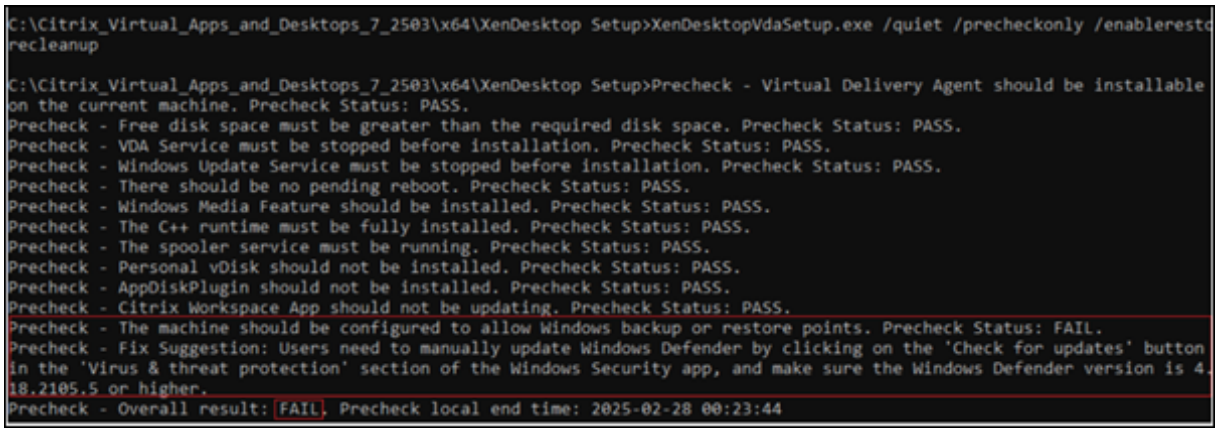
Perform precheck for install and upgrade of additional component - Citrix Backup and Restore

The command `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly` checks the prerequisites for Citrix Backup and Restore component as an optional check. If all prechecks pass except the optional check, the overall result is PASS.



The following commands check the prerequisites for Citrix Backup and Restore component as part of mandatory check:

- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /includeadditional "Citrix Backup and Restore"`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestore`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestorecleanup`



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

Step 2. View precheck results

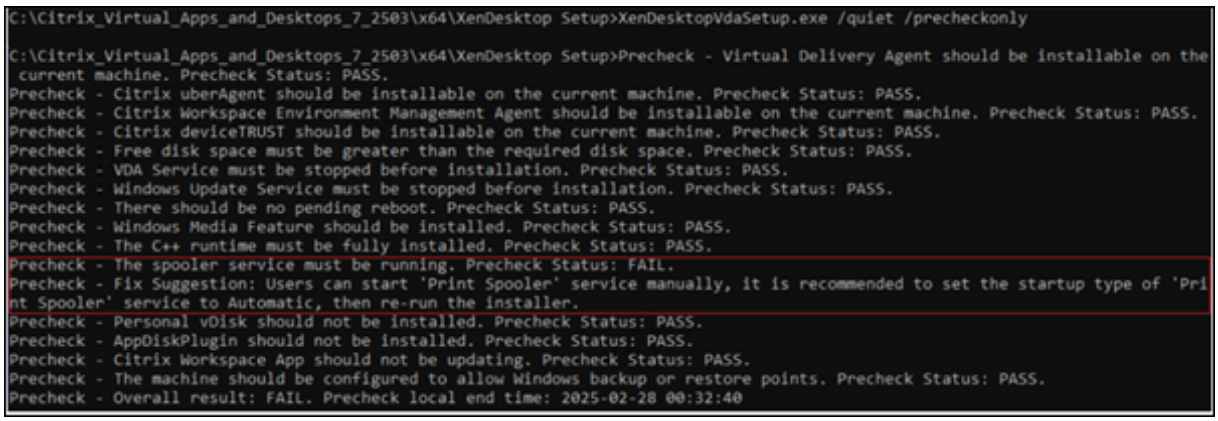
The precheck results are displayed in the command line, logged in `%temp%/Citrix/XenDesktop Installer/XenDesktop Installation.log` and saved in `%temp%/Citrix/XenDesktop Installer/PrecheckResult_{ yyyyMMddHHmmss } .json`. If the precheck fails, the overall result is `FAIL`, with suggested fixes for each issue.

Command line output

The precheck results in the command line include:

- Precheck criteria
- Precheck status
- Fix suggestions for failure
- Overall result
- End time.

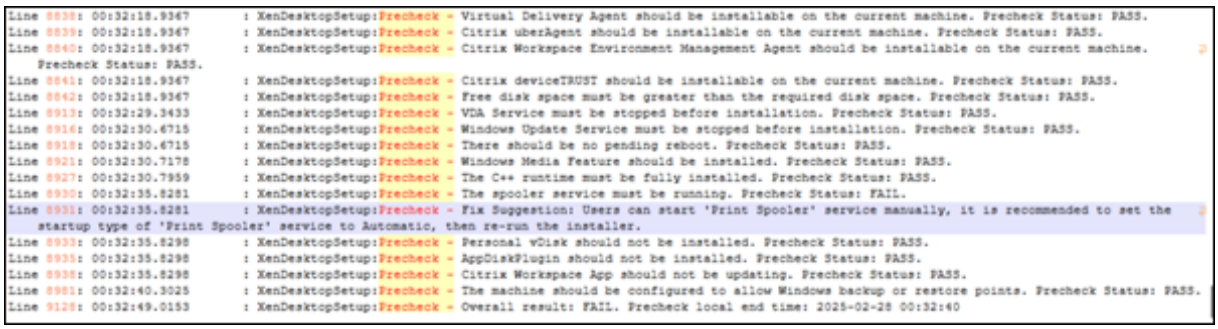
If the result is a `FAIL`, the suggestions to fix are available in the lines starting with **Precheck - Fix Suggestion:**



Log output

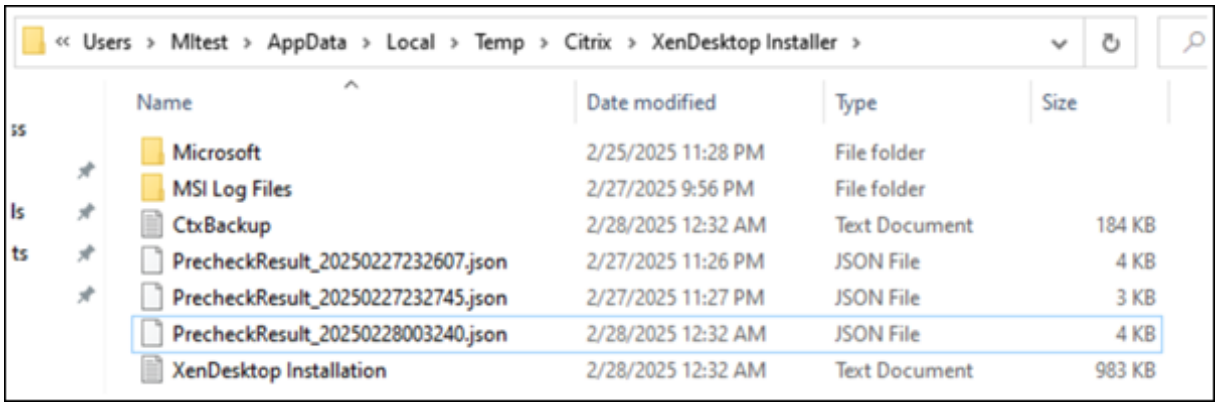
The pre-check results in `XenDesktop Installation.log` mirror those shown in the command line. To locate them, search for `Precheck -` in the log file.
If the overall result is a `FAIL`, the suggestions to fix are available in lines containing `Precheck - Fix Suggestion:`.

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



JSON output

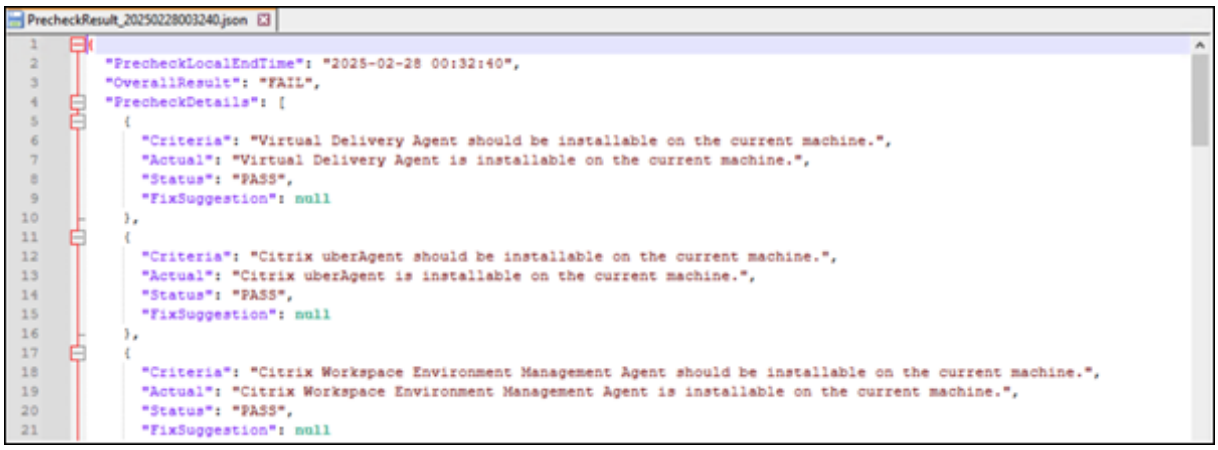
A `.json` file is generated every time a command with `/quiet /precheckonly` is run. The file is named `PrecheckResult_{ yyyyMMddHHmmss } .json`, with a timestamp suffix.



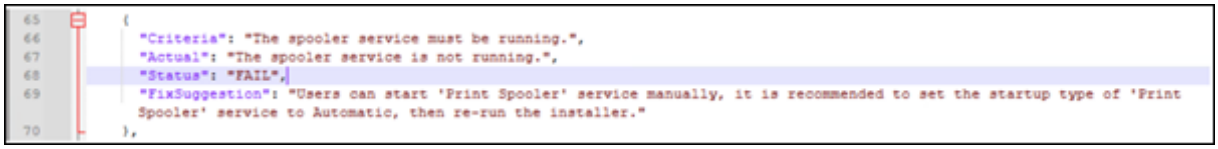
The `.json` file includes:

- Pre-check local end time
- Overall result
- Pre-check details
    - Criteria
    - Actual value
    - Status
    - Fix suggestion

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



Fix suggestions for each pre-check item with a status of `FAIL` can be found under the pre-check details section in the `.json` file.



Install VDAs using scripts

September 6, 2025

> **Note:**
>
> Citrix is not responsible for issues caused by scripts that are adapted to match customer production environments. For any install related Citrix issues, open a technical support case with the relevant install logs using the Citrix Support portal.

This article applies to installing VDAs on machines with Windows operating systems. For information about VDAs for Linux operating systems, see the Linux Virtual Delivery Agent documentation.

The installation media contains sample scripts that install, upgrade, or remove Virtual Delivery Agents (VDAs) for machines in Active Directory. You can also use the scripts to maintain master images used by Machine Creation Services™ and Citrix Provisioning (formerly Provisioning Services).

Required access:

- The scripts need Everyone Read access to the network share where the VDA installation command is located. The installation command is `XenDesktopVdaSetup.exe` in the full product ISO, or `VDAWorkstationSetup.exe` or `VDAServerSetup.exe` in a standalone installer.

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

- Logging details are stored on each local machine. To log results centrally for review and analysis, the scripts need Everyone Read and Write access to the appropriate network share.

To check the results of running a script, examine the central log share. Captured logs include the script log, the installer log, and the MSI installation logs. Each installation or removal attempt is recorded in a time-stamped folder. The folder title indicates the operation result with the prefix PASS or FAIL. You can use standard directory search tools to find a failed installation or removal in the central log share. Those tools offer an alternative to searching locally on the target machines.

Before beginning any installation, read and complete the tasks in Prepare to install.

Install or upgrade VDAs using the script

1. Obtain the sample script **InstallVDA.bat** from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script:
    - Specify the version of the VDA to install: `SET DESIREDVERSION`. The full value can be found on the installation media in the ProductVersion.txt file. However, a complete match is not required.
    - Specify the network share where the installer will be invoked. Point to the root of the layout (the highest point of the tree). The appropriate version of the installer (32-bit or 64-bit) is called automatically when the script runs. For example: `SET DEPLOYSHARE=\\fileserver1\share1`.
    - Optionally, specify a network share location for storing centralized logs. For example: `SET LOGSHARE=\\fileserver1\log1`).
    - Specify VDA configuration options as described in Install using the command line. The `/quiet` and `/noreboot` options are included by default in the script and are required: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`.
3. Using Group Policy Startup Scripts, assign the script to the OU containing your machines. This OU should contain only machines on which you want to install the VDA. When the machines in that OU are restarted, the script runs on all of them. A VDA is installed on each machine that has a supported operating system.

Remove VDAs using the script

1. Obtain the sample script UninstallVDA.bat from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script.

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

- Specify the version of the VDA to remove: `SET CHECK\\_VDA\\_VERSION`. The full value can be found on the installation media in the ProductVersion.txt file (such as 7.0.0.3018). However, a complete match is not required.
- Optionally, specify a network share location for storing centralized logs.

3. Using Group Policy Startup Scripts, assign the script to the OU containing your machines. This OU should contain only machines from which you want to remove the VDA. When the machines in the OU are restarted, the script runs on all of them. The VDA is removed from each machine.

Troubleshoot

- The script generates internal log files that describe script execution progress. The script copies a `Kickoff_VDA_Startup_Script` log to the central log share within seconds of starting the deployment. You can verify that the overall process is working. If this log is not copied to the central log share as expected, troubleshoot further by inspecting the local machine. The script places two debugging log files in the `%temp%` folder on each machine:

  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  Review these logs to ensure that the script is:

  - Running as expected.
  - Properly detecting the target operating system.
  - Correctly configured to point to the `ROOT` of the `DEPLOYSHARE` share (contains the file named `AutoSelect.exe`).
  - Capable of authenticating to both the `DEPLOYSHARE` and `LOG` shares.

- For information about how Citrix reports the result of component installations, see Citrix installation return codes.
- In the Studio display for a delivery group, the **Installed VDA version** entry in the **Details** pane might not be the version installed on the machines. The machine's programs and features display shows the actual VDA version.
- After a VDA is installed, it cannot deliver apps or a desktop to users until it registers with a Delivery Controller.

  To learn about VDA registration methods and how to troubleshoot registration issues, see VDA registration.

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

Third-party VDA deployment methods

September 6, 2025

To successfully deploy a Virtual Delivery Agent (VDA) using Microsoft System Center Configuration Manager (SCCM) or similar software distribution tools, such as Ansible and Microsoft Intunes, Citrix® recommends using the VDA installer in a sequence of steps.

> **Note:**
>
> The following articles describe only recommendations based on how Citrix has tested the environment. You can customize these steps according to your needs. Citrix is not responsible for any updates or tweaks needed to this to fit customer needs.

- Install VDAs using SCCM
- Install VDAs using Ansible
- Install VDAs using Microsoft Intune

Install VDAs using SCCM

September 6, 2025

Overview

Microsoft Endpoint Configuration Manager, formerly System Center Configuration Manager (SCCM) is a Windows product that enables the management, deployment, and security of devices and applications across an enterprise.

> **Note:**
>
> The following article describes only recommendations based on how Citrix® has tested the environment. You can customize these steps according to your needs. Citrix is not responsible for any updates or tweaks needed to this to fit customer needs.

Recommendations

- To successfully deploy a Virtual Delivery Agent (VDA) using SCCM or similar software distribution tools, Citrix recommends using the VDA installer in a sequence of steps.
- Citrix does not recommend using the VDA Cleanup Utility as part of a VDA installation or upgrade. Use the VDA Cleanup Utility only in the limited case when the VDA installer has previously failed.

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

Before you begin

The required number of restarts during the installation of the VDA depends on the environment. For example:

- A restart might be required for pending updates or restarts from earlier software installations.
- Files previously locked by other processes might need updates, forcing an extra restart.
- Some optional components in the VDA installer (such as Citrix Profile Management and Citrix Files) might require a restart.
- When you upgrade a VDA, the machine on which it is installed must be in maintenance mode, with no sessions.
- When a VDA installation runs for the first time on a machine, the VDA installer being used is copied onto that machine.
  For more information on VDA installation, see Installers.

SCCM Task Sequencer manages all required restarts.

Key steps to deploy VDA using SCCM

The following steps describe how to deploy VDA using SCCM on the virtual machine.

1. Install the VDA.
2. Create an organization unit (OU).
3. Verify the machines.
4. Use VDA to distribute content.

Step 1: Install the VDA

After identifying all prerequisites, use **SCCM Task Sequencer** to complete the following tasks:

1. Install the VDA from an accessible copy of the installation media or from one of the VDA stand-alone installers:

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   For more information about VDA installers, see Installers.

   > **Note:**

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

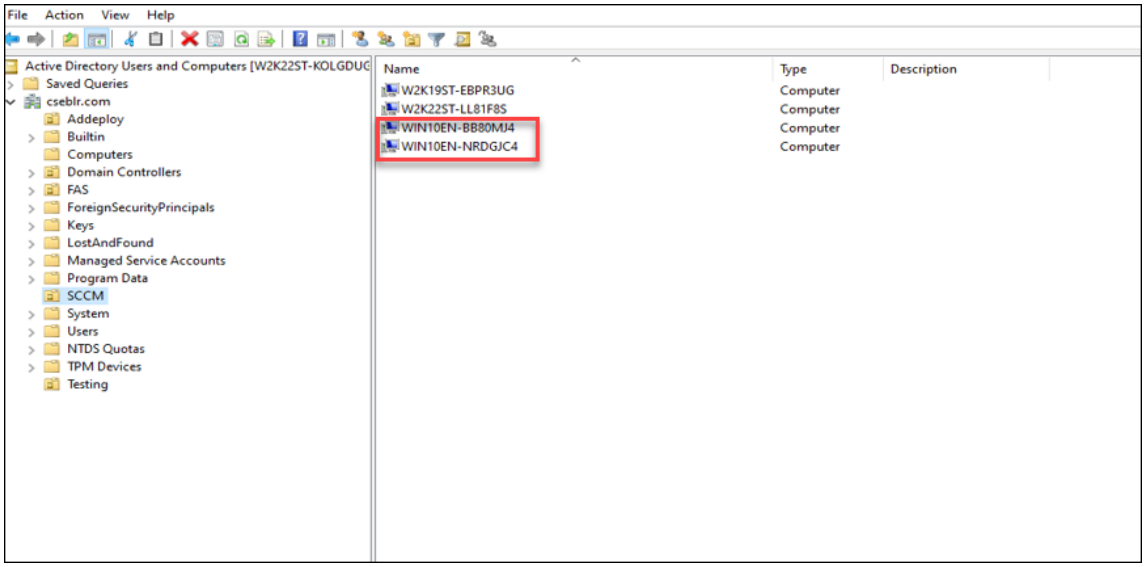
> When you upgrade a VDA, the machine on which it is installed must be in maintenance mode, with no sessions.

2. When a VDA installation runs for the first time on a machine, the VDA installer being used is copied onto that machine.
   - When you use a VDA installer other than `VDAWorkstationCoreSetup_XXXX.exe`, the VDA installer is copied to `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
   - When you use `VDAWorkstationCoreSetup_XXXX.exe`, the VDA installer is copied to `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`.
3. The directory location of the VDA installer is also stored in the registry `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall" "MetaInstallerInstallLocation"`.
4. Add the command-line options `/NOREBOOT`, `/NORESUME`, and `/QUIET` to your command-line options.
   - `/QUIET`: Don't show the user interface during installation, so that SCCM has control of the installation process.
   - `/NOREBOOT`: Suppress the VDA installer from restarting automatically. SCCM triggers restarts when needed.
   - `/NORESUME`: Usually, when a restart is needed during the installation, the VDA installer sets a runonce registry key (`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`). Windows uses the key to open the VDA installer when the machine restarts. This is an issue for SCCM, because SCCM cannot monitor the installation and capture the exit code.

Step 2: Create an organization unit (OU)

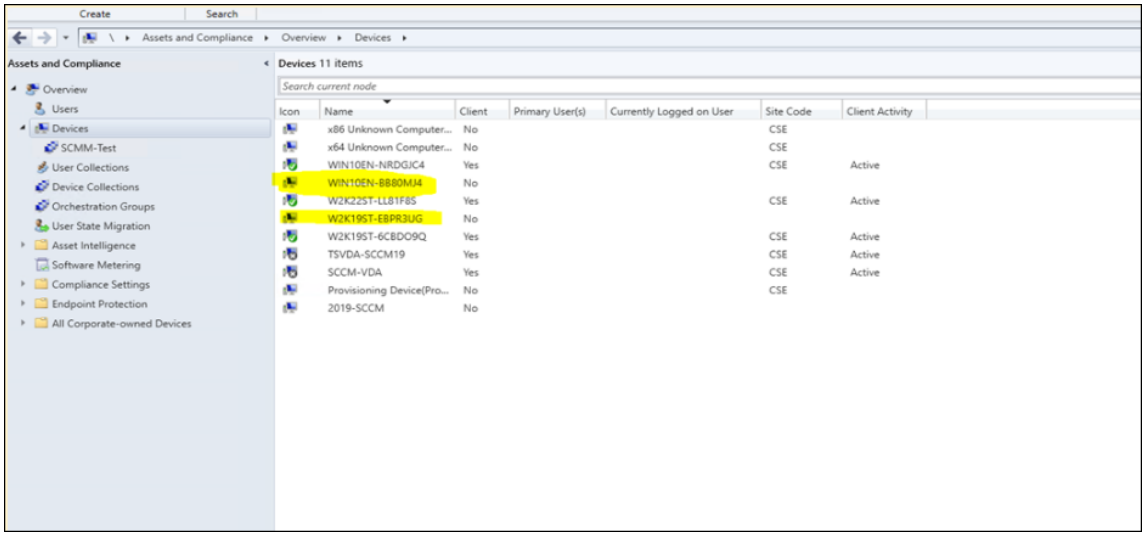
1. Create two domain-joined virtual machines you want to add to the OU. When the virtual machines are initially created, they are in the **Computers** folder. Move the virtual machines to the **SCCM** folder.
   Example: WIN10EN-BB80MJ4.cseblr.com
   W2K19ST-EBPR3UG.cseblr.com

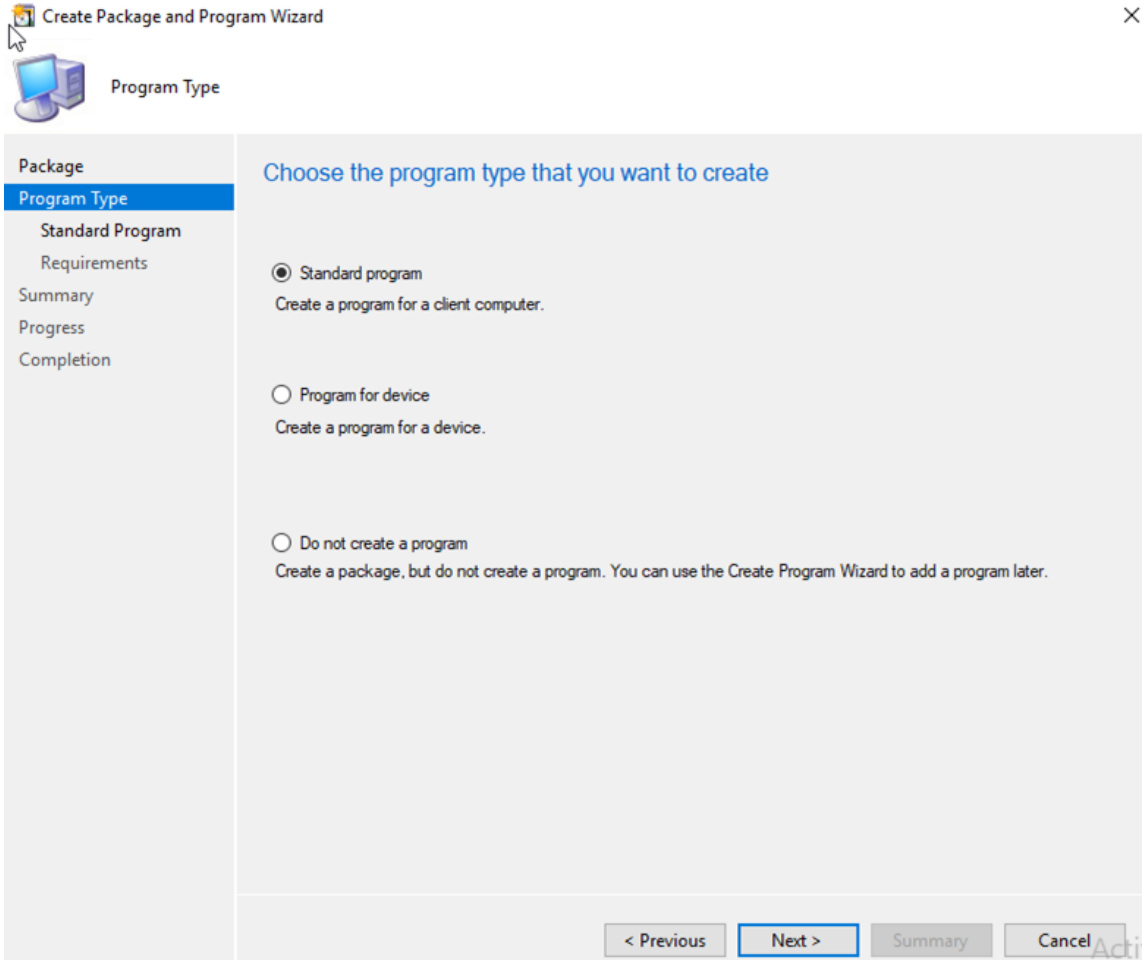
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. In Microsoft Configuration Manager, go to `\Administration\Overview\Hierarchy Configuration\Discovery Methods\`.
3. Click **Active Directory System Discovery**, and select the **Enable Active Directory System Discovery** check box to enable auto-discovery of the newly created virtual machines.
4. Click the icon to select new containers.
5. In the **Location** section, add the **Path** where your SCCM virtual machines are located.
6. Go to `\Administration\Overview\Site Configuration\Sites` and right-click the SCCM VDA.
7. Select **Client Installation Settings > Client Push Installation**. The **Client Push Installation Properties** window opens.
8. Once the VMs are set to `Enabled`, you can see the list of VMs as illustrated in the following images.

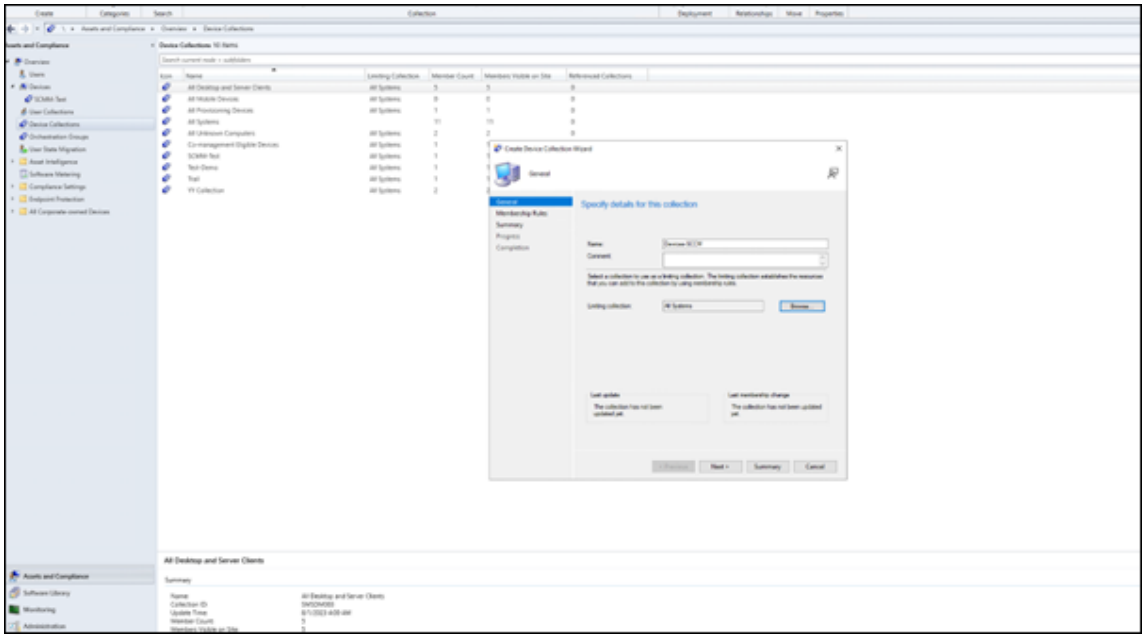
© 1997–2026 Citrix Systems, Inc. All rights reserved.



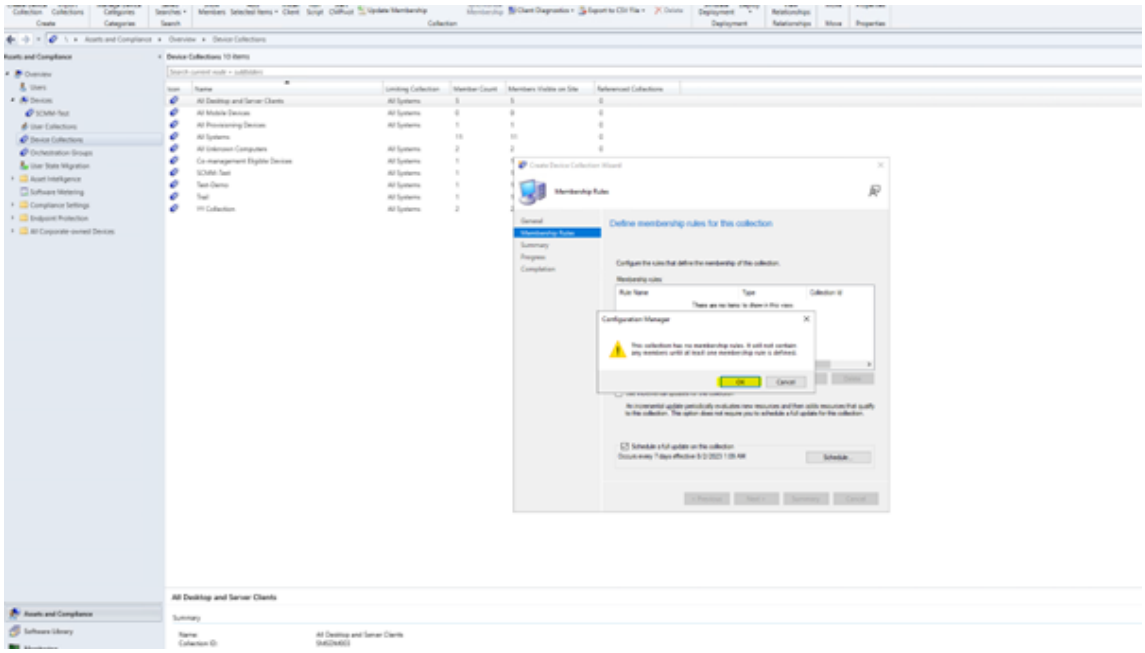


9. Create **Device collection** to create the OU. Enter the **Name** of the Collection Name.

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

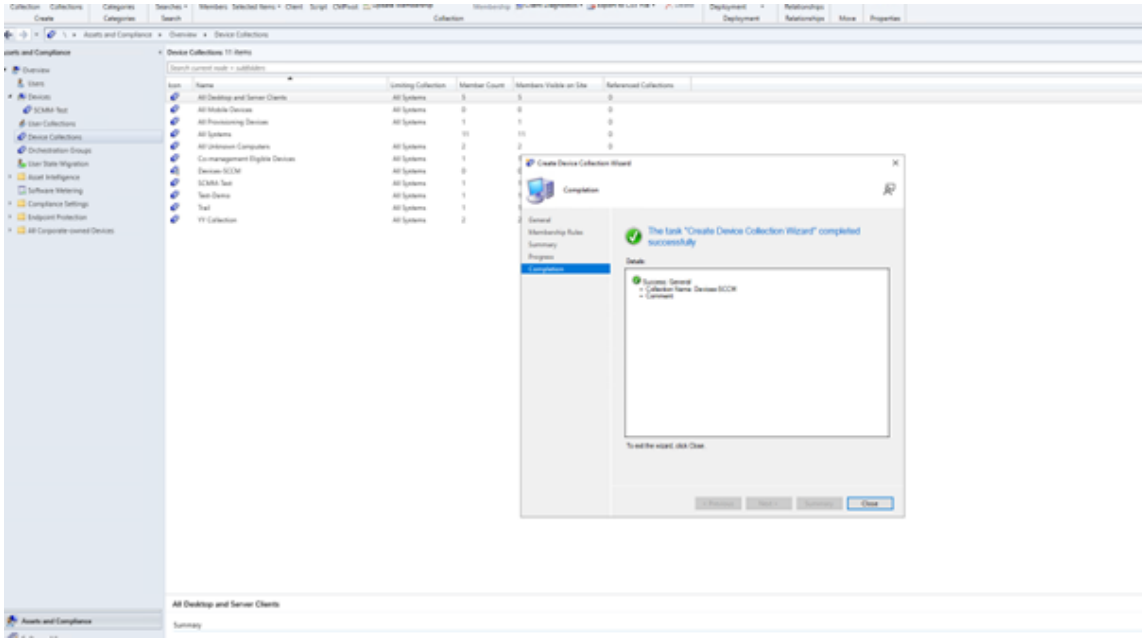


10. Follow the wizard instructions.



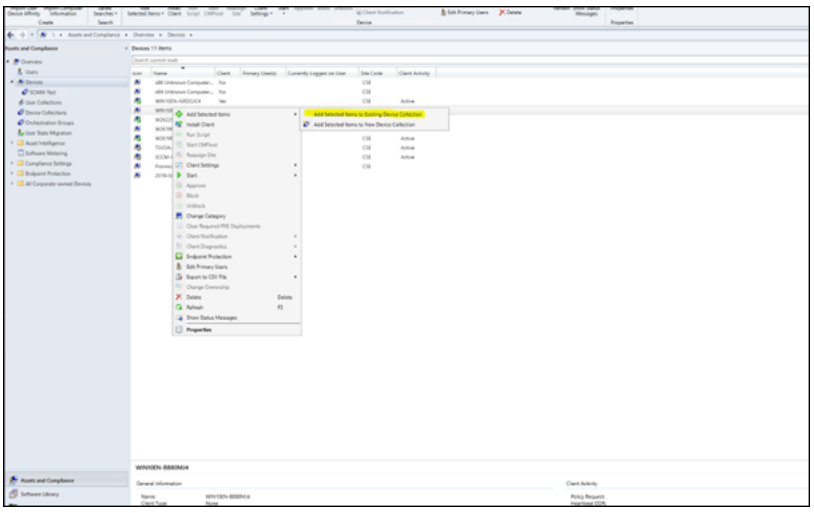
The OU is created.

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



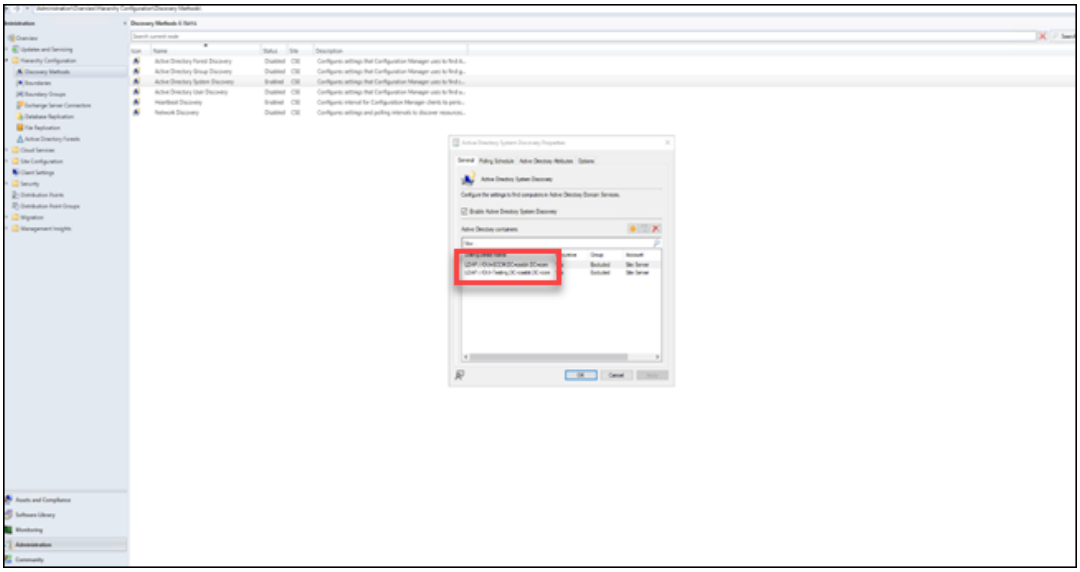
11. Add the created VMs to the newly created Device Collection.

    a) Right-click the VM. Select **Add Selected Items > Add Selected Items to Existing Device Collection**.

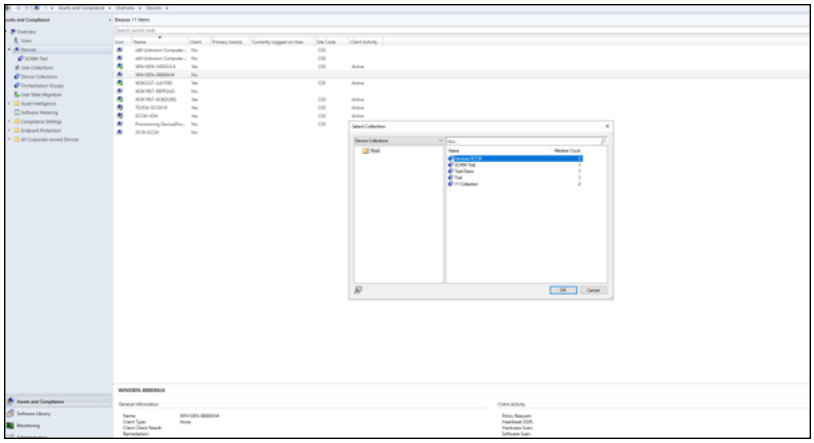


    b) In the **Select Collection** window, select the required device name. In this example, it is `Devices-SCCM`.

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

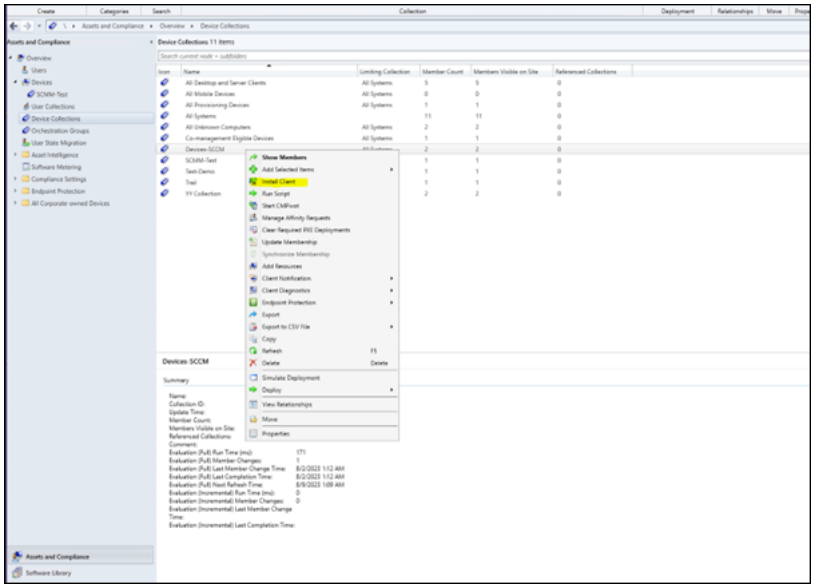


`Devices-SCCM` is listed in **Assets and Compliance > Overview > Device Collections**.

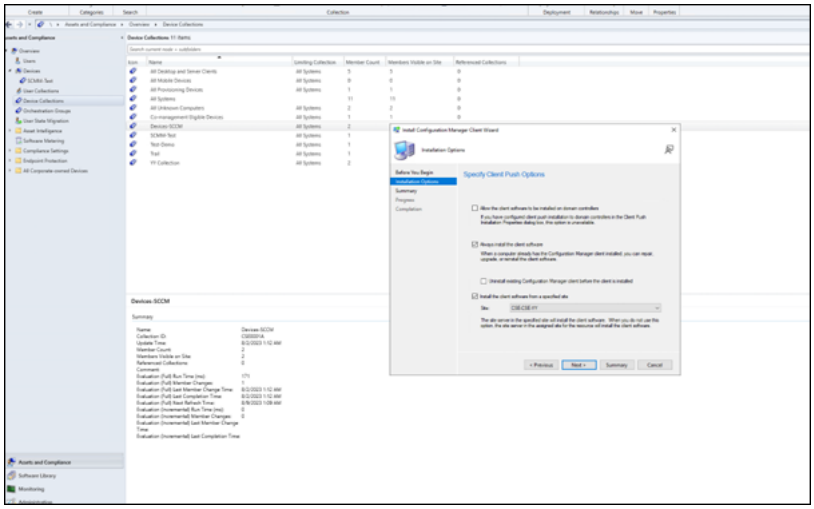


12. Select **Install Client** on Device Collector.

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

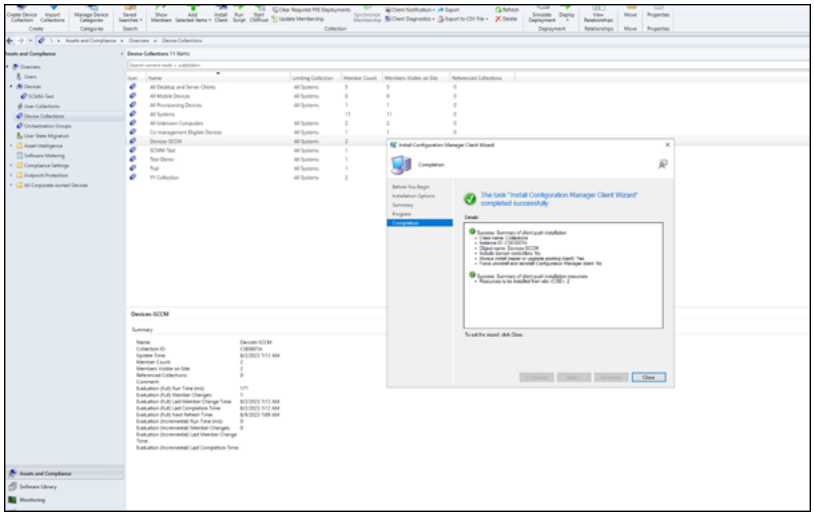


13. Select the required installation **Site**.



14. Follow the wizard instructions. **Install Configuration Manager Client Wizard** is completed successfully.

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

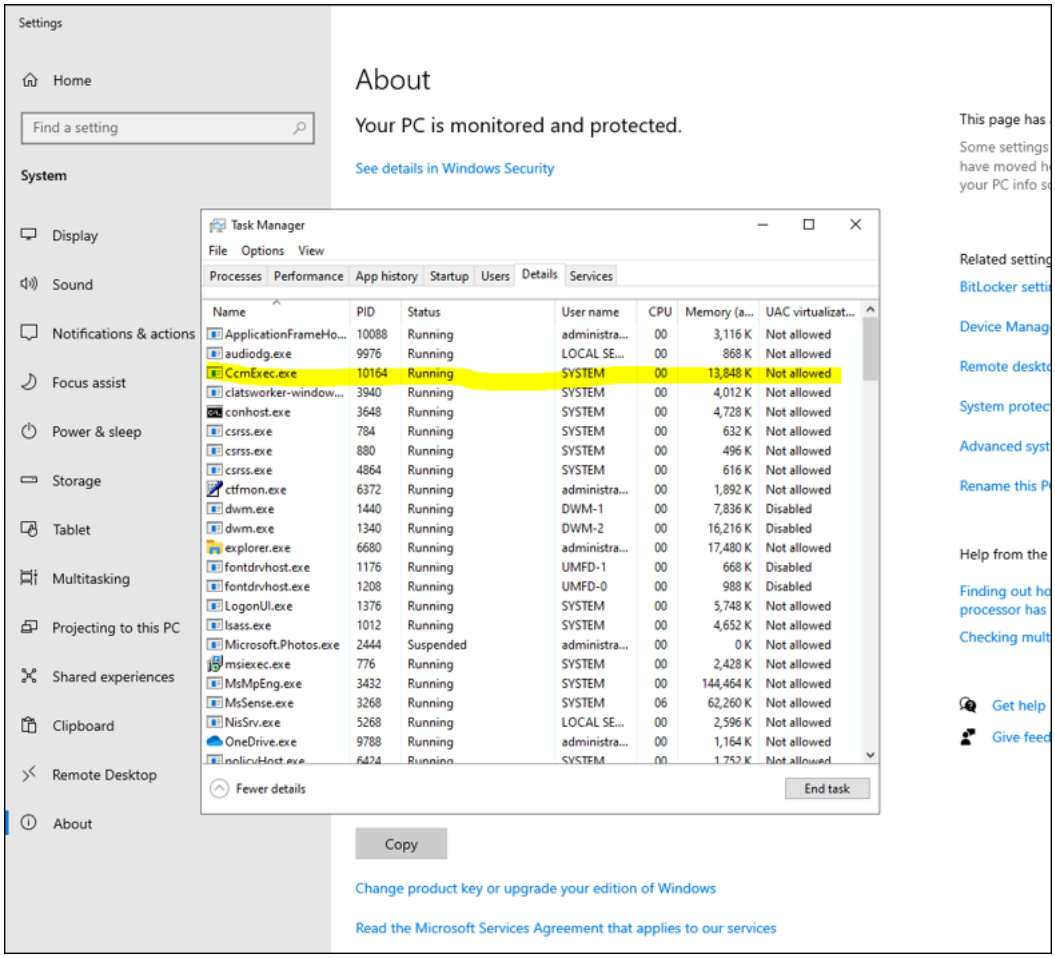


For detailed information, see Manage collections in the Microsoft documentation.

Step 3: Verify the machines

1. On the client machine, verify that the client is installed by checking if the `CCMExec` process is running.

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



2. Verify if the Client is running for the VMs on SCCM.

Step 4: Use VDA to distribute content

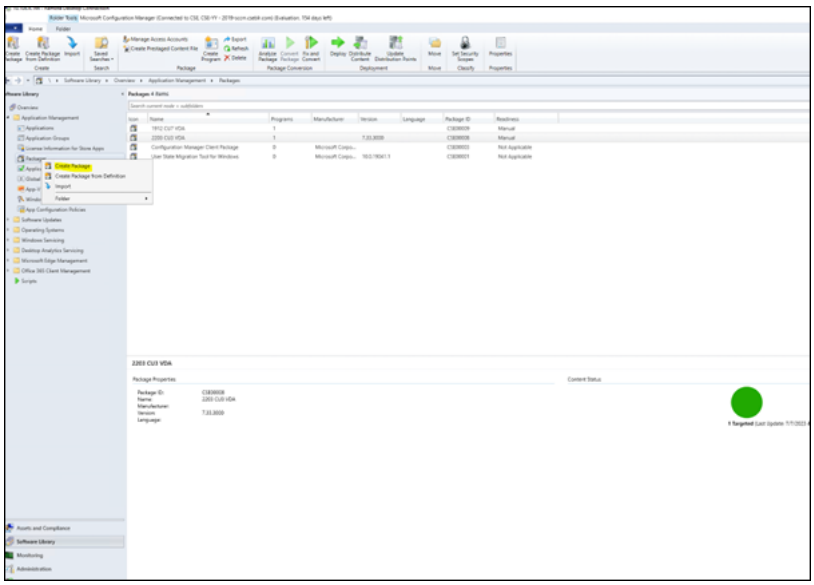
The following steps describe how you can use the deployed VDA to distribute content on the associated virtual machines.

1. Create a package
2. Distribute content

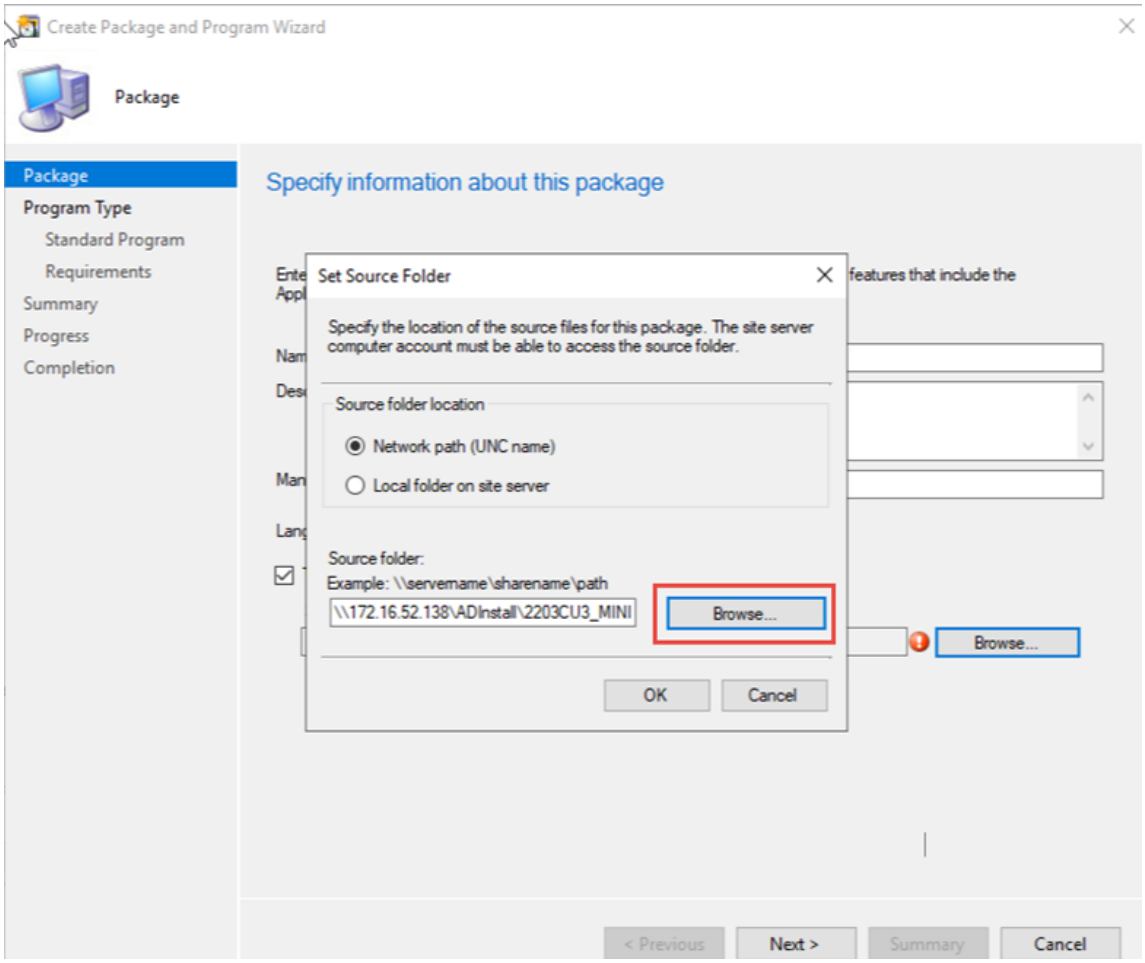
Create a package

1. To create a package, right-click the VDA you want and click **Create Package**.

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

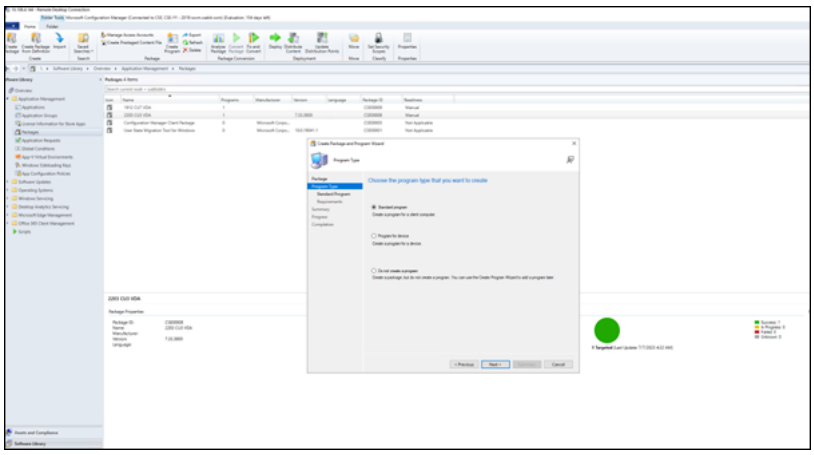


2. Specify the location of the source files for this package by clicking **Browse**.

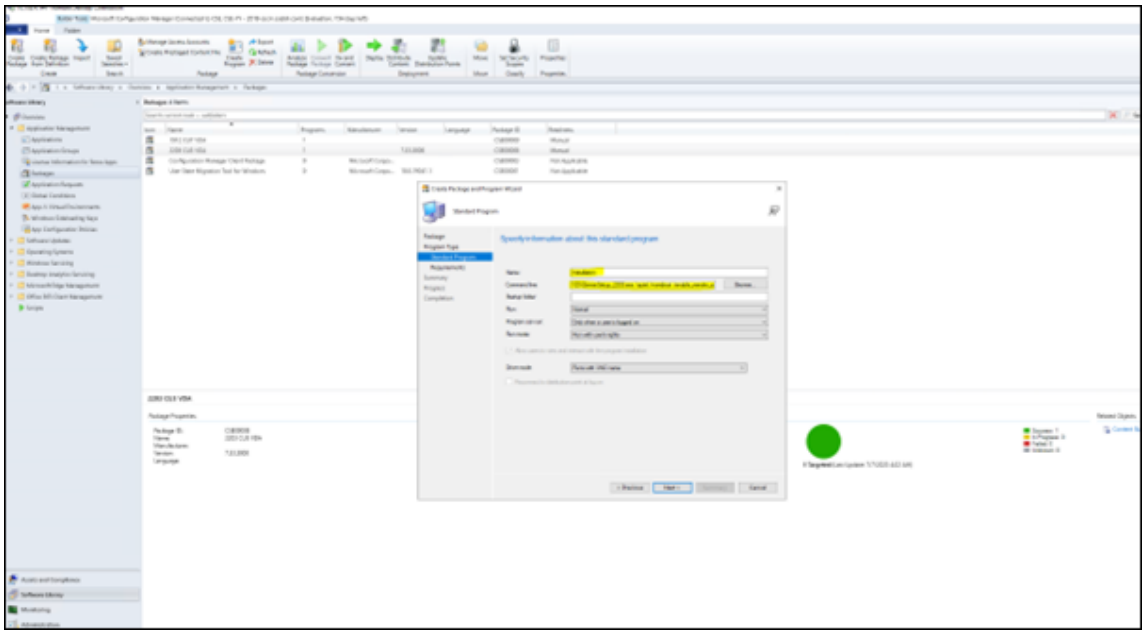


3. Select the package type that you want.

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

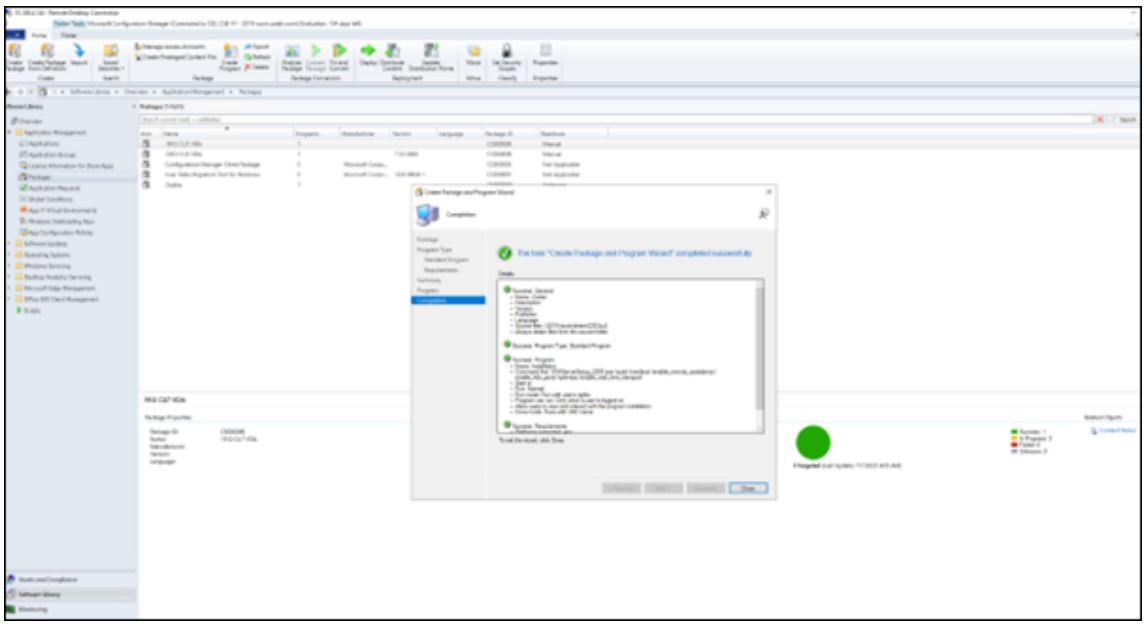


4. Enter the package **Name** and **Command line**.



5. Click **Next**.

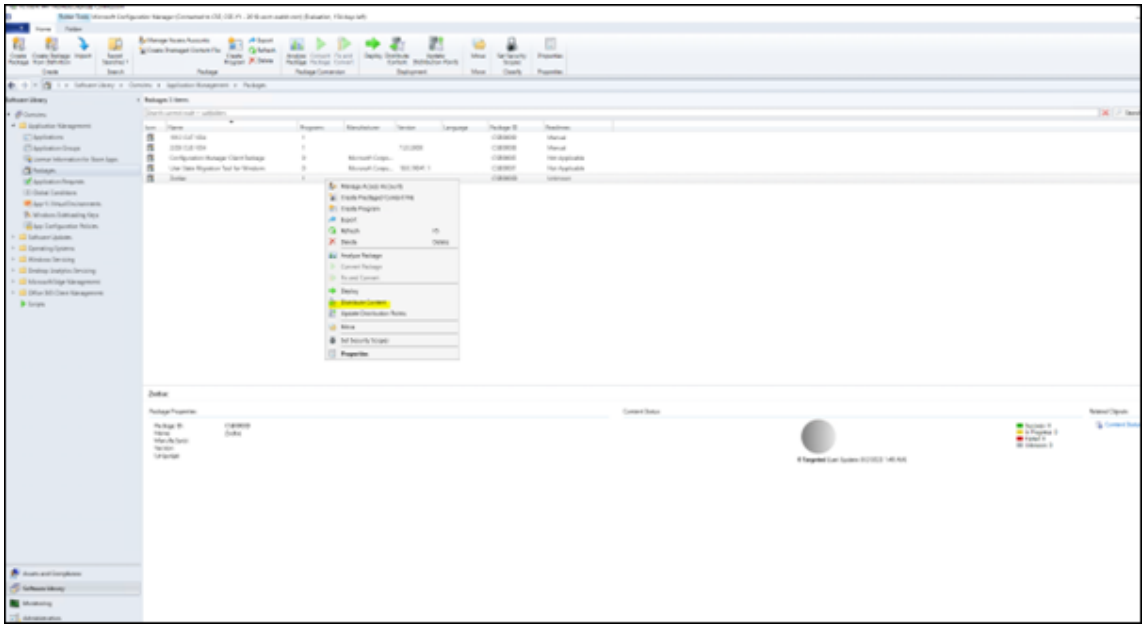
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For detailed information, see the Packages and programs in Configuration Manager in the Microsoft documentation.

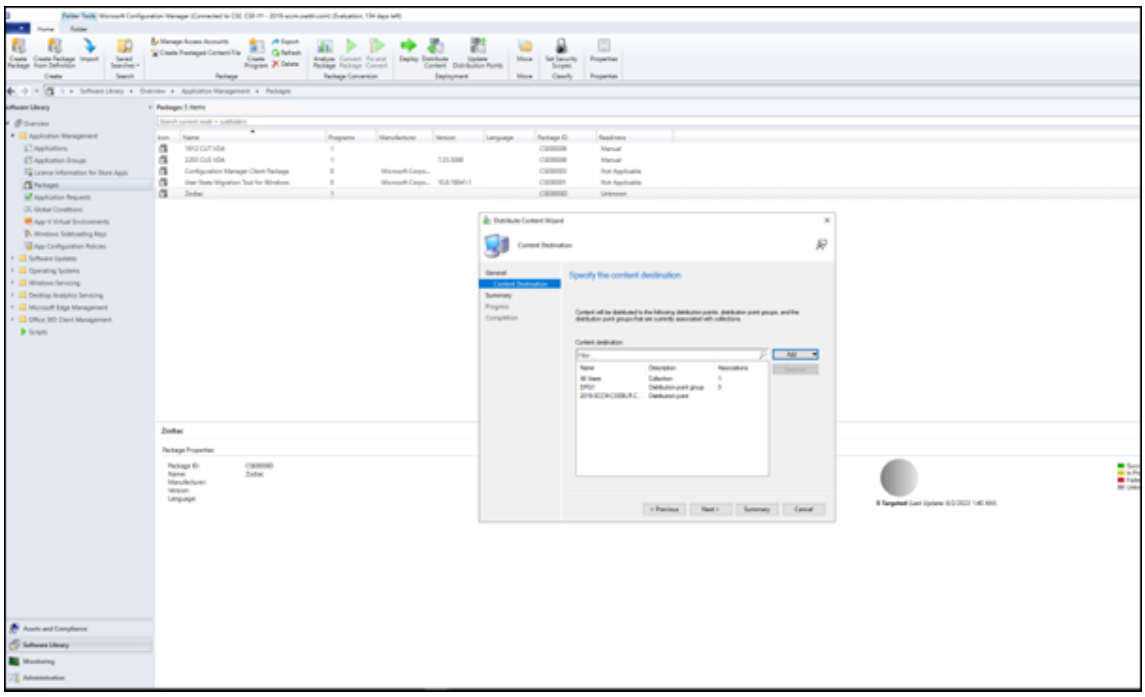
Distribute content

1. Right-click the package name you have created.
2. Select **Distribute Content**.

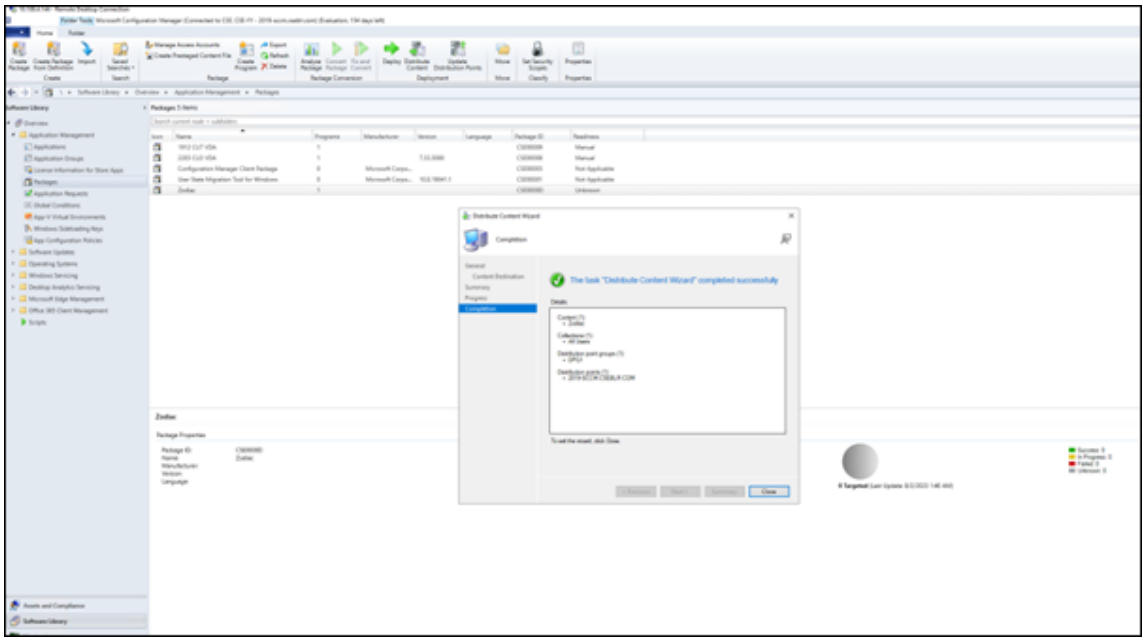


3. In the **Distribute Content Wizard** window, select the location of the source files for the package that you have created. In this example, it is `2019-SCCM`. Click **Next**.

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

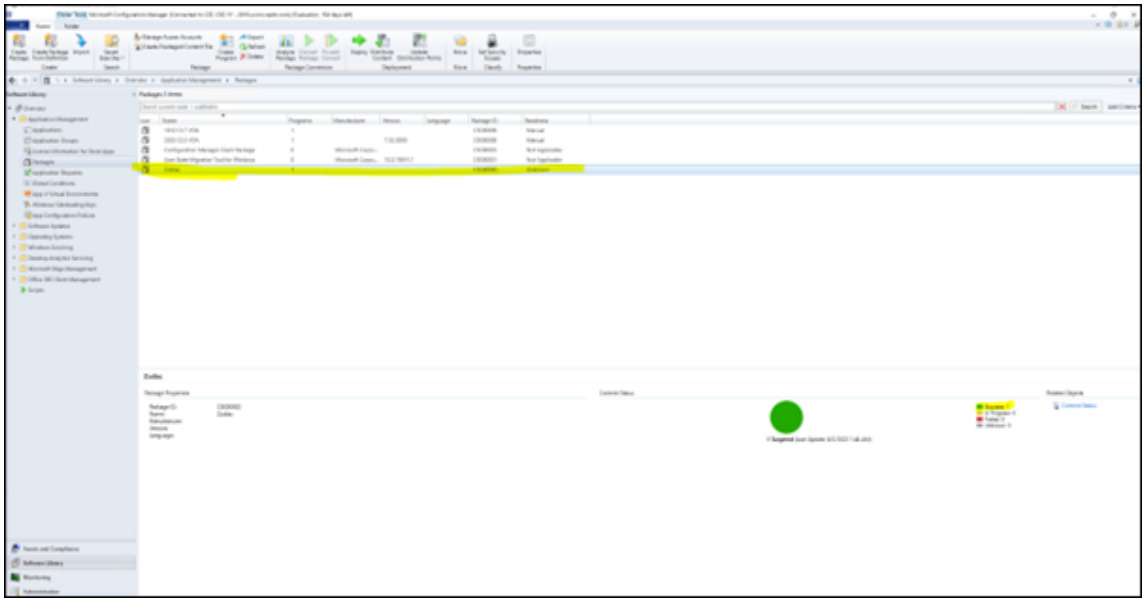


4. Verify that the Package (in this example, `Zodiac`) is available to deploy.



The following image illustrates that the package is available to deploy.

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

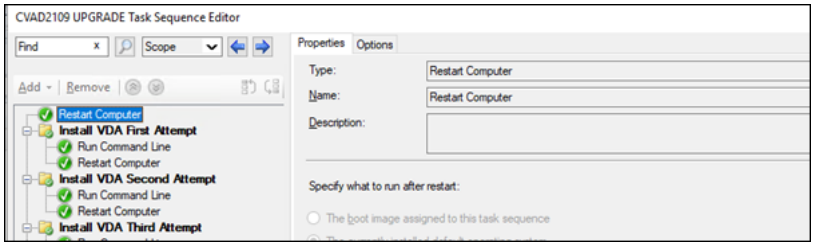


For detailed information, see Deploy and manage content for Configuration Manager in the Microsoft documentation.

Example installation sequence using SCCM

The following example shows the installation sequence.

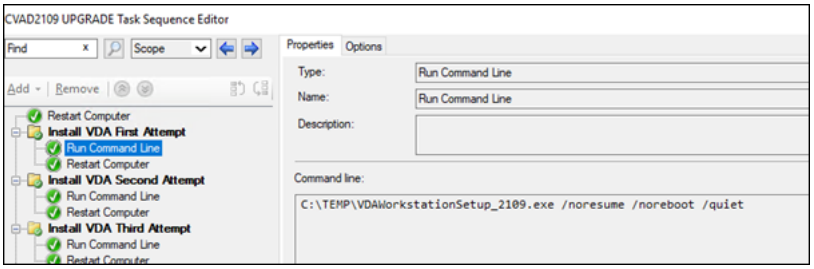
1. **Restart Computer:** Prepare the machine by restarting the machine.



2. **Install VDA First Attempt:** Start the VDA installation.

   a) Add the `/quiet`, `/noreboot`, and `/noresume` options to your command-line options.

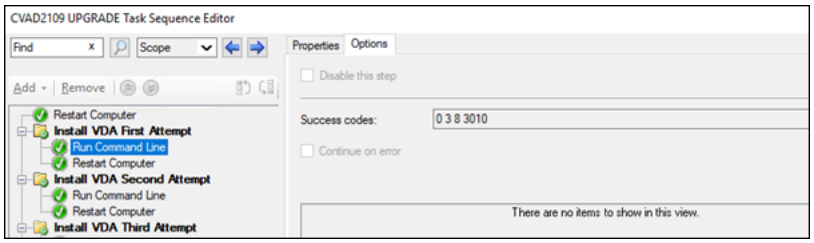
   b) Run the VDA installer of your choice (local image or one of the minimal installers).



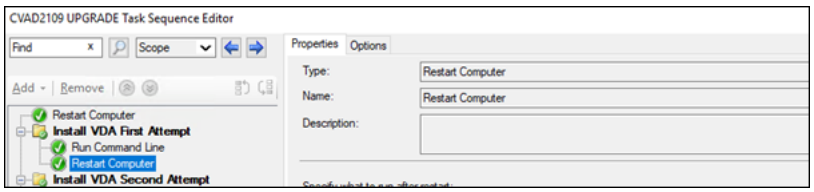
© 1997–2026 Citrix Systems, Inc. All rights reserved.

c) SCCM must capture the return code.

- If the return code is 0 or 8, the installation is complete, and a restart is needed.

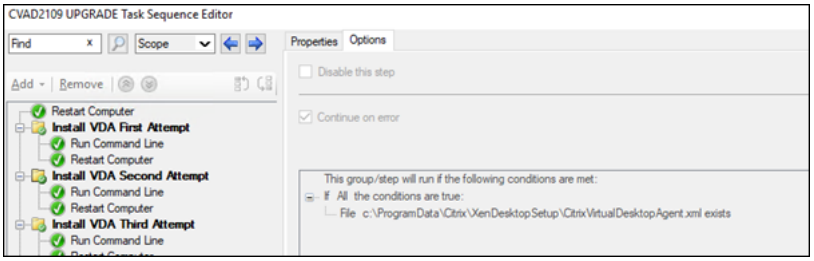


- If a return code is 3, restart the machine and then pass control to **Install VDA Second Attempt**.



3. **Install VDA Second Attempt:** Continue VDA installation.

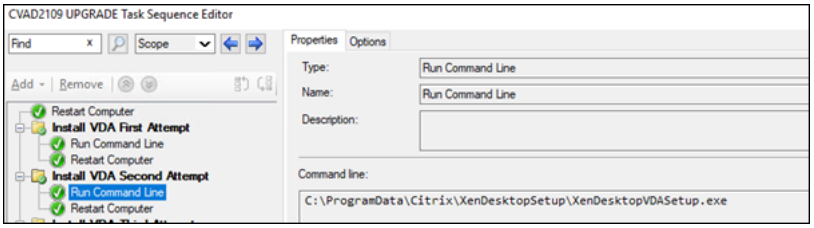
a) After **Install VDA First Attempt** if the file `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` exists, the installation is not complete and must be continued after the restart completes.



b) **Install VDA Second Attempt** repeats until the file `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` does not exist or a return code other than 0 or 8 is returned. Treat any other return code as an error, and INSTALL VDA SECOND ATTEMPT should report an error and stop.

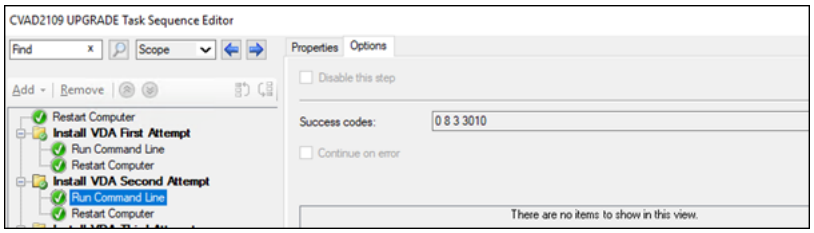
c) Resume the VDA installation by running the appropriate VDA installer (`XenDesktopVdaSetup.exe` for most cases, or `XenDesktopRemotePCSetup.exe` if `VDAWorkstationCoreSetup_X.exe` was used) from the file `%programdata%\Citrix\XenDesktopSetup\` directory with no command-line parameters. (The VDA installer uses the parameters it saved during the first run of the installer.)

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



d) Watch for the return code from the VDA installer.

- 0 or 8: Success, installation complete, restart required.



- 3: Installation is not complete. Restart the machine and repeat INSTALL VDA SECOND ATTEMPT until the file `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` does not exist or until a 0 or 8 is returned. Treat any other return code as an error, and INSTALL VDA SECOND ATTEMPT should report an error and end.

For more information about return codes see Citrix installation return codes.

VDA installation command examples

The available installation options vary, depending on which installer is used. See the following articles for command line option details.

- Install VDAs
- Install using the command line

Installation commands for Remote PC Access

- The following command uses the single-session core VDA installer (`VDAWorkstationCoreSetup.exe`):

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
  ```

- The following command uses the single-session full VDA installer (`VDAWorkstationSetup.exe`):

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

```
VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /
controllers “control.domain.com” /enable_hdx_ports /noresume /
noreboot
```

Installation command for dedicated VDI

- The following command uses the single-session full VDA installer (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “
  control.domain.com” /enable_hdx_ports /enable_remote_assistance /
  noresume /noreboot
  ```

Install VDAs using Microsoft Intune

September 6, 2025

Overview

This article describes how to deploy VDAs using Microsoft Intune. For more information, see the Microsoft documentation.

> **Note:**
>
> The following article describes only recommendations based on how Citrix® has tested the environment. You can customize these steps according to your needs. Citrix is not responsible for any updates or tweaks needed to this to fit customer needs.

Key steps to deploy VDA using Microsoft Intune

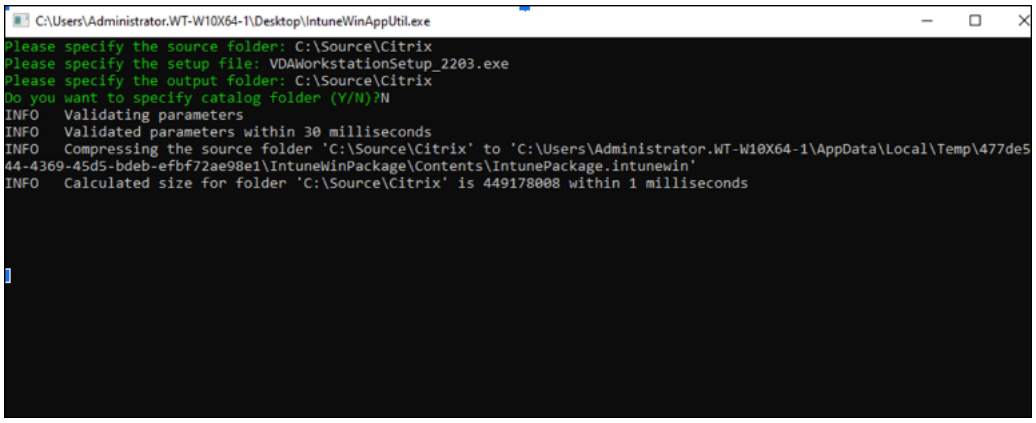
1. Prepare installation for the Citrix VDA.
2. Set up Microsoft 365 Developer Program Subscriber.
3. Add and assign an app.
4. Install the app on the enrolled device.

Step 1: Prepare installation for the Citrix VDA

1. Download the updated IntuneWinAppUtil.exe from GitHub.

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

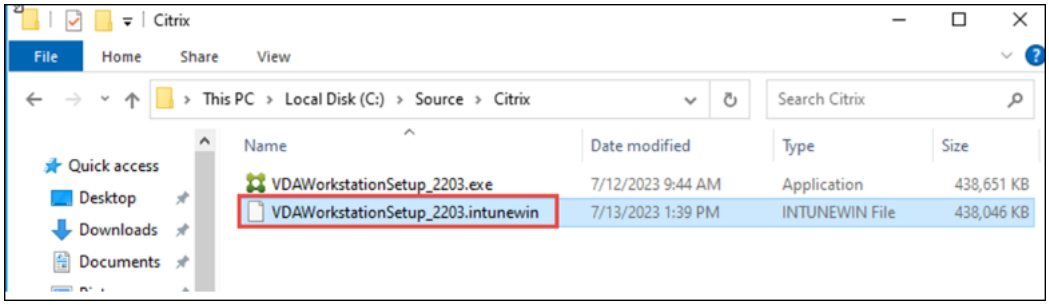
2. Run the `IntuneWinAppUtil.exe` file using **Run as administrator**.
3. Enter the following data:



   a) **Please specify the source folder**: Enter the folder that contains your application setup files. For example, C:\source\Citrix.
   b) **Please specify the setup file**: Enter the setup file name (such as setup.exe or setup.msi). For example, VDAWorkstationSetup_2203.exe.
   c) **Please specify the output folder**: Enter the path of the output folder to generate the .intunewin file. For example, C:\source\Citrix.
   d) **Do you want to specify catalog folder (Y/N)**: Type N.

> **Note:**
>
> Wait a few minutes while **Win32 Content Prep Tool** is running. Once it generates the `.intunewin` file, the status indicates 100% at the bottom of the command prompt.

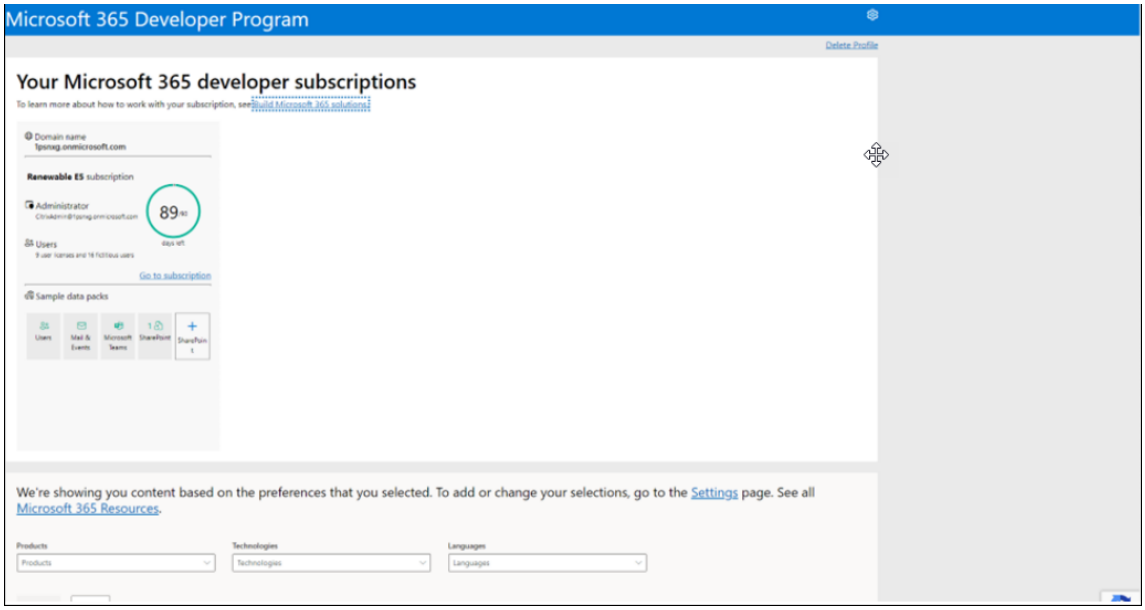
4. Once the process completes, go to the output folder (In this example, `C:\source\Citrix`) to get the Microsoft Intune deployment file.
5. Sign up for a Microsoft Intune free trial.



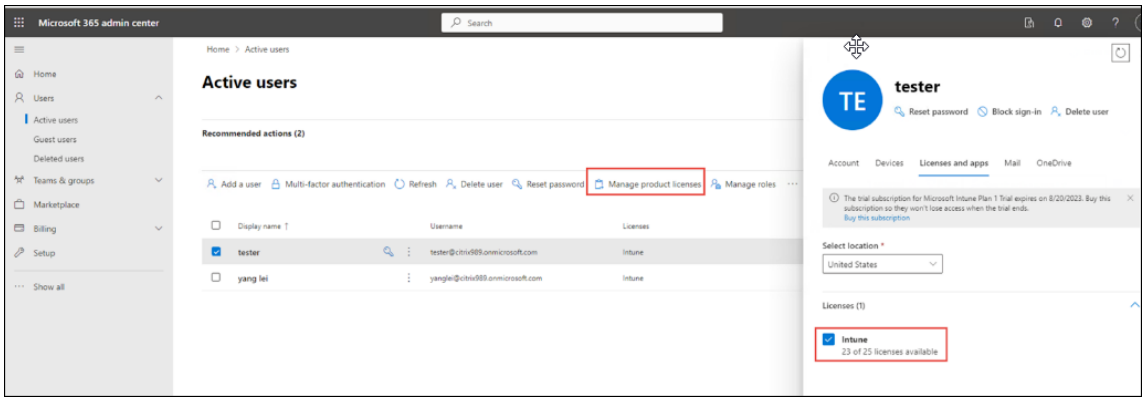
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Set up Microsoft 365 Developer Program Subscriber

1. Create the Instant sandbox to activate your subscription.
   To get your developer sandbox, go to your Microsoft 365 Developer Program dashboard and select **Add a new subscription**.

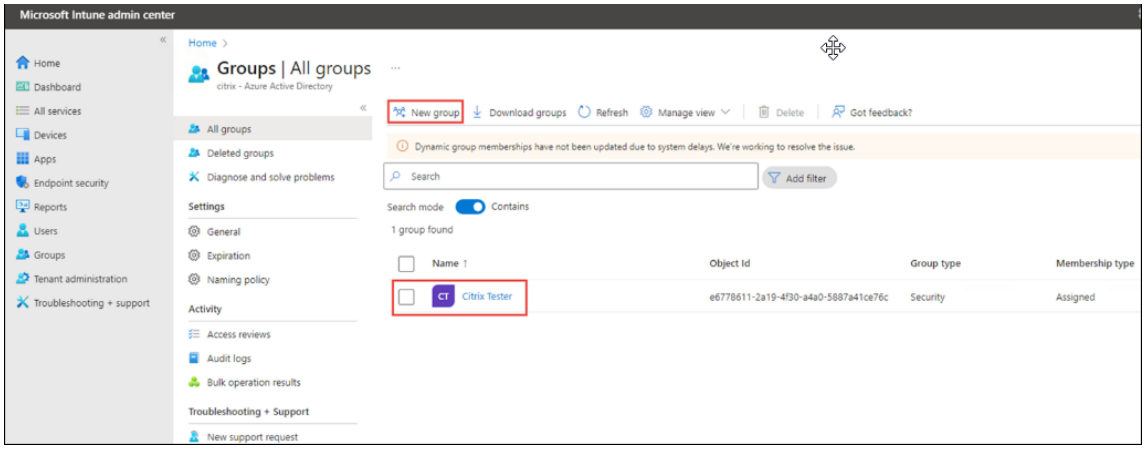


2. Create a user in the Microsoft 365 Admin center and assign a license to the user.



3. Create a group.

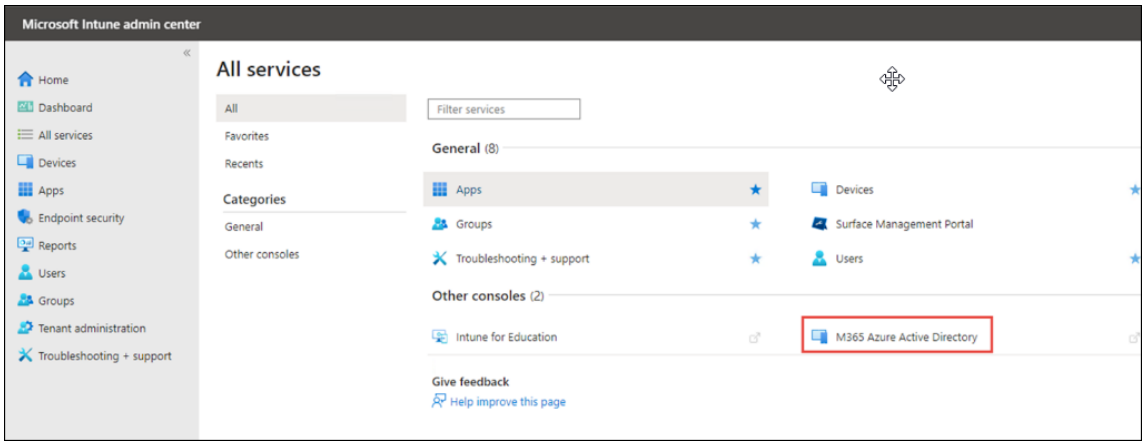
© 1997–2026 Citrix Systems, Inc. All rights reserved.



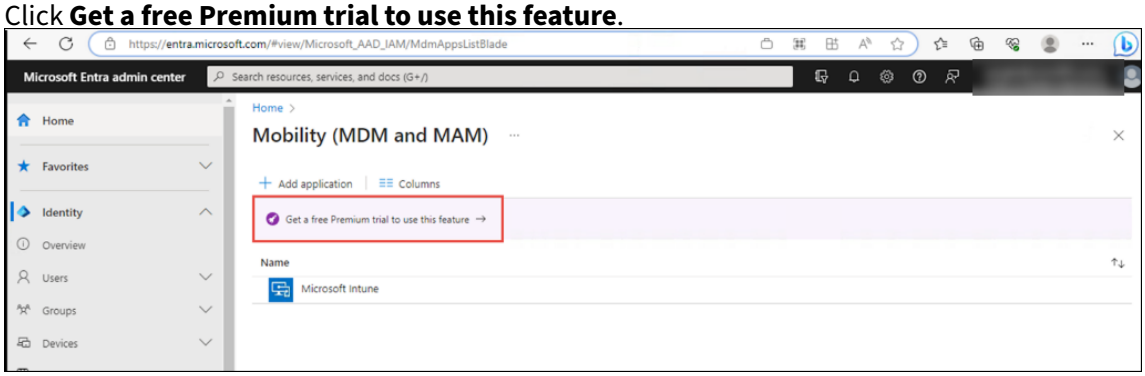
4. Once the group is created, you must provide the MDM authority to the group. Set up automatic enrollment. It can take a minute to activate.
   Or you can manually add the MDM authority to the group by completing the following steps:

   a) Go to **All services > Microsoft Entra**.
   b) Go to **settings > Mobility** and select **Microsoft Intune**.
   c) Select the group you have just created. This opens a page with the MDM user scope.
   d) Click **Save**.

5. In the **All Services** tab, click **M365 Azure Active Directory**.

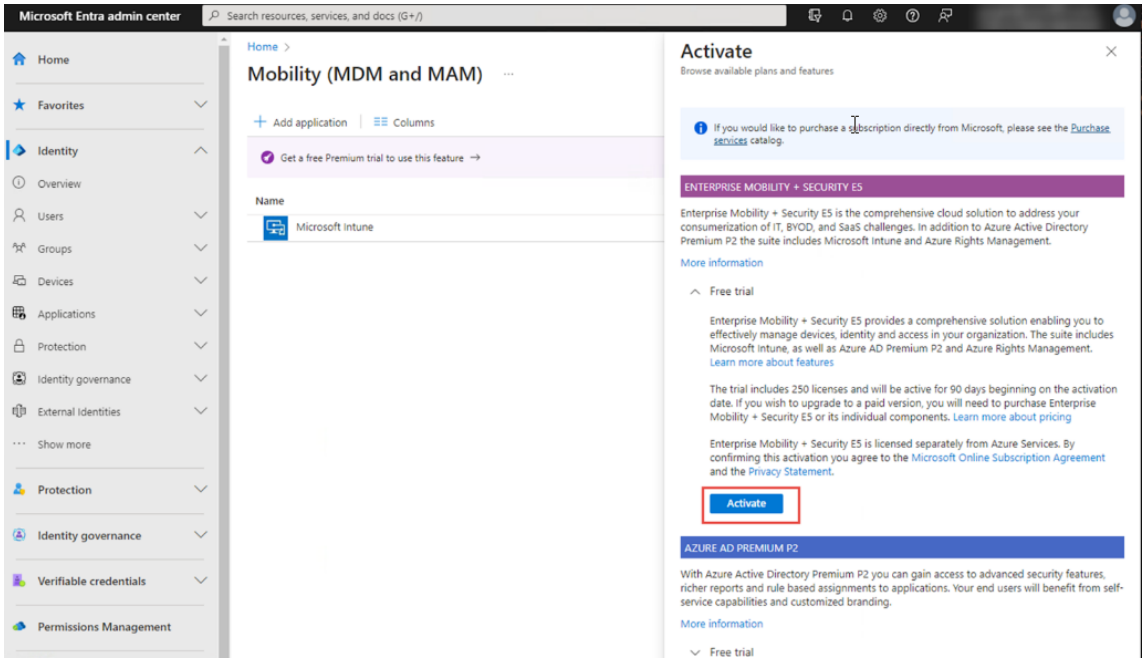


6. Click **Get a free Premium trial to use this feature**.

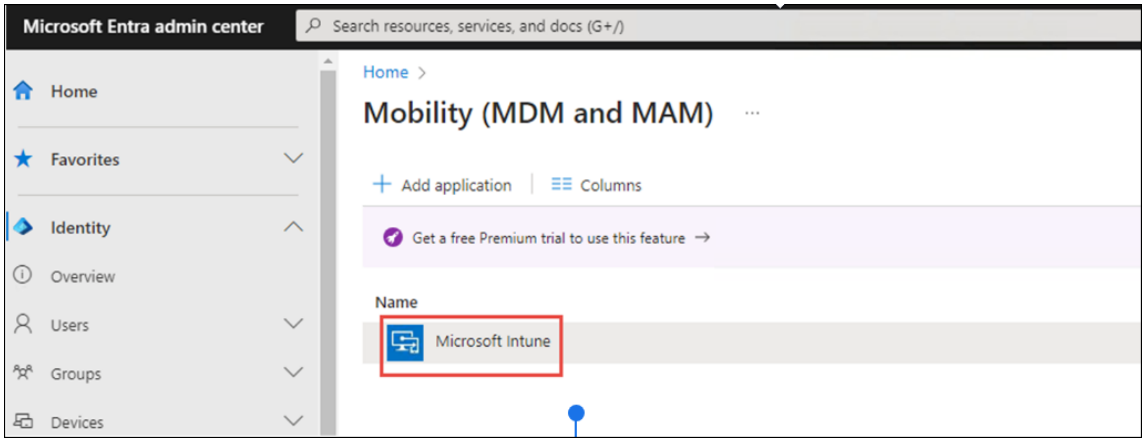


© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Click **Activate**.

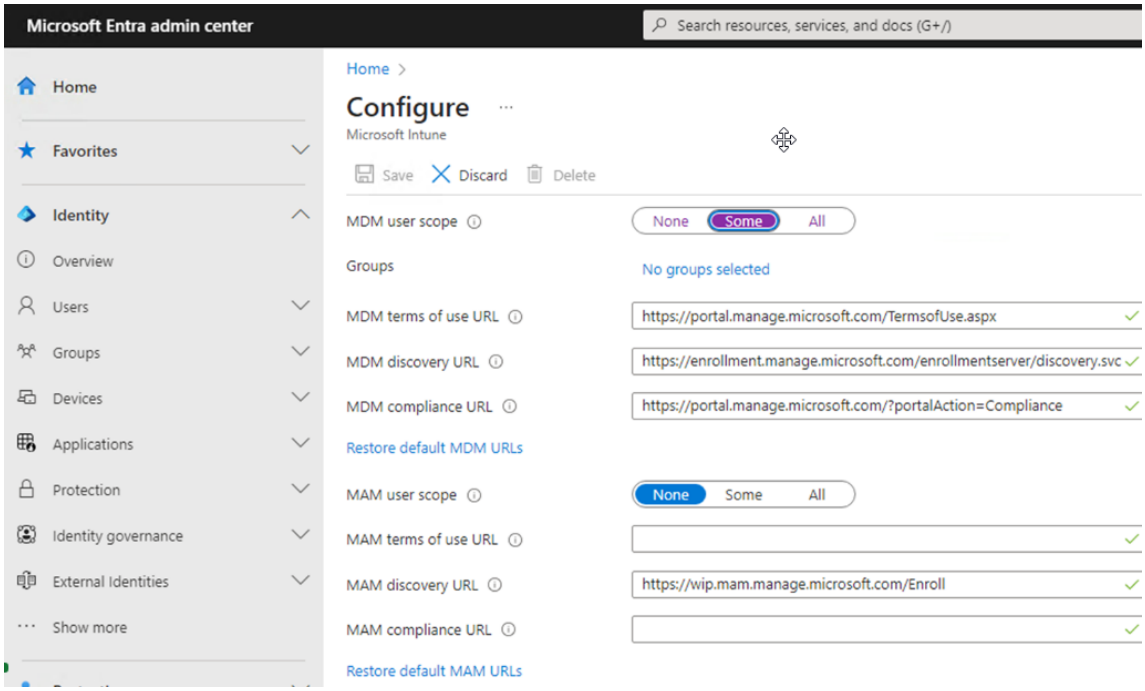


8. Now, click **Microsoft Intune**.

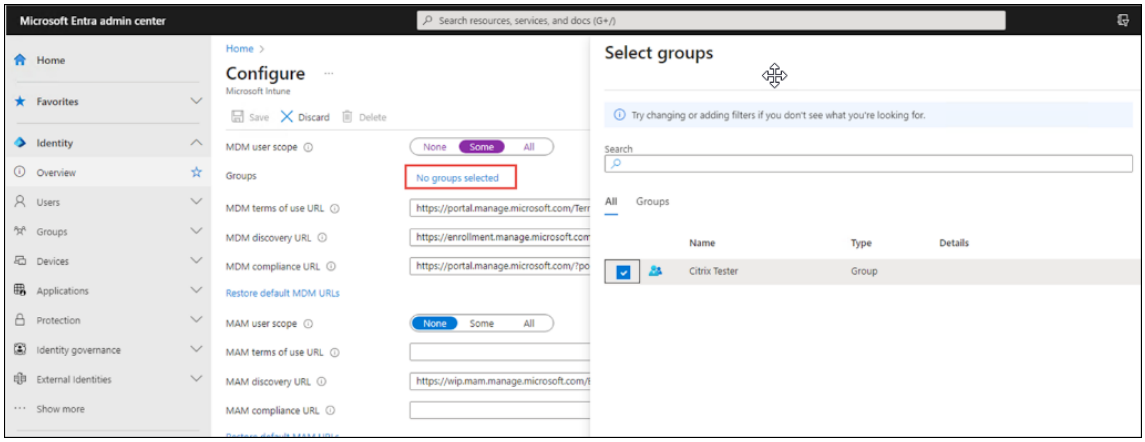


9. In the **Configure** tab, enter the required configurations.

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

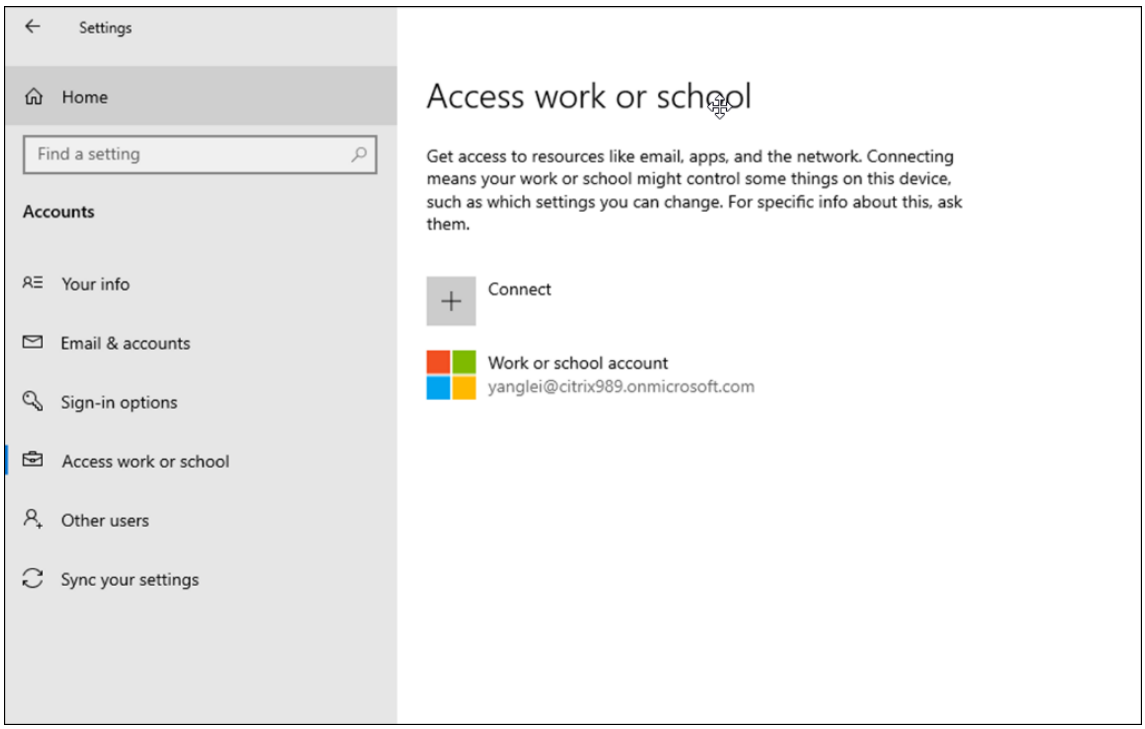


10. To add a group, click **No groups selected**.

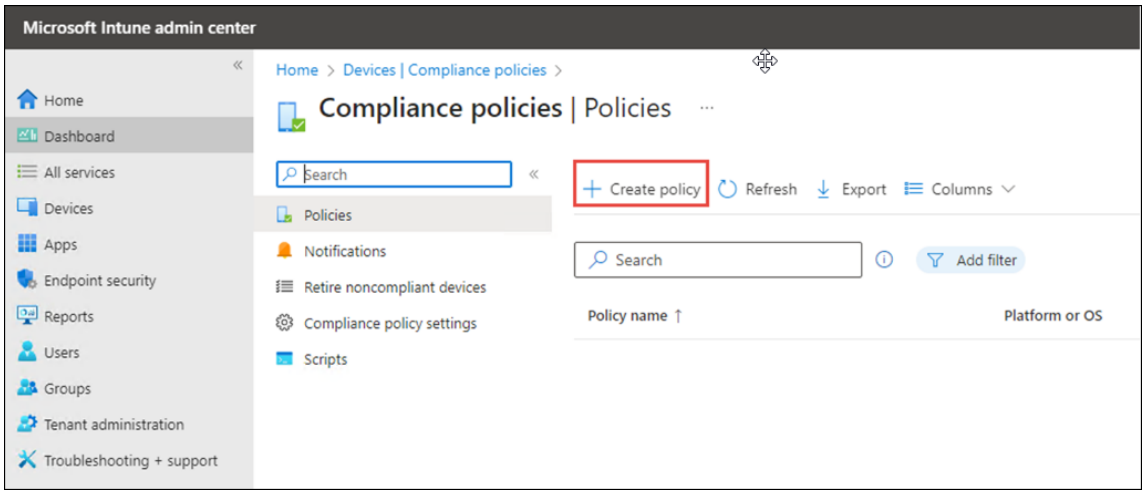


11. Enroll your device.

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

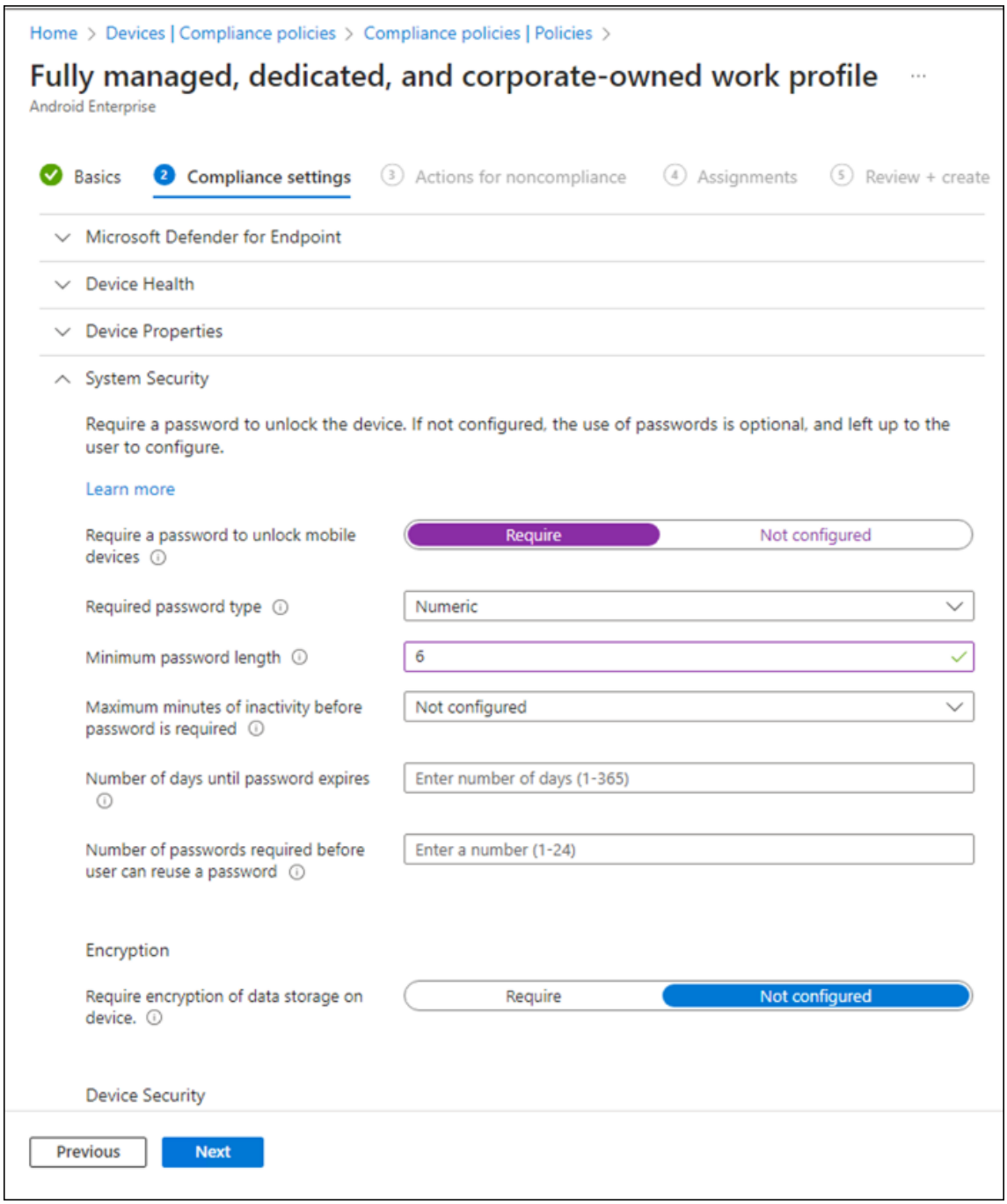


12. Create a device compliance policy to change your newly created Device's compliance to `Compliant`.



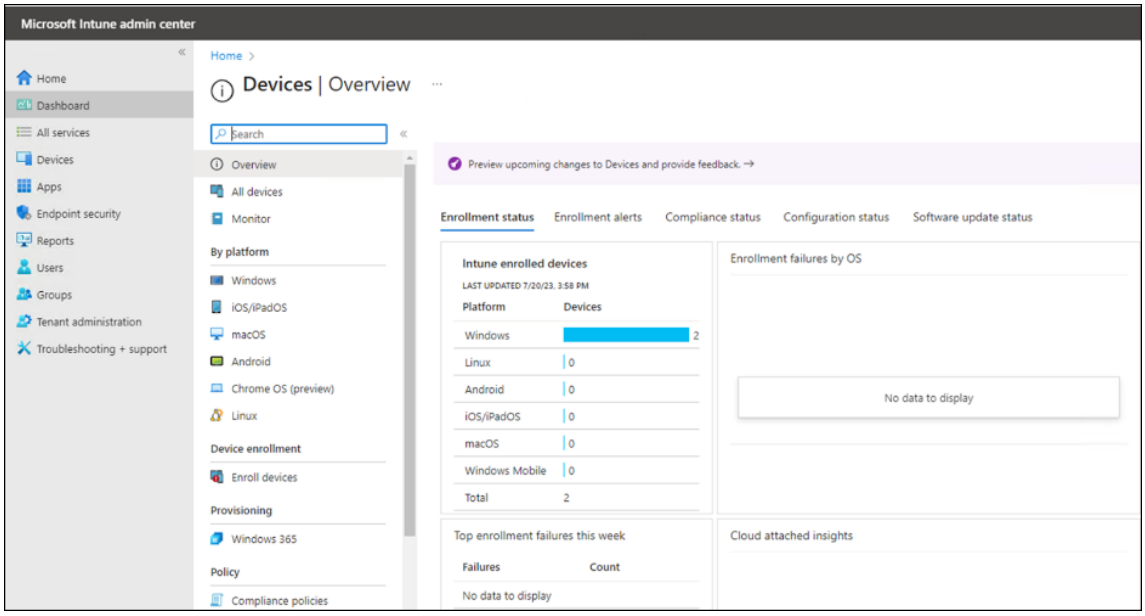
13. Go to the **Assignments** tab to add the newly created group.

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



14. Confirm the device enrollment.

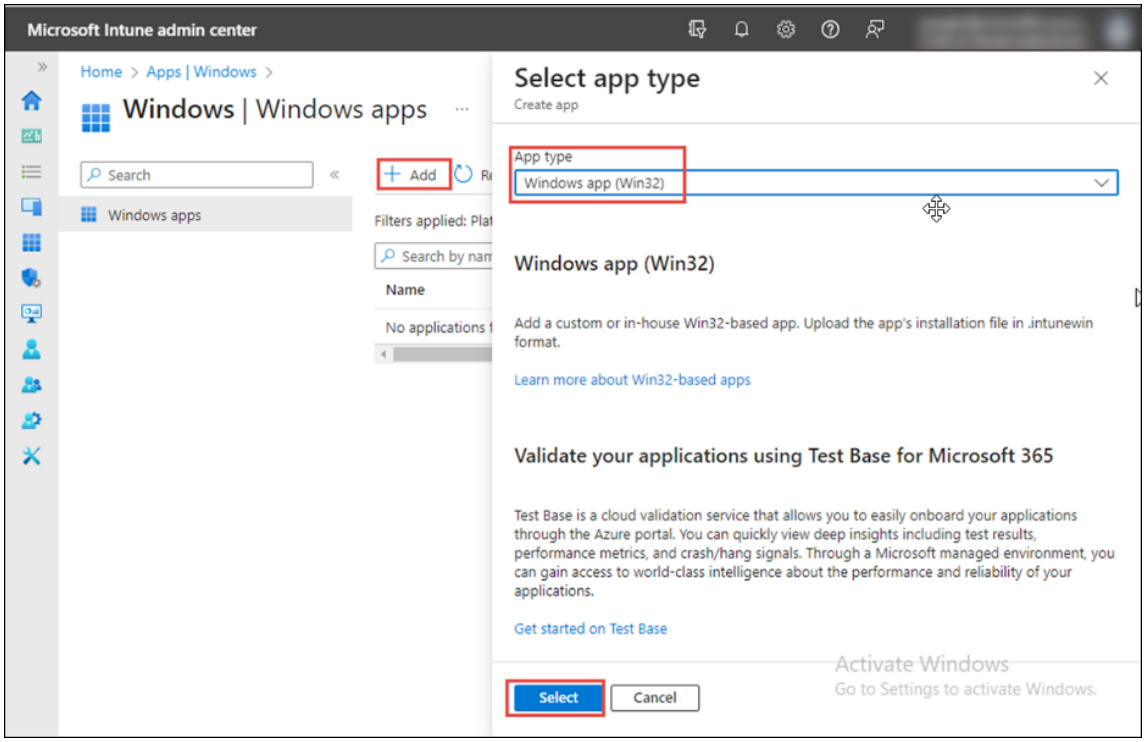
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For detailed information, see Microsoft 365 developer program.

Step 3: Add and assign an app

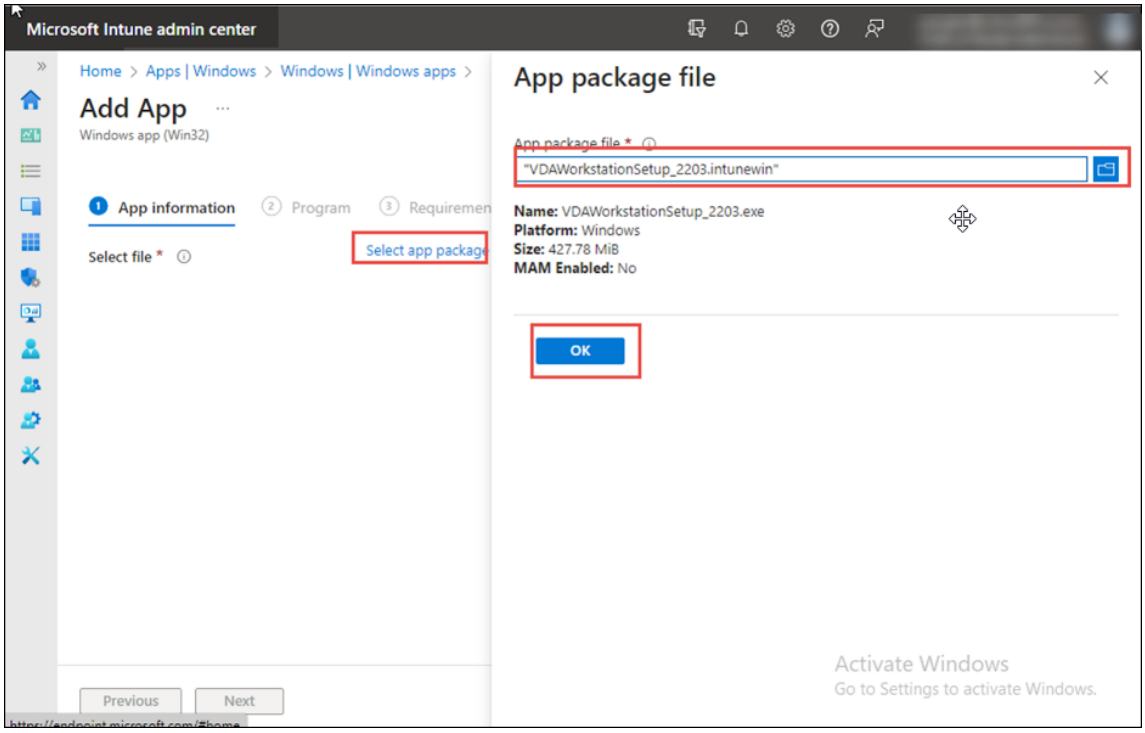
1. Sign in to Microsoft Intune admin center.
2. Select **Apps > All apps > Add** or go to **Apps > Windows > Windows Apps**.



3. On the **Select app type** pane, select **Other app types > Windows app (Win32)** and click **Select**.

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

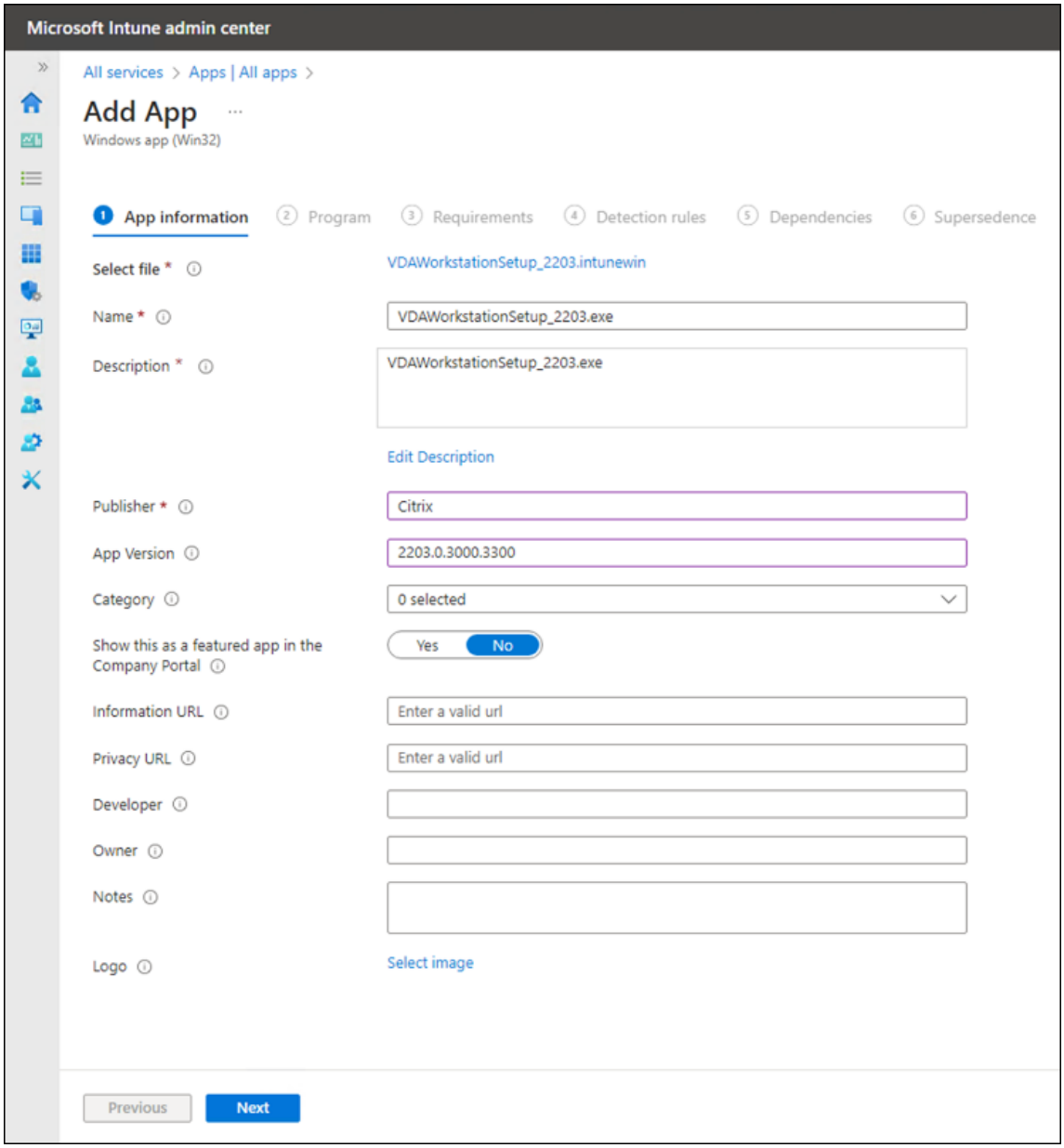
4. On the **Add app** pane, click **Select app package file**. Click **browse**.
5. Select the prepared file with the extension `.intunewin`. The prepared file is created during the Prepare installation for the Citrix VDA step. A page containing detailed information about the app is displayed.



> **Note:**
>
> - If you are using a server-core machine, you must use the VDA workstation core.
> - If you are using a Windows 10 desktop OS, you must use the VDA workstation.
> - If you are using a server OS (For example, Windows 2022), you must use the VDA server setup.
> - In this example, we are using the 2203 version but this is applicable for all versions.

6. Click **OK** on the **App package file** pane.
7. In the following screen, under the **App Information** tab, enter the **Name** of the App, and enter the **Description** of the Windows App. Enter the **Publisher** name as `Citrix`, and you can specify the additional app information here. Click **Next**.

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



8. On the next screen, enter the following values:

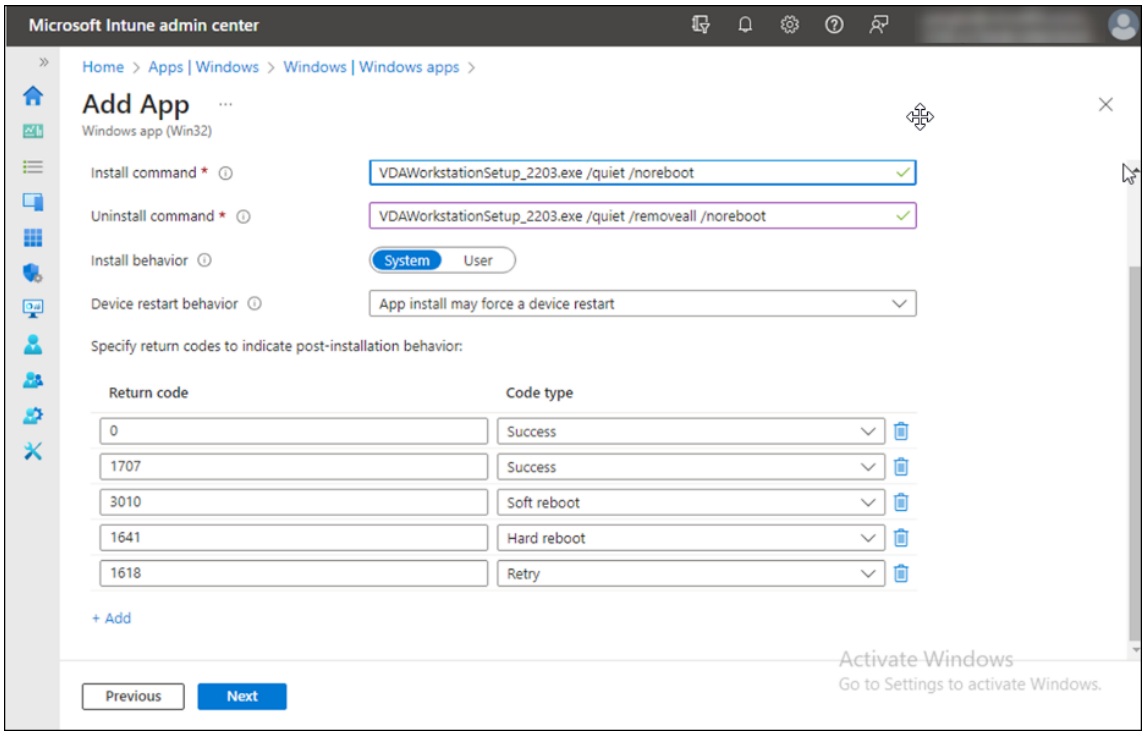
   - **Install command**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **Uninstall command**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **Install behavior**:
     - **System**: Select this option to install the app on all the devices in the group.
     - **User**: Select this option to install the app only on a specific user device in the group.

9. Click **Next**.

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

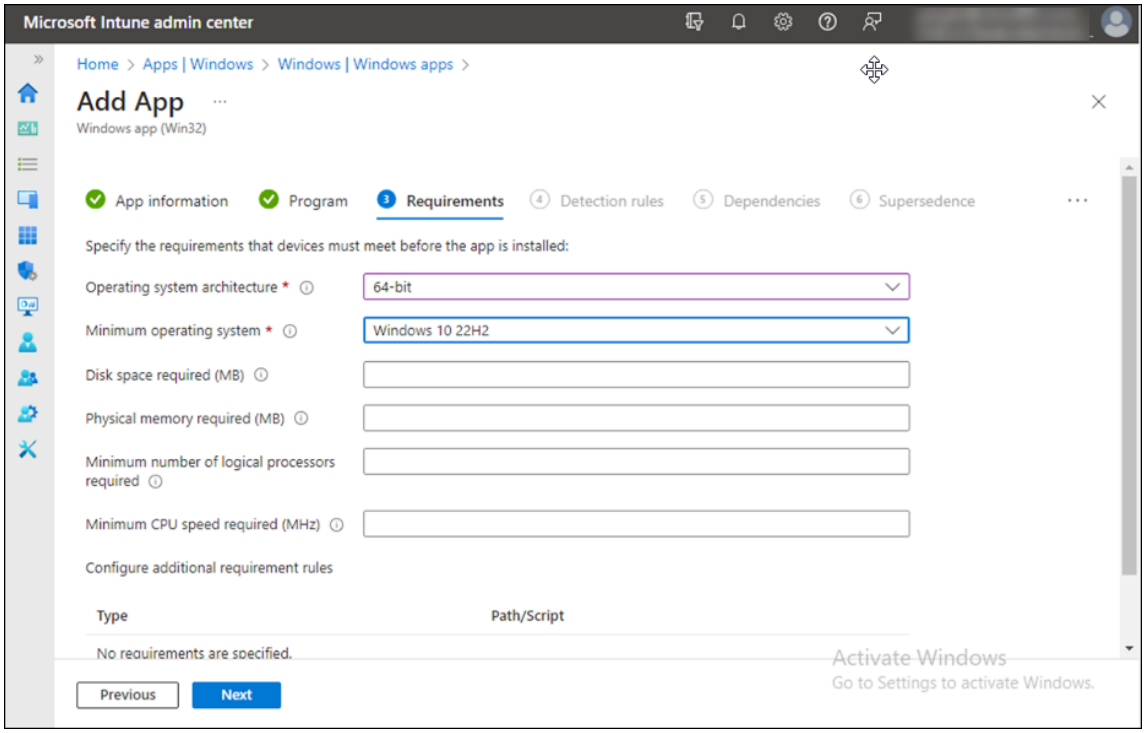
Note:

- This example uses the 2203 version, but you can use it with any version.
- Adding `/noreboot` to a command doesn't mean there won't be any reboots during installation or deployment, but only enforces mandatory reboots.
  For more information on scripts, see Command-line options for installing a VDA.
- For **Device restart behavior**, select **Intune will force a mandatory device restart**.
- In the **Return code** text box, enter `0`, `3` and `8` for post-installation success.
  For information on other return codes, see Citrix installation return codes.

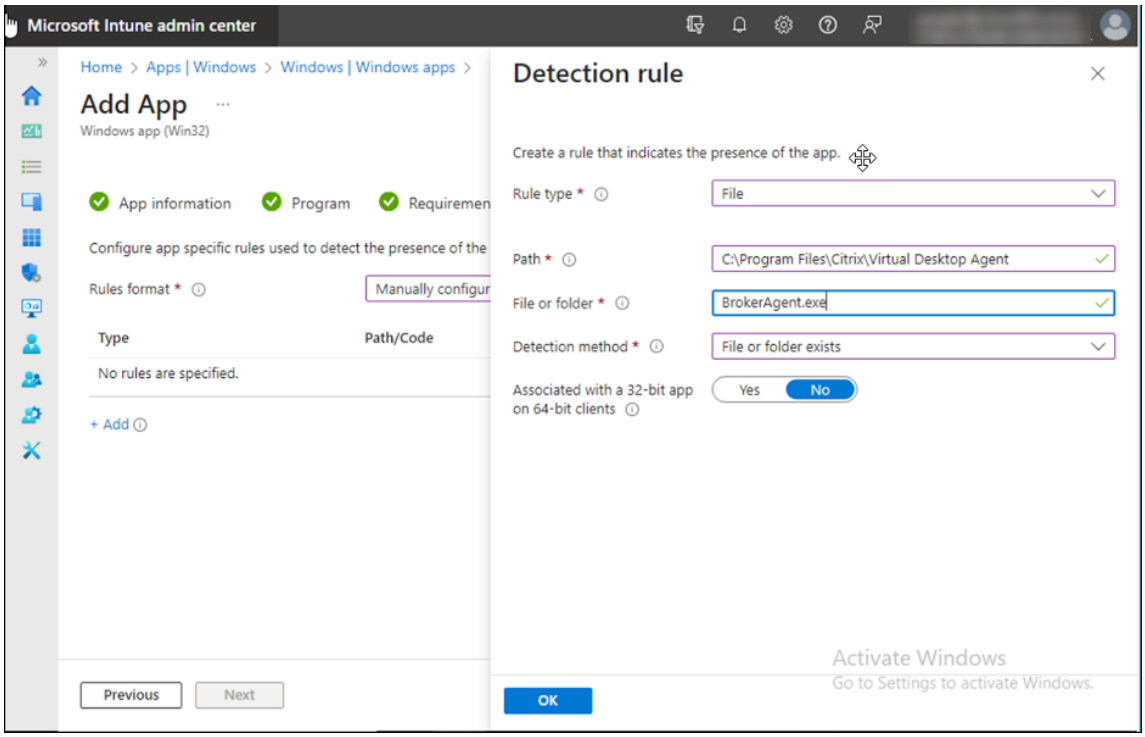


10. In the following screen, under the **Requirements** tab, enter the required values. Click **Next**.

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



11. In the following screen, under the **Detection rule** tab, add **Detection rule** to add the Broker agent. Click **OK**.

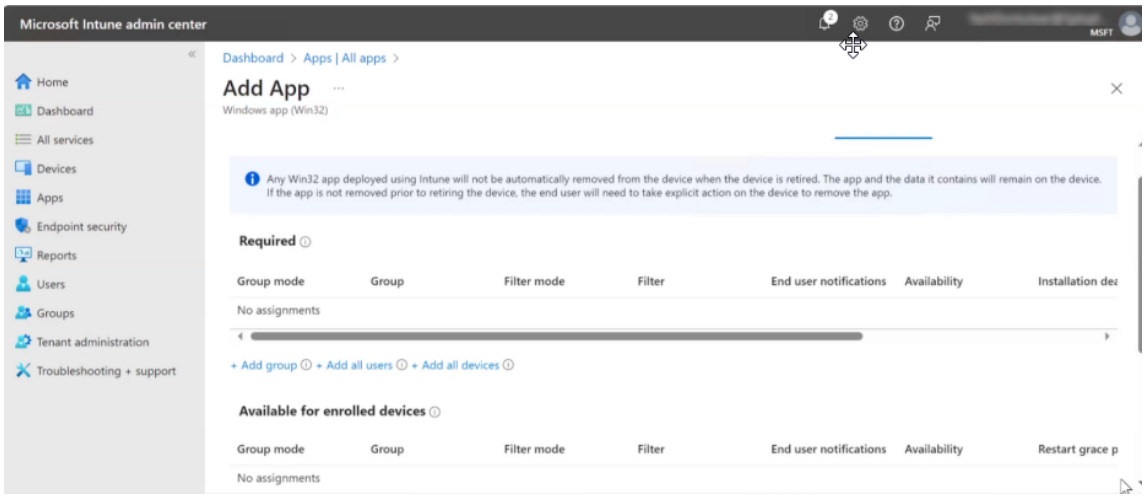


12. In the **Assignments** tab, you can add the devices in the following:

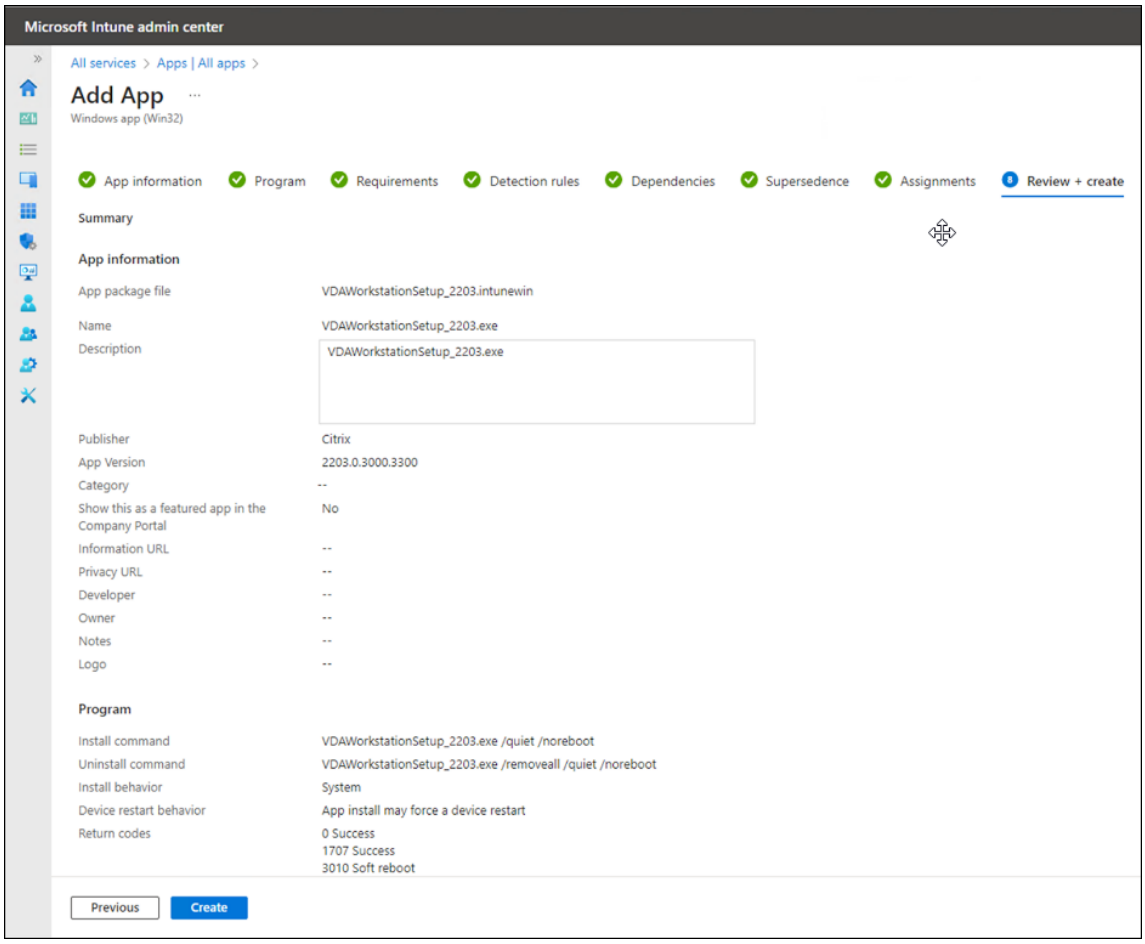
    - **Required**: The devices for which updates occur automatically.

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

- **Available for enrolled devices**: The devices for which updates occur manually.

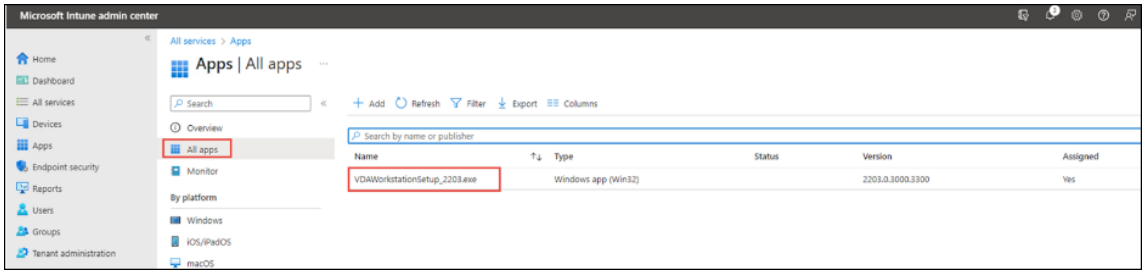


13. Review the details and click **Create**.



The app is assigned successfully.

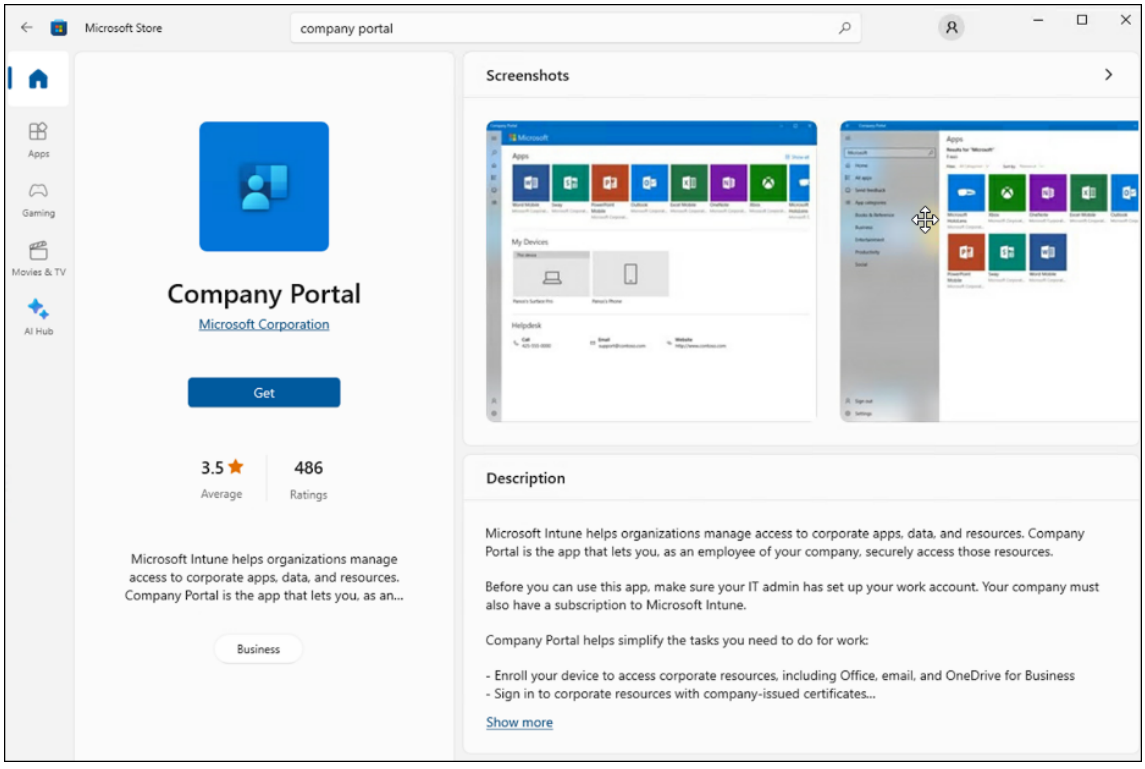
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For detailed information, see Add and assign an app.

Step 4: Install the app on the enrolled device

1. Sign in to your enrolled Windows 10 Desktop device.
   The device must be enrolled with Microsoft Intune. Also, you must sign in to the device using an account contained in the group you assigned to the app. For more information, see the Microsoft documentation.
2. From the **Start** menu, open **Microsoft Store**.
3. Browse for the **Company Portal** app and install it.



4. Run the **Company Portal** app.
5. Click the app that you added using Microsoft Intune.
   If you did not successfully assign any apps to the Intune user, the following message is displayed:

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

```
Your IT administrator did not make any apps available to you.
```

6. Click **Install**.

Create a site

November 18, 2025

> **Note:**
>
> - During site creation, after you add a license to enable Hybrid Rights License, public cloud hosts (such as Microsoft Azure, Google Cloud Platform, and Amazon Web Services) do not appear in the connection type list until the site creation completes.
> - Do not change the product edition or licensing model manually during or after enabling License Activation Service.

A site is the name you give to a Citrix Virtual Apps and Desktops™ deployment. It comprises the Delivery Controllers and other core components, Virtual Delivery Agents (VDAs), connections to hosts, machine catalogs, and delivery groups. You create the site after you install the core components and before creating the first machine catalog and delivery group.

If your Controller is installed on Server Core, use PowerShell cmdlets in the Citrix Virtual Apps and Desktops SDK to create a site.

When you create a site, you are automatically enrolled in the Citrix Customer Experience Improvement Program (CEIP). CEIP collects anonymous statistics and usage information, and then sends it to Citrix. The first data package is sent to Citrix approximately seven days after you create the site. You can change your enrollment at any time after site creation. Select **Settings** in the Web Studio left pane, and then locate the **Citrix Customer Experience Improvement Program** setting. For details, see http://more.citrix.com/XD-CEIP.

The user who creates a site becomes a full administrator. For more information, see Delegated administration.

Review this article before you create the site, so you know what to expect.

Step 1. Open the site creation wizard - Citrix Site Manager

Use the tool, Citrix Site Manager, to set up your Citrix Virtual Apps and Desktops deployment (also known as a site). The tool is installed automatically when you install a Delivery Controller.

To run this tool, open your desktop Start menu on a Delivery Controller, and select **Citrix > Citrix Site Manager**. See Install Web Studio.

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

Step 2. Site name

On the **Introduction** page, type a name for the site.

Step 3. Databases

> **Note:**
>
> Starting with version 2411, you can use Azure SQL Managed Instance for databases.

The **Databases** page contains selections for setting up the site, monitoring, and configuration logging databases. For details about database setup choices and requirements, see Databases.

> **Note:**
>
> If an SQL Server Always On Listener is configured for TLS encryption, you might be prompted to enter credentials with database creation permissions. Attempts to create the database still fail even if you enter valid administrator credentials. Verify that the SQL Server certificate includes the listener DNS name in the Subject Alternative Names (SAN). For more information, see https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates.

If you choose to install SQL Server Express for use as the site database (the default), a restart occurs after that software is installed. That restart does not occur if you choose not to install the SQL Server Express software for use as the site database.

If you are not using the default SQL Server Express, ensure that the SQL Server software is installed on the machines before creating a site. System requirements lists the supported versions.

If you want to add more Delivery Controllers to the site, and have already installed the Controller software on other servers, you can add those Controllers from this page. If you also plan to generate scripts that set up the databases, add the Controllers before generating the scripts.

Step 4. Licensing

On the **Licensing** page, specify the License Server address and then indicate which license to use (install).

> **Note:**
>
> - Ensure the License Server is running a minimum of version 11.17.2 build 53100 or later. Failure to meet this prerequisite blocks the Citrix Virtual Apps and Desktops site upgrades and site creation.
> - The License Activation Service (LAS) is a cloud-based licensing solution that provides an

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

> alternative to the traditional Citrix legacy licensing. For more information, see:
>
> - Citrix Virtual Apps and Desktops document: License Activation Service
> - Licensing document: License Activation Service
>
> - Do not change the product edition or licensing model manually during or after enabling License Activation Service.

- Specify the License Server address in the form `name:[port]`. The *name* must be an FQDN, NetBIOS, or IP address. FQDN is recommended. If you omit the port number, the default is 27000. Click **Connect**. You cannot proceed to the next page until a successful connection is made to the License Server.
- When a connection is made, **Use an existing license** is selected by default. The display lists the compatible products that this product can be configured as, based on currently installed licenses.
  - If the License Server is configured to use License Activation Service (LAS), the Metainstaller displays the entitlements. The entitlements are provided along with their corresponding license expiration dates. If you want to configure this product as one of the listed products using one of those licenses, select that entry.
  - If you already allocated and downloaded a license (using the Citrix Manage Licenses Tool) to use with this product, but haven't installed the license yet:
    - Click **Browse for license file**.
    - In the file explorer, locate and select the license you downloaded. The associated products now appear on the **Licensing** page of the site creation wizard. Select the entry you want to use.
  - If the product you want is not displayed, or if you have no allocated and downloaded licenses, you can allocate, download, and install a license. To do this, the License Server must have internet access. You must have a License Access Code for the product you want. Citrix emails that code to you.
    - Click **Allocate and download**.
    - In the **Allocate Licenses** dialog, enter the License Access Code sent by Citrix. Click **Allocate licenses**.
    - The products associated with the new license appear on the **Licensing** page of the site creation wizard. Select the entry you want to use.
- Alternatively, select **Use the free 30-day trial**, and install licenses later. For details, see the Licensing documentation.

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

Step 5. Summary

The **Summary** page lists the information you specified. Use the **Back** button if you want to change anything. When you're finished, click **Finish**.

More information

Host connection, network, and storage

If you are using VMs on a hypervisor or other service to deliver applications and desktops, you can optionally create the first connection to that host. You can also specify storage and network resources for that connection. After creating the site, you can modify this connection and resources, and create more connections. For details, see Connections and resources.

- For information specified on the **Connection** page, see Connections and resources.
  - If you are not using VMs on a hypervisor or other service (or if you use Web Studio to manage desktops on dedicated blade PCs), select the connection type **None**.
  - If you are configuring a Remote PC Access site and plan to use the Wake on LAN feature, select the **Microsoft System Center Virtual Machine Manager** or **Remote PC Wake on LAN** type. For more information, see Wake on LAN.

  In addition to the connection type, specify whether you will use Citrix tools (such as Machine Creation Services™) or other tools to create VMs.
- For information specified on the **Storage** and **Network** pages, see Host storage, Storage management, and Storage selection.
- If you have Hybrid Rights License and have added public cloud host connections (for example, AWS), those connections are listed here. To view those public cloud host connections, refresh Web Studio several minutes after adding them.

Remote PC Access

For information about Remote PC Access deployments, see Remote PC Access.

If you use the Wake on LAN feature, complete the configuration steps on the Microsoft System Center Configuration Manager before creating the site. For details, see Configuration Manager and Remote PC Access Wake on LAN.

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

Create and manage connections and resources

September 13, 2025

> **Important:**
>
> As of Citrix Virtual Apps and Desktops™ 7 2006, if your current deployment uses any of the following technologies, you can upgrade your deployment to the current release only after removing End of Life (EOL) items that use those technologies.
>
> - Personal vDisks (PvDs)
> - AppDisks™
> - Public cloud host types: Citrix CloudPlatform, Microsoft Azure Classic
>
> For details, see Remove PVD, AppDisks, and unsupported hosts.
>
> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

If you want to use public cloud host connections to your deployment, you need Hybrid Rights License to complete your fresh installation or upgrade to the current release.

When the installer detects one or more of the unsupported technologies or host connections without Hybrid Rights License, the upgrade pauses or stops, and an explanatory message appears. The installer logs contain details. For more information, see Upgrade a deployment.

Effect of Hybrid Rights License on host connection

There are three scenarios where the host connection to the public cloud hosts is affected based on Hybrid Rights License entitlement:

- To create a new host connection to the public cloud hosts, you must have Hybrid Rights License.
- If you have Hybrid Rights License but the license has expired, then the existing connections to public cloud hosts are marked as not entitled and enter into maintenance mode. When existing host connections are in maintenance mode, you cannot do the following:
  - Add or modify host connections
  - Create catalog and update image
  - Perform power actions

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

- When not entitled host connections change to entitled, existing hosting connections are re-enabled.

Introduction

You can optionally create your first connection to hosting resources when you create a Site. Later, you can change that connection and create other connections. Configuring a connection includes selecting the connection type from among the supported hypervisors and the storage and network that you select from the resources for that connection.

Read Only Administrators can view connection and resource details. You must be a Full Administrator to perform connection and resource management tasks. For details, see Delegated administration.

Where to find information about connection types

You can use the supported virtualization platforms to host and manage machines in your Citrix Virtual Apps or Citrix Virtual Desktops environment. The System requirements article lists the supported types.

For details, see the following information sources:

- **XenServer (formerly Citrix Hypervisor™):**
  - XenServer virtualization environments.
  - XenServer® documentation.
- **Nutanix Acropolis:**
  - Nutanix virtualization environments.
  - Nutanix documentation.
- **VMware:**
  - VMware virtualization environments.
  - VMware product documentation.
- **Microsoft Hyper-V:**
  - Microsoft System Center Virtual Machine Manager virtualization environments article.
  - Microsoft documentation.
- **Public Cloud host connections (AWS, Google Cloud, Microsoft Azure, Nutanix cloud and partner solutions, and VMware cloud and partner solutions):** For information related to public cloud hosts, see Set up resource type.

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

> **Note:**
>
> The information sources direct you to the Citrix DaaS™ documentation. If you are familiar with the public cloud hosts in the Citrix DaaS product, the on-premises version has several differences. In on-premises Virtual Apps and Desktops, the management interface is known as Web Studio. Updates are rolled out to the service approximately every four weeks. So, you might find that certain features available with the service are not available with the on-premises version.

Host storage

A storage product is supported when managed by a supported hypervisor. Citrix Support assists those storage product vendors in troubleshooting and resolving issues, and documents those issues in the knowledge center, as needed.

When provisioning machines, data is classified by type:

- Operating system (OS) data, which includes master images.
- Temporary data. This data includes all non-persistent data written to MCS-provisioned machines, Windows page files, user profile data, and any data that is synchronized with ShareFile. This data is discarded each time a machine restarts.

Providing separate storage for each data type can reduce load and improve performance on each storage device, making best use of the host's available resources. It also enables appropriate storage to be used for the different data types –persistence and resilience is more important for some data than others.

Storage can be shared (located centrally, separate from any host, used by all hosts) or local to a hypervisor. For example, central shared storage can be one or more Windows Server 2012 clustered storage volumes (with or without attached storage), or an appliance from a storage vendor. The central storage might also provide its own optimizations such as hypervisor storage control paths and direct access through partner plug-ins.

Storing temporary data locally avoids having to traverse the network to access shared storage. It also reduces load on the shared storage device. Shared storage can be more costly, so storing data locally can lower expenses. These benefits must be weighed against the availability of sufficient storage on the hypervisor servers.

When you create a connection, you choose one of two storage management methods: storage shared by hypervisors, or storage local to the hypervisor.

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.

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 method does not require persistence or as much resilience as the data in the shared storage, referred to as 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. 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: Microsoft System Center Virtual Machine Manager does not allow temporary data cache disks on local storage when using Clustered Storage Volumes (CSV).

Create a connection to store temporary data locally and then enable and configure nondefault values for each VM's cache disk size and memory size. The default values are tailored to the connection type, and are sufficient for most cases. For details, see Create machine catalogs.

The hypervisor can also provide optimization technologies through read caching of the disk images locally. For example, XenServer offers IntelliCache™, which reduces 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, master images and other OS data are transferred to the hypervisors in the Site. This process occurs for initial machine creation and future image updates. This process 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.

Create a connection and resources

You can optionally create the first connection when you create the Site. The Site creation wizard contains the connection-related pages described in the following sections.

If you are creating a connection after you create the Site, start with step 1.

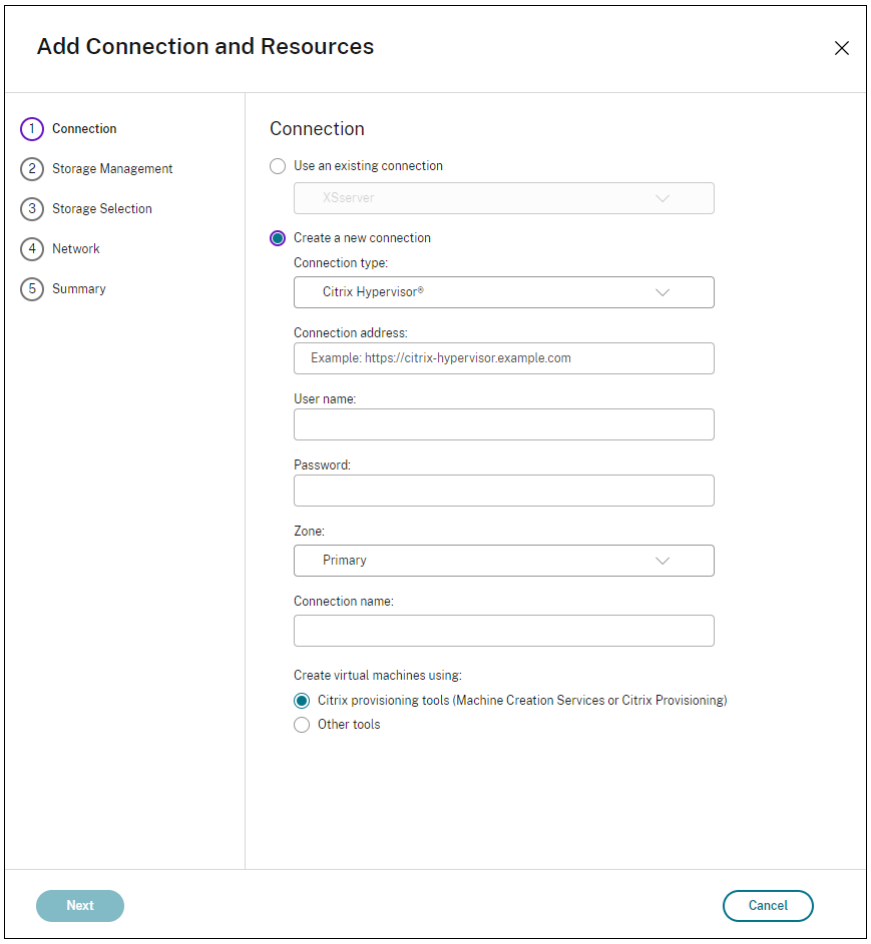
> **Important:**
>
> The host resources (storage and network) must be available before you create a connection.

1. Sign in to Web Studio.
2. Select **Hosting** in the left pane.

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

3. Select **Add Connections and Resources** in the action bar.
4. The wizard guides you through the following pages (specific page content depends on the selected connection type). After completing each page, click **Next** until you reach the **Summary** page.

Connection



On the **Connection** page:

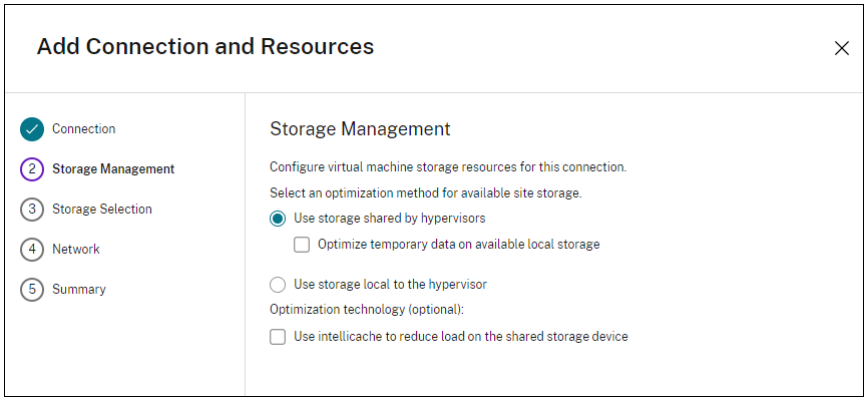
- To create a connection, select **Create a new Connection**. To create a connection based on the same host configuration as an existing connection, select **Use an existing Connection** and then choose the relevant connection.
- Select the hypervisor you are using in the **Connection type** field. Public cloud host connections are listed in the drop-down list only if you use Hybrid Rights License. Alternatively, you can use the PowerShell command `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true to get the following:
  - List of all Citrix supported hypervisor plugins, including third party plugins.

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

- Availability of hypervisor plugin. If the availability status is **false**, possible reason could be that the hypervisor plug-in is not installed correctly or you are not entitled with Hybrid Rights License.

- The connection address and credentials fields differ, depending on the selected connection type. Enter the requested information.
- Enter a connection name. This name appears in Web Studio.
- Choose the tool you use to create virtual machines: Web Studio tools (such as Machine Creation Services™ or Citrix Provisioning) or other tools.

Storage management



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.

- If you choose storage shared by hypervisors, indicate if you want to keep temporary data on available local storage. (You can specify nondefault temporary storage sizes in the machine catalogs that use this connection.) **Exception:** When using Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager does not allow temporary data cache disks on local storage. Configuring that storage management setup in Web Studio fails.

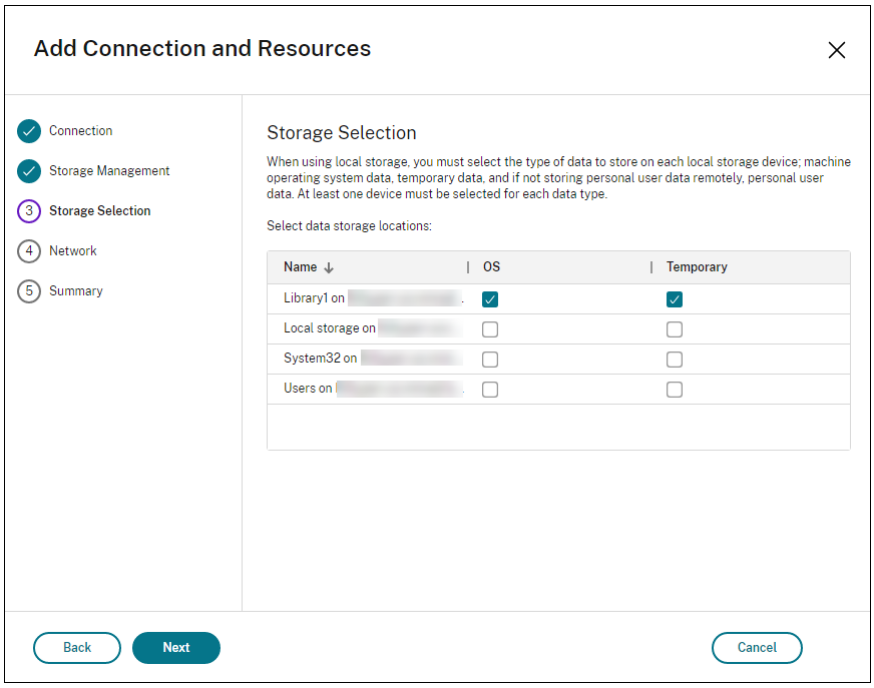
If you use shared storage in a XenServer pool, indicate if you want to use IntelliCache to reduce the load on the shared storage device. See Use IntelliCache for XenServer connections.

> **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**

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

> **data on available local storage**.

Storage selection

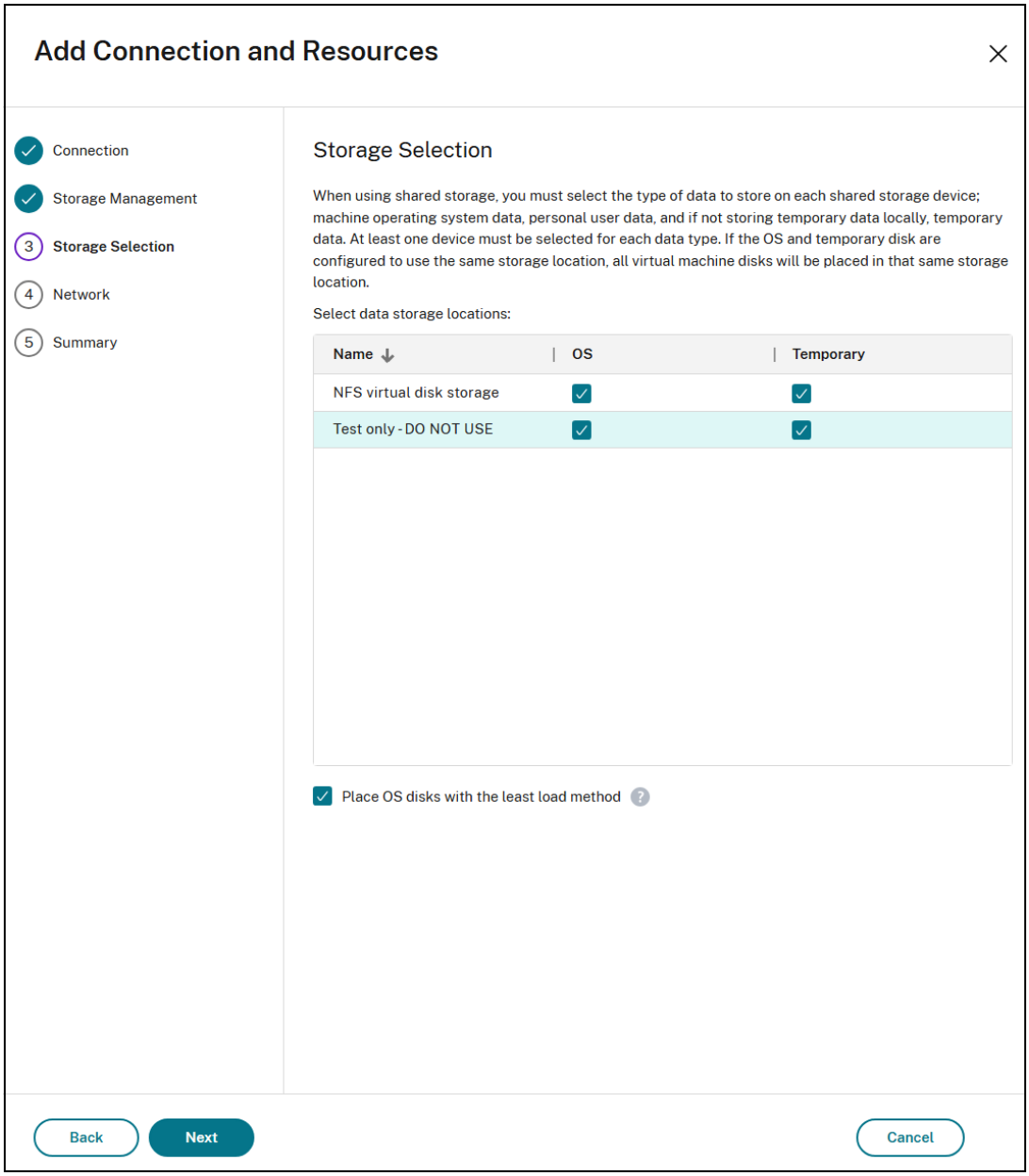


For more information about storage selection, see Host storage.

Select at least one host storage device for each available data type. The storage management method you selected on the previous page affects which data types are available for selection on this page. Select at least one storage device for each supported data type before you can proceed to the next page in the wizard.

> **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 **Detail**s panel displays changes to the storage allocation method. You can adjust it using the **Edit storage** option on the **OS Storage** page. Alternatively, you can use PowerShell to achieve the same goal. See Flexible storage location option for VMs.

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 preceding graphic, "1 storage device selected"). When you hover over that entry, the selected device names appear.

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

1. Click **Select** to change the storage devices to use.
2. In the **Select Storage** dialog box, select or clear the storage device check boxes, and then click **OK**.

Network

On the **Network** page, enter a name for the resources. This name appears in Web Studio to identify the storage and network combination associated with the connection.

Select one or more networks that the VMs use.

Summary

On the **Summary** page, review your selections. When you're done, click **Finish**.

Remember: Storing temporary data locally allows you to configure nondefault values for temporary data storage when you create the Machine Catalog containing machines using this connection. See Create Machine Catalogs.

Edit connection settings

Do not use this procedure to rename a connection or to create a connection. Those connections are different operations. 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.

You cannot change the **GPU** settings for a connection, because Machine Catalogs accessing this resource must use an appropriate GPU-specific master image. Create a connection.

1. Sign in to Web Studio.
2. Select **Hosting** in the left pane.
3. Select the connection and then select **Edit Connection** in the action bar.
4. Follow the guidance for the settings available when you edit a connection.
5. 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.

Connection Properties page:

- To change the connection address and credentials, 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.

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

> **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.

Advanced page:

- For a Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN connection type, which is used with Remote PC Access, enter **ConfMgr Wake Proxy**, magic packets, and packet transmission information.
- The throttling threshold settings enable you to specify a maximum number of power actions allowed on a connection. These settings can help when power 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 and must not be changed.
- The **Simultaneous actions (all types)** setting specifies 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 the **Connection options** field only under the guidance of a Citrix Support representative or explicit documentation instructions.

Shared Tenants page:

Add tenants and subscriptions that share the Azure Compute Gallery with the subscription of this connection. As a result, when creating or updating catalogs, you can select shared images from those tenants and subscriptions.

- Enter the **Application ID** and **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.
- Specify shared tenants and subscriptions. You can add up to eight shared tenants. For each tenant, you can add up to eight subscriptions.
- Click **Save** and **Apply** when you're done.

Enter information in the **Connection options** field only under the guidance of a Citrix Support representative.

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

Edit networks

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 to exit.

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. Sign in to Web Studio.
2. Select **Hosting** in the left pane.
3. 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 maintenance mode on or off for individual machines. Also, you can turn maintenance mode on or off for machines in Machine Catalogs or Delivery Groups.

Delete a connection

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 is referenced by that catalog. If this connection is referenced by a catalog, you have the option to delete the catalog. Before you delete a catalog, make sure it is not used by other connections.

1. Sign in to Web Studio.
2. Select **Hosting** in the left pane.
3. Select the connection and then select **Delete Connection** in the action bar.

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

4. If this connection has machines stored on it, you are asked whether the machines should be deleted. If they are to be deleted, specify what should be done with the associated Active Directory computer accounts.

Rename or test a connection

1. Sign in to Web Studio.
2. Select **Hosting** in the left pane.
3. Select the connection and then select **Rename Connection** or **Test Connection** in the action bar.

View machine details on a connection

1. Sign in to Web Studio.
2. Select **Hosting** in the left pane.
3. 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 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, click **Unfold**, and then select from the lists of properties and operators.

Manage machines on a connection

1. Sign in to Web Studio.
2. Select **Hosting** in the left pane.
3. Select a connection and then select **View Machines** in the **Action** pane.
4. Select one of the following in the action bar. Some actions are not available, depending on the machine state and the connection host type.

Action	Description
Start	Starts the machine if it is powered off or suspended.
Suspend	Pauses the machine without shutting it down, and refreshes the list of machines.
Shut down	Requests the operating system to shut down.

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

Action	Description
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 above.)
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 is powered off before the updates are complete.

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

Edit storage

You can display the status of servers that are used to store operating system and temporary data for VMs that use a connection. You can also specify which servers to use for storage of each data type.

1. Sign in to Web Studio.
2. Select **Hosting** in the left pane.
3. Select the connection and then select **Edit Storage** in the action bar.
4. In the left pane, select the data type: operating system, or temporary.
5. Select or clear the check boxes for one or more storage devices for the selected data type.
6. Click **OK**.

Each storage device in the list includes its name and storage status. Valid storage status values are:

- **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 in this storage.
- **Not in use:** The storage is not being used for creating machines.

If you clear the check box 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 it is possible for that location to become full even after it stops being used for creating machines.

Delete, rename, or test resources

1. Sign in to Web Studio.
2. Select **Hosting** in the left pane.
3. Select the resource and then select the appropriate entry in the action bar: **Delete Resources**, **Rename Resources**, or **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 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.

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

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")
```

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 Citrix Virtual Apps and Desktops site.

Follow the steps on Web Studio:

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

1. From **Manage**, 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 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.
- **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.

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.

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

> - A customer-managed resource tagged with all Citrix tags is detected as an orphaned resource. However, if you add another tag CitrixDetectIgnore with value as true to that resource, then the resource is ignored while detecting orphaned resources.

Limitations

- Only a built-in full admin or cloud admin role admin user can run the PowerShell command and get the list of orphaned resources.
- 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 in case of possible heavy workload.

To display the list of orphaned resources:

1. Open a **PowerShell** window.
2. 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>
```

To display the list of orphaned resources from an subscription id:

1. Open a **PowerShell** window.
2. 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>
```

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

> **Note:**
>
> Check the resources carefully before deleting.

Where to go next

For information on connection to specific host types, see:

- Connection to AWS
- Connection to XenServer
- 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

If you're in the initial deployment process, create a machine catalog.

Connection to AWS

April 7, 2026

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to AWS cloud environments.

> **Note:**
>
> Before creating a connection to AWS, you need to first finish setting up your AWS account as a resource location. See AWS cloud environments.

Create a connection

When you create a connection from Web Studio:

- 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.

© 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 Virtual Apps and Desktops™ management 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.

> **Note:**
>
> After you create a connection, attempts to update the API key and secret key might fail. To resolve the issue, check your proxy server or firewall restrictions and ensure that the following address is contactable: `https://*.amazonaws.com`.

Host connection default values

When you create host connections in AWS cloud environments, the following default values are displayed:

Option	Absolute	Percentage
Simultaneous actions (all types)	125	100
Maximum new actions per minute	125	

MCS supports 100 maximum concurrent provisioning operations by default.

Cross-account provisioning

There are use-cases where the Delivery Controllers would like to be placed in a primary 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 Delivery controllers 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 Delivery Controllers, and provisioned VMs in different regions and/or accounts be able to communicate amongst each other.

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

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

To allow Delivery Controllers 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 (link to the topic below).

Set up VPC peering

Let's assume that VPC A is in the primary account (Account A) and it has the Delivery Controllers 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, VPC B's CIDR Block.
    - If it is a different account but 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 primaryaccount (Delivery Controller™ 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 Delivery Controller 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 above.
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 name mentioned above "primary-account-citrix role"which has the ability to 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 Delivery Controllers in Account A.

Delivery Controller 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 Delivery Controller 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:

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

- `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>'

$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.

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.

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

Define IAM permissions

Use the information in this section to define IAM permissions for Citrix Virtual Apps and Desktops 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:

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**. Select **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 group of users. Users in the group are granted permissions to perform only those actions that are required for Citrix Virtual Apps and Desktops.

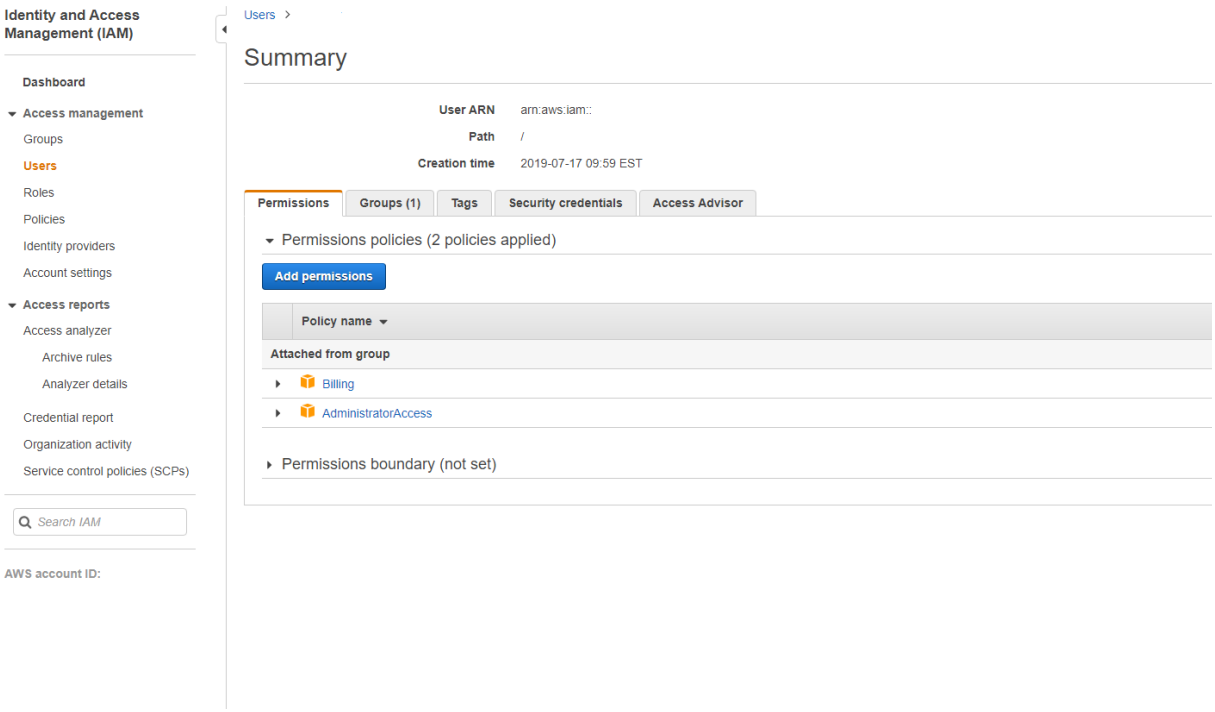
> **Important:**
>
> Use the policy text provided in the example earlier to list the actions that Citrix Virtual Apps and Desktops uses to perform actions within an AWS account without restricting those actions to specific resources. Citrix recommends that you use the example for testing purposes. For production environments, you might choose to add further restrictions on resources.

Set IAM permissions

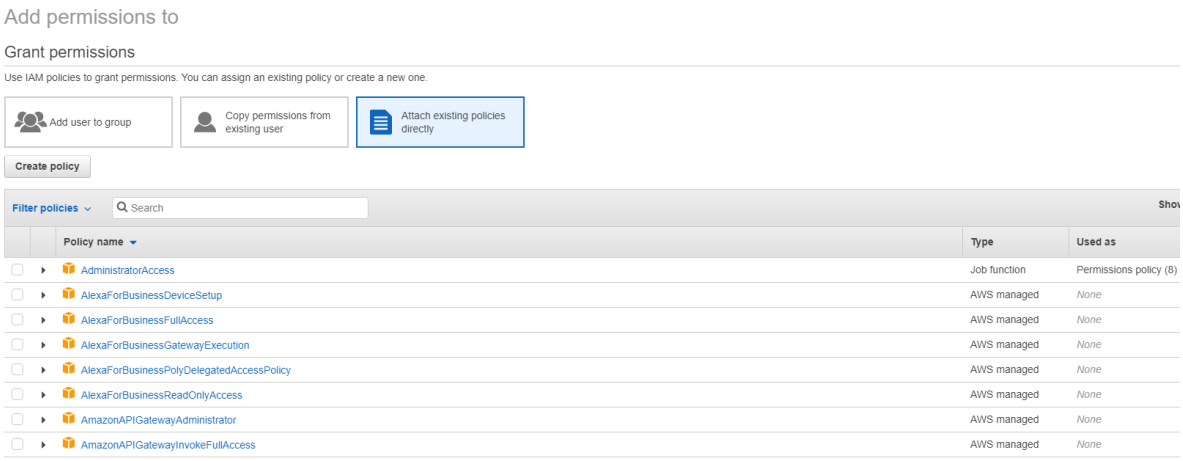
Set the permissions in the **IAM** section of the AWS Management Console:

1. In the **Summary** panel, select the **Permissions** tab.
2. Select **Add permissions.**

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

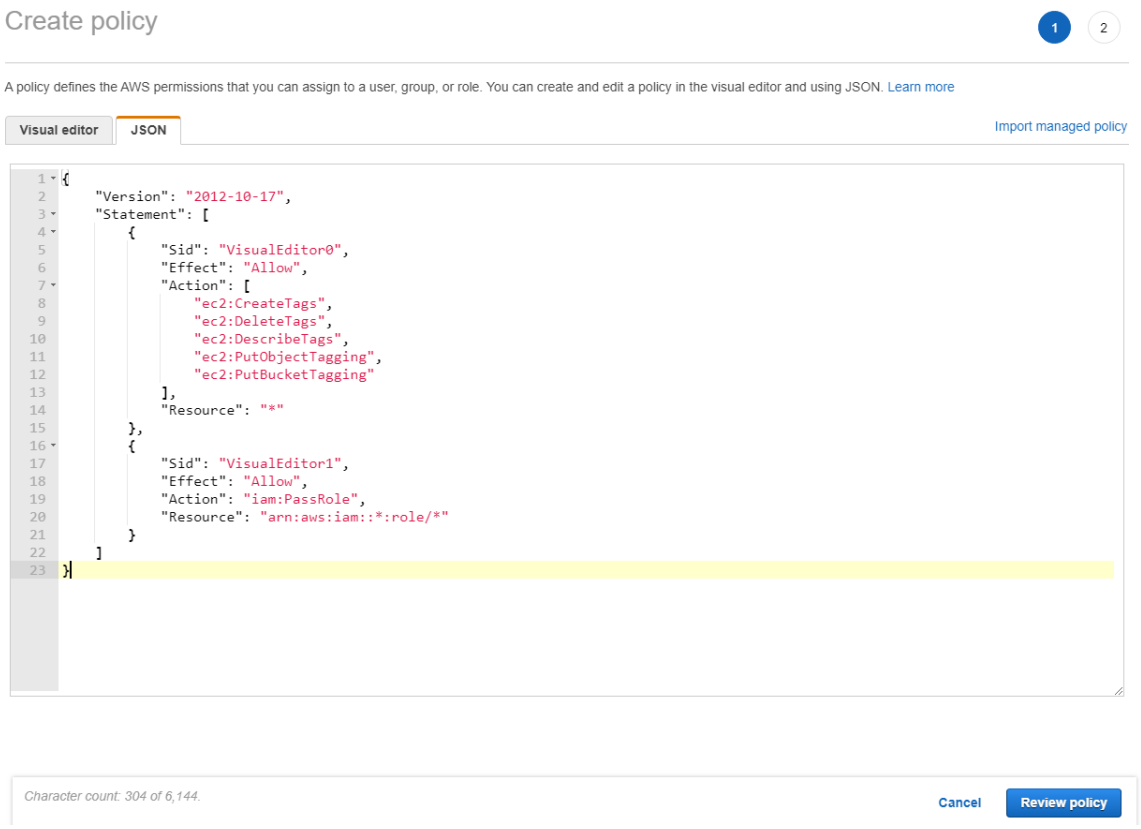


In the **Add Permissions to** screen, grant permissions:



Use the following as an example in the **JSON** tab:

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



> **Tip:**
>
> The noted JSON example might not include all the permissions for your environment. See How to Define Identity Access Management Permissions Running Citrix Virtual Apps and Desktops on AWS for more information.

Required AWS permissions

This section contains the complete list of AWS permissions.

> **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 from AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
```

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

```
6
7               "Action": [
8                   "ec2:DescribeAvailabilityZones",
9                   "ec2:DescribeSubnets",
10                  "ec2:DescribeVpcs",
11                  "ec2:DescribeRegions"
12              ],
13              "Effect": "Allow",
14              "Resource": "*"
15           }
16
17      ]
18   }
```

Power management of VMs

VMs are powered on or off.

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:DescribeInstances",
9                  "ec2:StartInstances",
10                 "ec2:StopInstances",
11                 "ec2:RebootInstances",
12                 "ec2:DescribeInstanceStatus"
13             ],
14             "Effect": "Allow",
15             "Resource": "*"
16          }
17
18     ]
19  }
```

Creating, updating, or deleting VMs

A machine catalog is created, updated, or deleted with VMs provisioned as AWS instances.

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
```

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

```
                "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: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: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": "*"
         }

    ]
}
```

> **Note:**
>
> The EC2 section related to security groups 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.

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`
- `ec2:DescribeLaunchTemplates`

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

> **Important:**
>
> - You can add a VM to existing machine catalogs without any volume worker operation such as volume worker AMI, and volume worker VM.
> - If you delete an existing catalog that used volume worker before, all artifacts including 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"
            ],
            "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",
```

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

```
                    "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": {

                    "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 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": [
```

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

```
        {

            "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 using **role_based_auth** security key and secret key.

> **Important:**
>
> To use **role_based_auth**, first configure the desired IAM role on all Delivery Controllers in our site. Using Web 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",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
```

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

```
                "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",
                "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": "*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
```

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

```
            "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/*"
        }

    ]
}
```

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.

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-`

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

`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 Set IAM permissions.

Where to go next

- If you're in the initial deployment process, see Create machine catalogs
- For AWS specific information, see Create an AWS catalog

More information

- Connections and resources
- Create machine catalogs

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

Connection to Azure Local

August 22, 2025

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Azure Local environments.

Create a host connection

You can create a host connection using:

- Studio
- PowerShell

Use Studio

1. In Studio UI, navigate to the **Hosting** node and create a fresh new hosting connection using **Microsoft® Azure™ Arc** as the connection type.
2. Enter connection details following the guidance in the wizard. If you use an existing SPN, make sure that the SPN has been granted the contributor role of the subscription.
3. Browse the cluster through **Region > Resource Group**.
4. Complete the settings on the following pages.

Use PowerShell

Header of the script Make sure that you provide the correct parameter values defined in the header of the script.

```
$azureSubscription = "" # Azure Subscription ID
$azureTenantId = "" # Azure AD Tenant ID
$appClientId = "" # Client ID of an Azure AD application which is grant
    with sufficient permissions
$appClientSecret = "" # Client secret of above client ID
$appClientSecretExpirationDateTimestamp = "" # Client secret expiration
    date in epoch timestamp format
$region = "" # Azure region of your Azure Local cluster
$resourceGroupName = "" # Azure resource group of your Azure Local
   cluster
$zoneUid = "" # Zone UID of your resource location
$hostingConnectionName = "" # Name of the created hosting connection
```

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

Create a host connection

```
asnp Citrix.Host.Admin.V2
[SecureString]$appClientSecretSecureString = $appClientSecret |
    ConvertTo-SecureString -AsPlainText -Force
$conn = New-Item -ConnectionType "Custom" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"><Property xsi:type=`"StringProperty`" Name=`"
    SubscriptionId`" Value=`"$azureSubscription`" /><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=`"TenantId`"
    Value=`"$azureTenantId`" /></CustomProperties>" -HypervisorAddress @
    ("https://management.azure.com/") -Path @("XDHyp:\Connections\
    $hostingConnectionName") -Persist -PluginId "AzureArcFactory" -Scope
     @() -SecurePassword $appClientSecretSecureString -UserName
    $appClientId -ZoneUid $zoneUid
New-BrokerHypervisorConnection -HypHypervisorConnectionUid $conn.
    HypervisorConnectionUid
Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid $conn.
    HypervisorConnectionUid -Name
    Citrix_Orchestration_Hypervisor_Secret_Allow_Edit -Value true
Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid $conn.
    HypervisorConnectionUid -Name
    Citrix_Orchestration_Hypervisor_Secret_Expiration_Date -Value
    $appClientSecretExpirationDateTimestamp
```

Where to go next

- For creating an Azure Local machine catalog, see Create an Azure Local machine catalog.

More information

- Connections and resources
- Create machine catalogs

Connection to XenServer®

February 20, 2026

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to XenServer virtualization environments.

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

> **Note:**
>
> Before creating a connection to XenServer, you need to first finish setting up your XenServer account as a resource location. See XenServer virtualization environments.

Create a connection to XenServer

When you create a connection to XenServer (formerly Citrix Hypervisor™), you must provide the credentials for a VM Power Admin or higher-level user.

Citrix recommends using HTTPS to secure communications with XenServer. To use HTTPS, you must replace the default SSL certificate installed on XenServer.

You can configure high availability if it is enabled on the XenServer server. For Citrix Virtual Apps and Desktops versions 2507 LTSR and later, if you are using HTTPS and want to configure high-availability servers, you can install a wildcard certificate for all servers in a pool. However, for versions earlier than 2507 LTSR, an individual certificate for each server is required.

You can select a GPU type and group, or pass through, if the XenServer supports vGPU. The display indicates if the selection has dedicated GPU resources.

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.)

You can use Citrix Provisioning (formerly Provisioning Services) and Machine Creation Services™ (MCS) to provision:

- legacy BIOS for supported Desktop or Server OS VMs.
- UEFI for supported Desktop or Server OS VMs, including Secure Boot.

> **Note:**
>
> Pool operator permissions or higher are required when configuring MCS.

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 number 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.

- Shared storage must be NFS when using IntelliCache.

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

- Citrix recommends that you use a high performance local storage device to ensure the fastest possible data transfer.

To use IntelliCache, you must enable it in both this product and XenServer.

- When installing XenServer, select **Enable thin provisioning (Optimized storage for Virtual Desktops)**. Citrix does not support mixed pools of servers that have IntelliCache enabled and servers that do not. For more information, see the XenServer documentation.
- In Citrix Virtual Apps and Desktops™, IntelliCache is disabled by default. You can change the setting only when creating a XenServer connection; you cannot disable IntelliCache later. When you add a XenServer connection:
  - Select **Shared** as the storage type.
  - Select the **Use IntelliCache** check box.

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

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

Task	Minimum role required
Power on or off the VMs	VM Operator

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

- Connections and resources
- Create machine catalogs

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

Connection to Google cloud environments

March 5, 2026

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 environments.

Add a connection

Follow the guidance in Create a connection and resources. The following description guides you through setting up a hosting connection:

1. From **Manage > Configuration**, 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**.
   - **Connection type**. Select **Google Cloud** from the menu.
   - **Connection name**. Type a name for the connection.
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.

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

After creating 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.

Service endpoint URLs

You must have access to the following URLs:

- https://oauth2.googleapis.com
- https://cloudresourcemanager.googleapis.com
- https://compute.googleapis.com
- https://storage.googleapis.com
- https://cloudbuild.googleapis.com

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 project has limited permissions in this project, specifically, only permissions to use the VPC.

Create a secure environment for GCP managed traffic

You can allow private Google access to your Google Cloud projects. This implementation enhances security to handle sensitive data. To achieve this, you can do one of the following:

- Include the following ingress rules of VPC service controls for Cloud Build Service Account. If you do this step, then do not follow the steps below for creating a secure environment for GCP managed traffic.

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
```

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

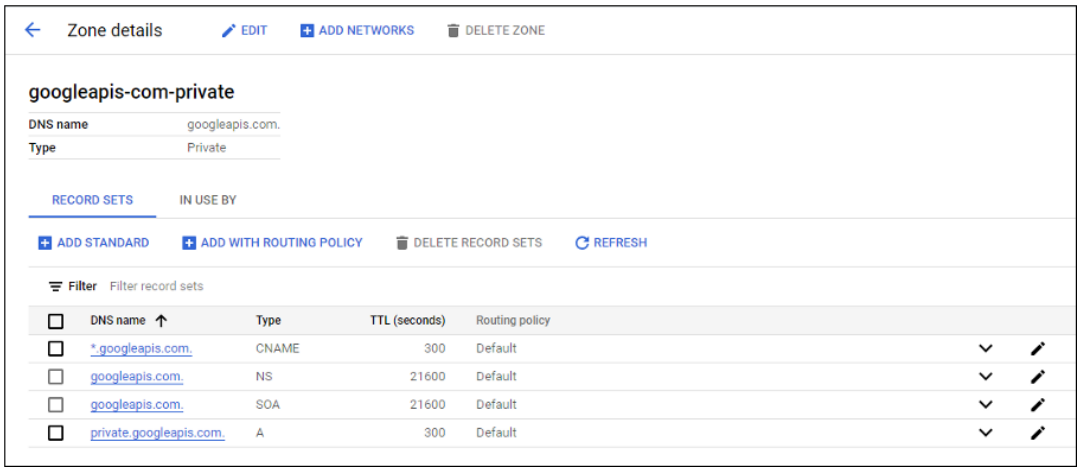
```
All projects
Services =
Service name: All services
```

- If you are using a private worker pool, add `UsePrivateWorkerPool` in `CustomProperties`. For information on the private worker pool, see Private pools overview.

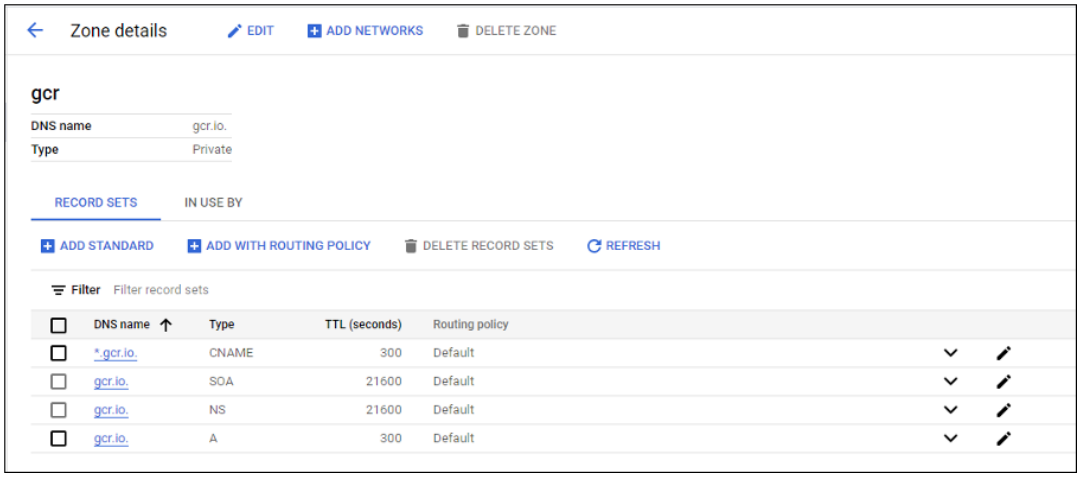
Requirements to create a secure environment for GCP managed traffic

The requirements to create a secure environment for GCP managed traffic are:

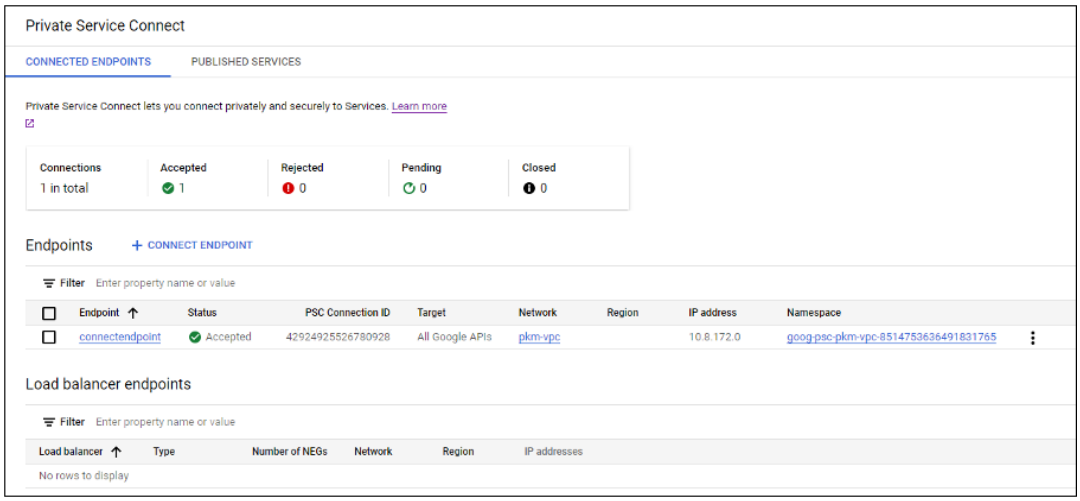
- Ensure that the hosting connection is in maintenance mode when updating the custom properties.
- To use private worker pools, the following changes are required:
  - For Citrix Cloud™ Service Account, add the following IAM roles:
    - Cloud Build Service Account
    - Compute Instance Admin
    - 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.



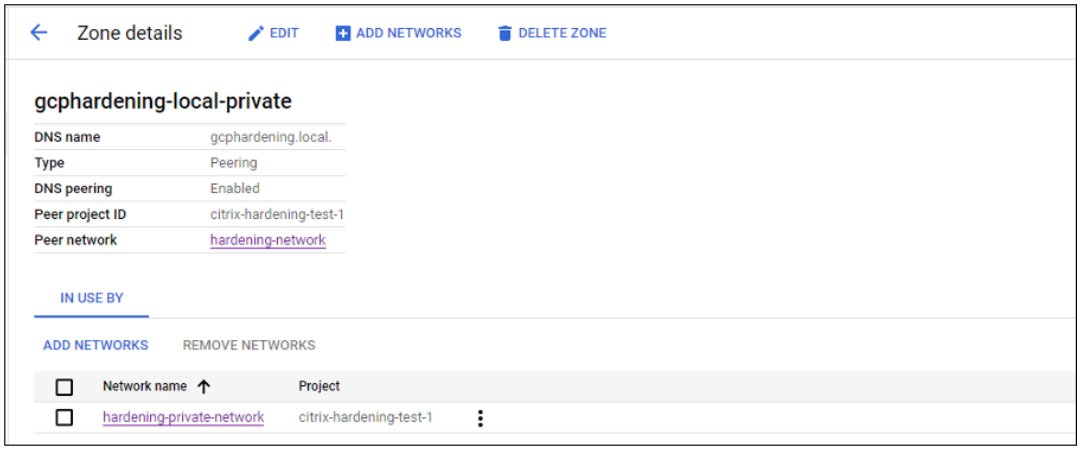
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 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.



- 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:

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

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
```

Enable the private worker pool

To enable the private worker pool, 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 property setting `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool"Value="True"/>`. 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="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:

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

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR
    CONNECTION NAME HERE>') -SecurePassword $securePassword -
    UserName $gcpServiceAccount -CustomProperties $customProperty
```

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.

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

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

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\myglobalkey.cryptokey
     ```

   - To get regional encryption keys within the same project:

     ```
     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: myanother-project):

     ```
     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: myanother-project):

     ```
     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:

```
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

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

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
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
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
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
```

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

```
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
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
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.

© 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.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
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
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 re-

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

quired 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.
- (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

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

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:

```
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
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
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
```

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

```
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
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
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
iam.serviceAccounts.actAs
compute.resourcePolicies.use
cloudkms.cryptoKeyVersions.useToDecrypt
cloudkms.cryptoKeyVersions.useToEncrypt
```

© 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 Google Cloud Platform (GCP) specific information, see Create a Google Cloud Platform catalog

More information

- Connections and resources
- Create machine catalogs

Connection to HPE Moonshot

September 13, 2025

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:

- Web Studio
- PowerShell commands

Create a connection using Web 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:

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

- Citrix Virtual Apps and Desktops™ 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.
- Citrix Virtual Apps and Desktops 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. Citrix Virtual Apps and Desktops 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.

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.

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

- 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.

> **Note:**
>
> A mismatch in the certificate thumbprint between the Citrix Database and the Moonshot server triggers a warning in Web Studio. However, this warning doesn't appear in MMC-based Studio.

Manage connections

This section details how you can manage connections:

- Fix certificate issues using the Web Studio
- Update thumbprint value using PowerShell command

Fix certificate issues

Citrix Virtual Apps and Desktops 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.
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:

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

1. Get the connection details of a connection. For example:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. Update the thumbprint value. For example:

```
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 AWS specific information, see Create an HPE Moonshot machine catalog

More information

- Connections and resources
- Create machine catalogs

Connection to Microsoft Azure

December 9, 2025

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

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.

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

> **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 cloud 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 Web Studio
- Create a connection using a previously created service principal

This section shows you how to complete these tasks:

- Create a service principal and connection using Web Studio
- Create a service principal using PowerShell
- Get the application secret in Azure
- Create a connection using an existing service principal

Considerations

- Citrix® recommends using Service Principal with contributor role. However, see 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.
- 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 add them back explicitly. However, exercise this option carefully, because it has unintended effects for other resources that the account can access.

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

- There is a known issue where certain accounts are detected as directory guests when they are actually members. Configurations like this typically occurs with older established directory accounts. Workaround: add an account to the directory, which takes the proper membership value.
- 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 Web Studio

> **Important:**
>
> This feature is not yet available for Azure China subscriptions.

With Web 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 Azure AD.

Before you start, make sure that you've met these prerequisites:

- You have a user account in your subscription's Azure Active Directory 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. These permissions can be revoked after you create host connection. For more information about roles, see Azure AD 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, enter your Azure subscription ID and a name for the connection. After you enter the subscription ID, the **Create new** button is enabled.

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

> **Note:**
>
> The connection name can contain 1–64 characters, and cannot contain only blank spaces nor the characters `\/;:#.*?=<>|[]{ } "'()'`.

4. Select **Create new** and then enter the Azure Active Directory account user name and password.
5. Select **Sign in**.
6. Select **Accept** to give Citrix Virtual Apps and Desktops™ the listed permissions. Citrix Virtual Apps and Desktops creates a service principal that allows it to manage Azure resources on behalf of the specified user.
7. After you select **Accept**, you return to the **Connection** page in the wizard.

   > **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.

8. On the **Connection Details** page, select **Next**.

   > **Note:**
   >
   > You cannot proceed to the next page until you successfully authenticate to Azure and consent to giving the required permissions.

9. Configure resources for the connection. Resources comprise the region and the network.
   - 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 nor 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.
10. 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.

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

In the **Add Connection and Resources** list, select the connection to view the details. The **Details** tab shows the Application ID.

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 Azure AD.
- **ApplicationName:** Name for the application to be created in Azure AD.

Detailed steps are as follows:

Connect to your Azure Resource Manager subscription.

```
1 `Connect-AzAccount`
```

1. Select the Azure Resource Manager subscription where you want to create the service principal.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

2. Create the application in your AD tenant.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. Create a service principal.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. Assign a role to the service principal.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. 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:

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

1. Get the **Application ID** from the Web Studio or using PowerShell.
2. Sign in to the Azure portal.
3. In Azure, select **Azure Active Directory**.
4. From **App registrations** in Azure AD, 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 Web Studio.

Make sure you have these items ready:

- SubscriptionId
- ActiveDirectoryID (tenant ID)
- 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, 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 nor 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**.

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

- **Active Directory ID** (tenant ID). Enter the Directory (tenant) ID of the application that you registered with Azure AD.
- **Application ID**. Enter the Application (client) ID of the application that you registered with Azure AD.
- **Application secret**. Create a secret key (client secret). The registered application uses the key to authenticate to Azure AD. 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 see a warning icon on the specific host connection in the Hosting node starting 14 days before the secret key expires. However, if the secret key expires, you receive errors.

  > **Note:**
  >
  > For security purposes, the expiration period cannot be more than two years from now.

- **Authentication URL**. This field is automatically populated and is not editable.
- **Management URL**. This field is automatically populated and is not editable.
- **Storage suffix**. This field is automatically populated and is not 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`.

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

- 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 }`.

5. After selecting **Save**, you return to the **Connection Details** page. Select **Next** to continue to the next page.
6. Configure resources for the connection. Resources comprise the region and the network.
   - 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 nor 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
- Enable image sharing in Azure
- Add shared tenants to a connection using Web Studio
- Implement image sharing using PowerShell
- 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 issues related to power operations.

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

> **Tip:**
>
> For more information, see Improving Azure performance with Machine Creation Services.

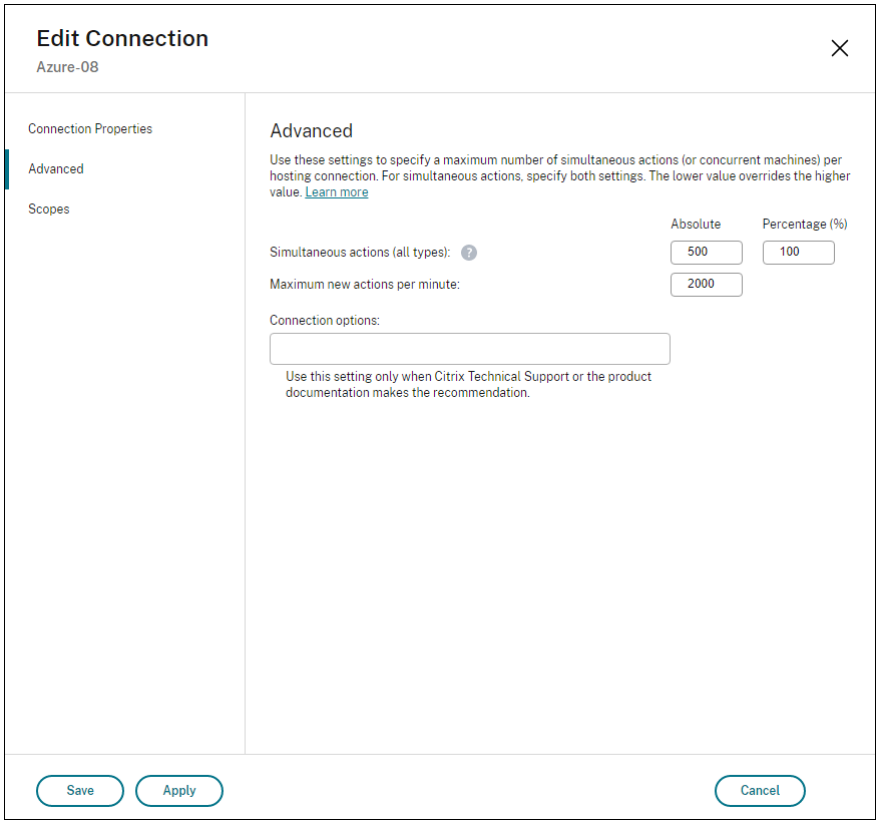
To help mitigate these issues, you can remove MCS internal throttling to use more of the available request quota from Azure.

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 Web Studio to configure Azure operations for a given Azure connection:

1. In Web Studio, select **Hosting** in the left pane.
2. Select the connection.
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`.

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 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 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.

For information on selecting an image from a different subscription using PowerShell commands, Select an image from a different subscription.

Share images across tenants To share images across tenants with Azure Compute Gallery, create an application registration.

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 which has the gallery image. For more information, see Authenticate requests across tenants.

To create a catalog using an image from a different tenant using PowerShell commands:

1. Update hosting connection custom properties with shared tenant IDs.
2. Select an image from a different tenant.

Add shared tenants to a connection using Web Studio

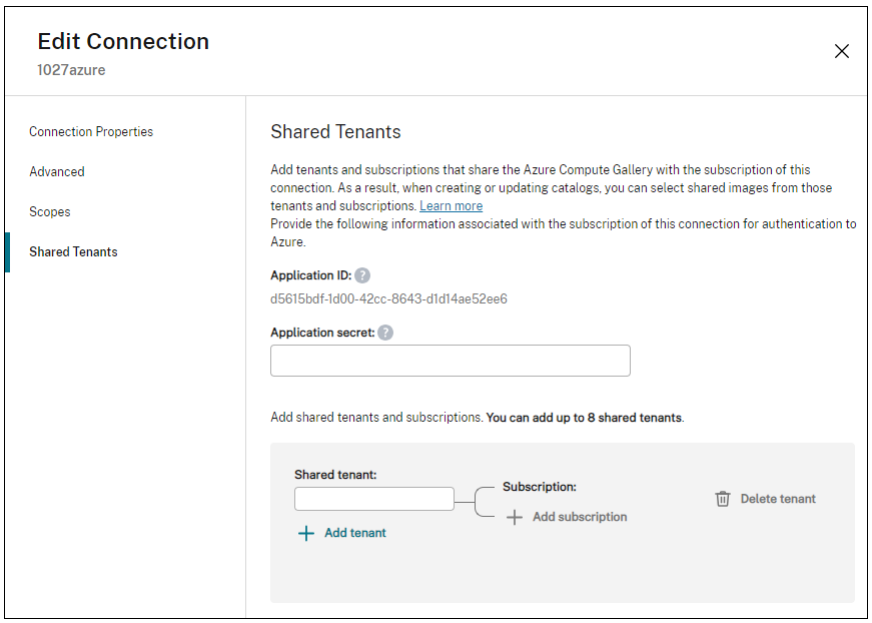
When creating or updating machine catalogs in Web Studio, you can select shared images from different Azure tenant and subscriptions (shared through the Azure Compute Gallery). The feature requires that you provide shared tenant and subscription information for associated host connections.

> **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:

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

1. In Web Studio, select **Hosting** in the left pane.
2. Select the connection and then select **Edit Connection** in the action bar.



3. In **Shared Tenants**, do the following:
   - Provide the application ID and application secret associated with the subscription of the connection. Citrix Virtual Apps and Desktops uses this information to authenticate to Azure AD.
   - Add tenants and subscriptions that share the Azure Compute Gallery with the subscription of the connection. You can add up to 8 shared tenants and 8 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

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.

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

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.resourcegroup\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.resourcegroup\sigtestdef.imagedefinition"
```

7. Create and update an MCS catalog using the following elements:

   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

   For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

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 `Shared Tenants` is:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
```

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

```
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-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" -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.

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

```
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.resourcegroup\efg.gallery
```

6. Select one image definition, and then list all image versions of that image definition.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
```

7. Create and update an MCS catalog using the following elements:

   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

   For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Manage the application secret and secret expiration date

Be sure to change the application secret for a connection before the secret expires. You see a warning icon on the specific host connection in the **Hosting** node starting 14 days before the secret key expires. However, if the secret key expires, you receive errors.

Create an application secret in Azure You can create an application secret for a connection through the Azure portal.

1. Select **Azure Active Directory**.
2. From **App registrations** in Azure AD, select your application.
3. Go to **Certificates & secrets**.
4. Click **Client secrets > New client secret**.
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.

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

7. In the Web 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 the Web Studio to add or modify the expiration date for the application secret in use.

> **Note:**
>
> You see a warning icon on the specific host connection in the **Hosting** node starting 14 days before the secret key expires. However, if the secret key expires, you receive errors.

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.

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
- `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:

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

```
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>"
```

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.

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

> **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"] }
 '
```

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"] }
'
```

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

- 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 '
    ew0KICAiJGlkIjogIjEiLA0KICAiTWF4Um93cyI6IDUsDQogICJSb3dzVG9Ta2lwIjogMjUs
    =='
```

- 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 '{
```

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

```
2  "containedresourcetypes": ["vm", "templatespecversion"] }
3  '
```

- Filter for Image with tag Citrix internal tag and limit max records with `MaxRecords` and location.

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\
       ctx04con01unit01" -ResourceType resourceGroup -MaxRecords 5 -
       AdditionalDataFilter '{
2  "containedresourcetypes": ["manageddisk", "snapshot", "
       imageversion", "storageaccount"], "location": ["eastus", "
       westus"] }
3  '
```

- Retrieve all resource group without consideration on tags `CitrixResource`.

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\
       ctx04con01unit01" -ResourceType resourceGroup -MaxRecords 50 -
       AdditionalDataFilter '{
2  "containedresourcetypes": ["manageddisk", "snapshot", "
       imageversion", "storageaccount"] }
3  ' -Force $true
```

Connect to Azure Sovereign Airgap cloud environment

The Azure Sovereign Airgap cloud environment is suitable for top-secret workloads that must be on segregated network domains. You can connect to Azure Sovereign Airgap cloud environment using a custom property `DisableInstanceDiscovery` while creating a host connection.

```
1  <Property xsi:type="StringProperty" Name="DisableInstanceDiscovery"
       Value="true" />
```

See Create-HostingConnection.ps1 for more information on creating an Azure host connection.

Required Azure permissions

This section contains the minimum and general permissions required for Azure.

Minimum permissions

Minimum permissions give better security control. However, new features that require additional permissions fail because of using only minimum permissions.

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

Creating a host connection Add a new 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"
```

Power management of VMs Power on or off the machine instances.

```
"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 image is managed disk or snapshots are located 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",
"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",
```

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

```
"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",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/locations/usages/read",
"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

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 located 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 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, then the snapshots, or VHD is in a region different from the region of hosting connection:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
```

- If you use 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",
```

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

```
"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",
"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",
"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",
```

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

```
"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",
"Microsoft.Network/locations/usages/read",
```

General permission

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",
"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",
```

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

```
"Microsoft.Compute/virtualMachines/write",
"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",
"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",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

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

Validate host connection in Azure non-secret environment

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.

- 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.

   ```
   1 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:

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

To test a connection at the subscription level with higher level of authorization required:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\
    AzureCon -SecurePassword $password -UserName 922e65d5-38ae-4cf5
    -xxxx-xxxxxxxxx
```

Example:

To test a connection at the resource group level without 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.

Validate host connection in Azure secret environment

You can validate if a host connection has the required permissions in an Azure secret environment using a PowerShell command `Test-HypHypervisorConnection`.

However, to successfully get the validation result, create or update an existing host connection to have a custom property `AuthenticationObjectId`. This property stores the Object ID of the service principal tied to the hosting connection.

> **Note:**
>
> Get the Object ID of the Service Principal from the Azure portal. Do not use the ID of the Application.

Create or update a host connection to include AuthenticationObjectId

Use `New-Item` to create a host connection and add `AuthenticationObjectId` as a custom property. Example:

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

```
New-Item -ConnectionType 'Azure' -HypervisorAddress @('http://
    hypervisorhost1.example.com','http://hypervisorhost2.example.com')`
     -LoggingId $loggingId -Path @('XDHyp:\\Connections\\Example') -
        Persist -Scope @() `
     -Password 'Password' -UserName 'root' -CustomProperties <Property
        xsi:type="StringProperty" Name="AuthenticationObjectId" Value="
        Object ID of the service principal"/>
```

Use `Set-Item` to update an existing host connection to add `AuthenticationObjectId` as a custom property. The steps to do this are:

1. Open a PowerShell window using the Remote PowerShell SDK.
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="AuthenticationObjectId" Value="Object ID of the service principal"/>` to the `CustomProperties`.
4. In the PowerShell window, assign a variable to the modified custom properties.
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`.
7. Run `dir` to verify the updated `CustomProperties` settings.

   ```
   Set-Item -PSPath XDHyp:\Connections\$connName -CustomProperties <
       Property xsi:type="StringProperty" Name="AuthenticationObjectId
       " Value="Object ID of the service principal"/> -username $cred.
       username -Securepassword $cred.password
   ```

Validate the host connection for the permissions

To validate the host connections for the required roles and permissions, run the following commands:

- If you have roles and permissions assigned at the subscription level:

  ```
  Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<
      Your-HostingConnection>
  ```

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

- If you have roles and permissions assigned at the resource group level:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<
    Your-HostingConnection>  -CustomProperties $CustomProperties

$CustomProperties = '<CustomProperties xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance" xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation">'`
+ '<Property xsi:type="StringProperty" Name="ResourceGroups"
    Value="ExampleResourceGroup" />'`
+ '</CustomProperties>'
```

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

- Connections and resources
- Create machine catalogs

Connection to Microsoft System Center Virtual Machine Manager

May 5, 2025

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).

> **Note:**
>
> Before creating a connection to VMM, you need to first finish setting up your VMM account 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.

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

- Enter 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

- Connections and resources
- Create machine catalogs

Connection to Nutanix

August 14, 2026

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to Nutanix.

> **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

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

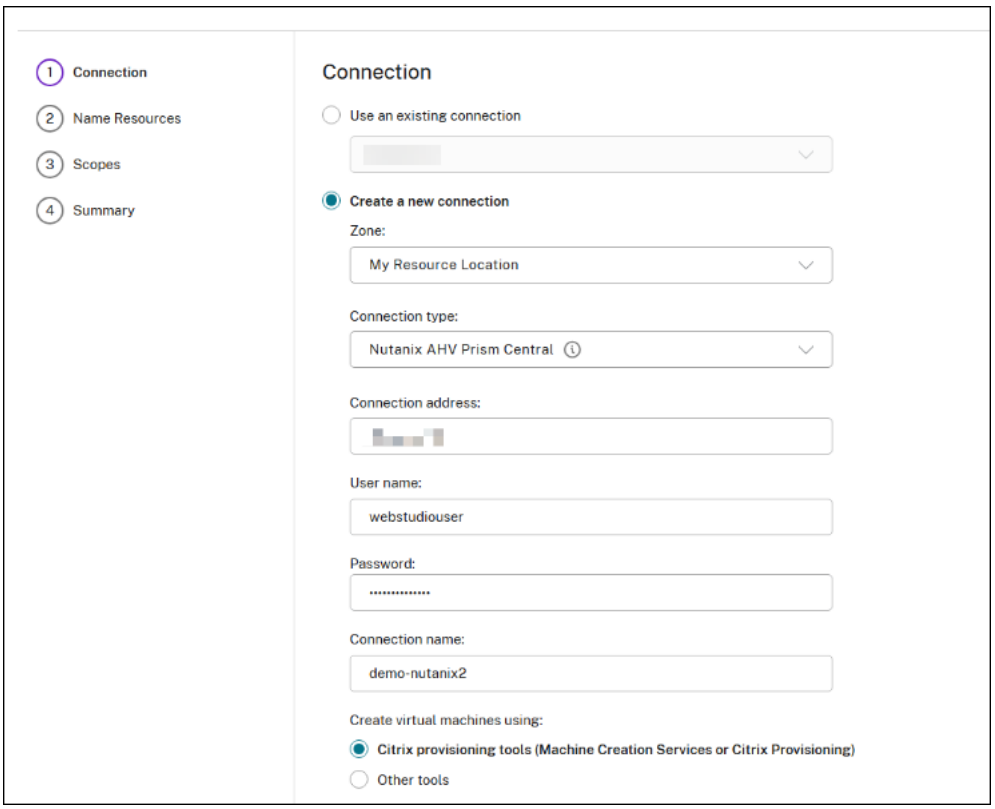
Limitation

- 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. 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.

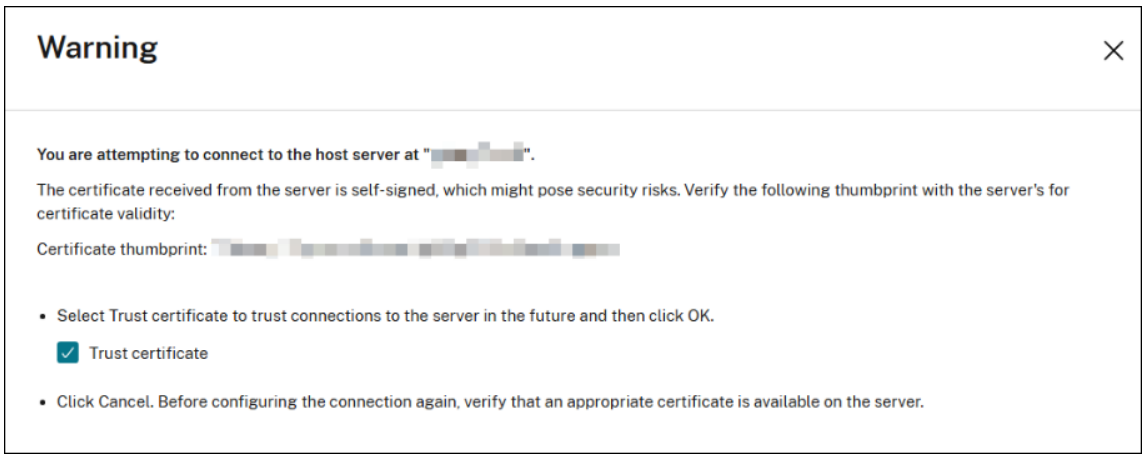


> **Note:**
>
> While creating the host connection, network or cluster selection is not required. A hosting unit name is only needed. Select the network and cluster while creating the machine catalog.

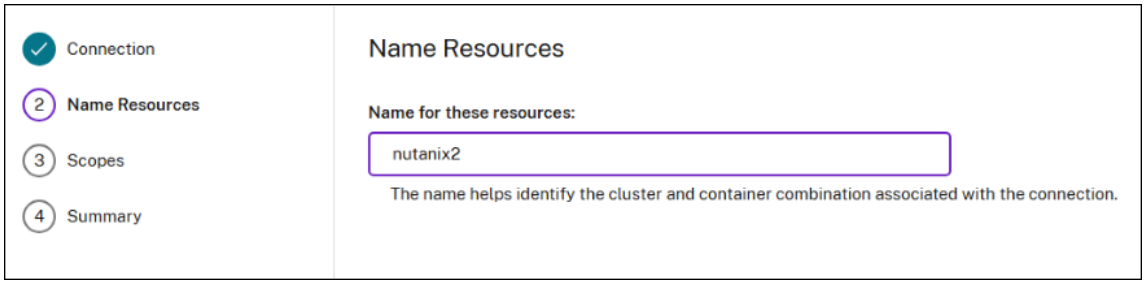
6. After you click **Next**, Citrix Virtual Apps and Desktops receives a private CA-signed certificate and you see a **Warning** page. For information, see Secure connections to the Nutanix Prism Central.

   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 Virtual Apps and Desktops 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 Virtual Apps and Desktops 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
- `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.

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

Manage host connections

You can manage an existing host connection using:

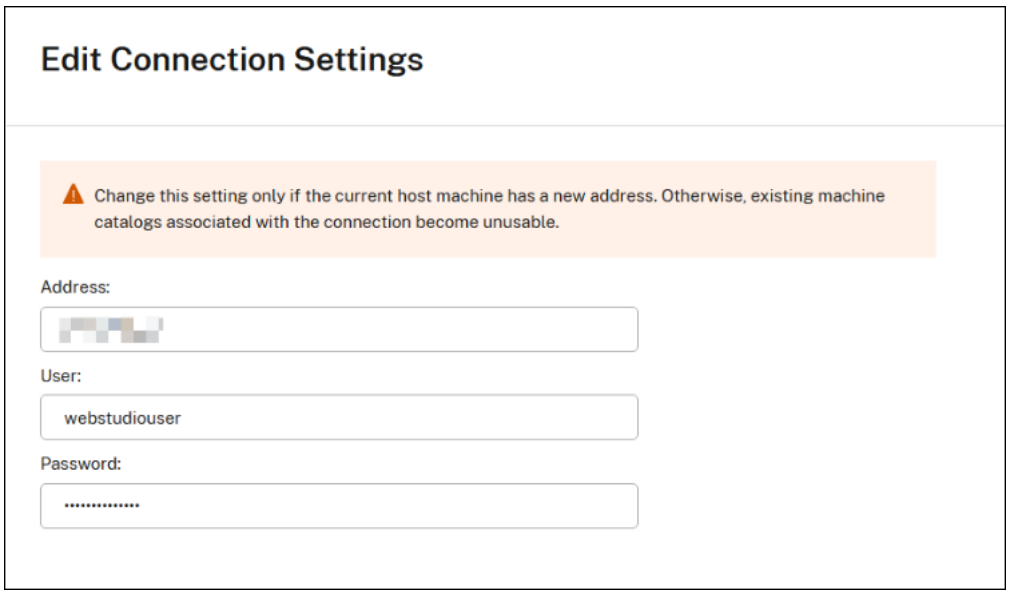
- Studio
- PowerShell

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**.
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**.

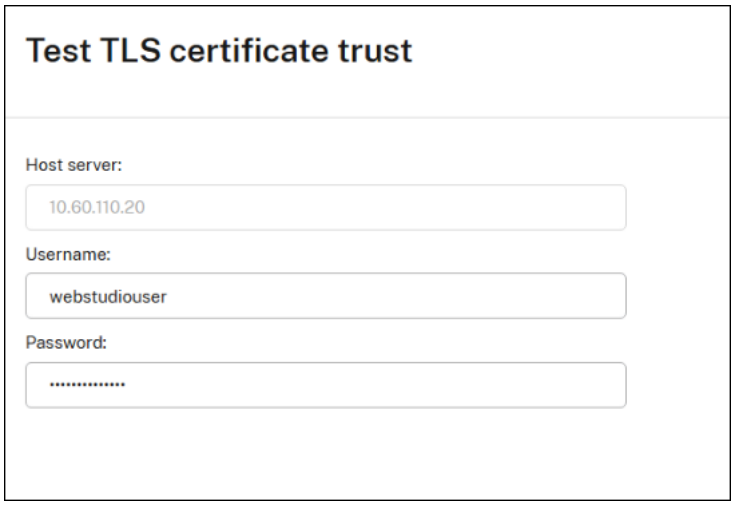


4. Select **Trust certificate** on the **Warning** page to trust the new certificate thumbprint.

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

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**.



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>")  -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.

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

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
- 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

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

- 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:

- 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

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

Storage Container:

- View Storage Container
- View Storage Container Datastore
- View Storage Container Stats

Storage Policy:

- View Storage Policy

Subnet:

- View Subnet
- View Subnet Vnic

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.

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

2. 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.

        > **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

November 12, 2025

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 Virtual Apps and Desktops 2507 CU1 and later 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 Virtual Apps and Desktops supports Nutanix Cloud Clusters (NC2) in the following cloud hypervisor for the Nutanix Prism Element plug-in.

- AWS

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

Connect to Nutanix Prism

After you create a Nutanix cluster, connect to Nutanix Prism.
To connect to Nutanix Prism:

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 Web Studio, select **Hosting** in the left pane.

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

2. Click **Add Connection and Resources**.
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

- Connections and resources
- Nutanix virtualization environments
- Nutanix cloud and partner solutions

Connection to Red Hat OpenShift

September 13, 2025

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:

- Web Studio
- PowerShell

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

Create a connection using Web Studio

1. In Web Studio, open **Hosting > Add Connection and Resources**.
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
$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:

- Web Studio
- PowerShell

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

Create hosting units using Web 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**.
   - 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.

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

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\
    $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
- Create machine catalogs

Connection to VMware

March 31, 2026

Create and manage connections and resources describes the wizards that create a connection. The following information covers details specific to VMware virtualization environments.

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

> **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.

Create a connection

In the connection creation wizard:

1. Select the VMware connection type.
2. Specify the address of the access point for the vCenter SDK.
3. Specify the credentials for a VMware user account you set up earlier that has permissions to create VMs. Specify the user name in the form domain/username.

VMware SSL thumbprint

The VMware SSL thumbprint feature eliminates the need to manually create a host connection to a VMware vSphere hypervisor. It is no longer required to manually create a trust relationship between the Delivery Controllers in the Site and the hypervisor's certificate before creating a connection.

The VMware SSL thumbprint feature stores the untrusted certificate's thumbprint on the Site database. This configuration ensures that the hypervisor can be continuously identified as trusted by Citrix Virtual Apps and Desktops™, even if not by the Controllers.

When creating a vSphere host connection in Studio, a dialog box allows you to view the certificate of the machine you are connecting to. You can then choose whether to trust it.

Required privileges

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 Virtual Apps and Desktops operations and the minimum required VMware privileges.

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

> **Note:**
>
> The permissions list display name, specifically the *User Interface*, is different for some vSphere versions. For example, in vSphere 6.7 the *User Interface* permission is **Change Memory** and **Change Settings**, rather than **Settings** and **Memory** as described in the required privileges noted on this page.

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
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network

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

SDK	User interface
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
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

Image update and rollback

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

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
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

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

SDK	User interface
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
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 (vSAN)

To view, create, or delete storage policies during catalog creations on a vSAN 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
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

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

> `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
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.

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

SDK	User interface
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
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.

Obtain and import a certificate

To protect vSphere communications, Citrix® recommends that you use HTTPS rather than HTTP.

HTTPS requires digital certificates. Use a digital certificate issued from a certificate authority that meets your organization's security policy.

If you are unable to use a digital certificate issued from a certificate authority, you can use the VMware-installed self-signed certificate. Only use this method if your organization's security policy permits it. Add the VMware vCenter certificate to each Delivery Controller.

1. Add the fully qualified domain name (FQDN) of the computer running vCenter Server to the hosts file on that server, 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 Delivery Controllers.
   b) On the Controller, navigate to the location of the exported certificate and open the rui.crt file.

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

Download the certificate using a web browser. If you are using Internet Explorer, 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) View the certificate and click the Details tab.
e) Select **Copy to file and export in .CER format**, providing a name when prompted to do so.
f) Save the exported certificate.
g) Navigate to the location of the exported certificate and open the .CER file.

Import directly from Internet Explorer running as an administrator.

- Open your web browser and make a secure web connection to the vCenter server (for example https://server1.domain1.com).
- Accept the security warnings.
- Click the address bar displaying the certificate error.
- View the certificate.

3. Import the certificate into the certificate store on each of your Controllers.

a) Click the **Install certificate** option, select **Local Machine**, and then click **Next**.
b) Select **Place all certificates in the following store**, and then click **Browse**. Select **Trusted People** and then click **OK**. Click **Next** and then click **Finish**.

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

- Connections and resources
- Create machine catalogs

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

Connection to VMware cloud and partner solutions

May 5, 2025

After setting up Azure VMware Solution (AVS) cluster, Google Cloud VMware Engine, and VMware cloud on AWS, create the connections. See Connection to VMware for creating connections.

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

- Connections and resources
- Create machine catalogs

Service accounts for machine identity management

November 7, 2025

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:

- create or delete computer accounts in Active Directory without entering the domain credentials every time.
- manage stale Azure AD joined or Microsoft Intune enrolled devices without manually deleting them through the Azure AD or Intune portal.

Supported service account types

Citrix® allows the creation of the following service account based on the type of identity provider.

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

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.

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

May 5, 2025

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 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:

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

- 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 Web 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'
```

> **Note:**
>
> The `$password` is the matching password for the provided domain user account.

Perform machines identity-related actions

After an Active Directory or a Hybrid Azure AD 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

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

```
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.

Manage service accounts

May 5, 2025

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.

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

> **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.
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 Azure AD 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**.

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

3. Select the **Service Accounts** tab.
4. Select a service account and click **Delete**.

Image management

August 11, 2025

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 versions across hosting units within host connections of the same connection type. 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 within host connections of the same connection type. (only for Azure and VMware)

> **Note:**
>
> - This feature is currently applicable to Azure, Azure, Red Hat OpenShift, and VMware virtualization environments.
> - You can create an MCS machine catalog without using prepared images. In that case, you cannot get the benefits of the feature.

Use cases

Some of the use cases of image management functionality are:

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

- *Version management*: Image versions allow you to:
  - manage different iterations or updates to a particular image.
  - 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 the Web Studio from the image:

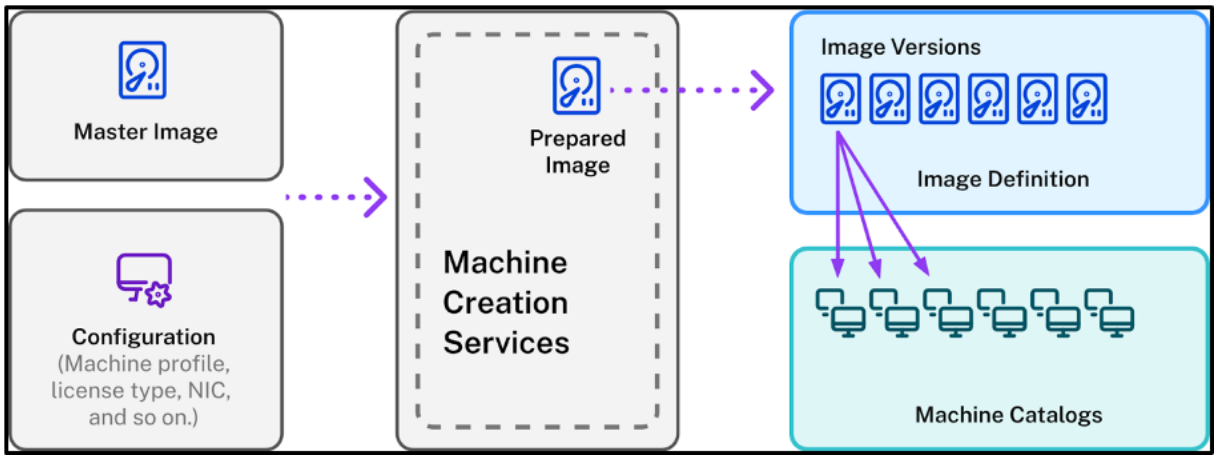


Image definition: Image definitions are a logical grouping of versions of an image. The image definition holds information about:

- why the image was created

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

- what OS it is for
- 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. You can share image versions across hosting units in both Azure and VMware environments, whether the hosting units are in the same hosting connection or not.

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. You can also share image version specs across hosting units in both Azure and VMware environments, whether the hosting units are in the same hosting connection or not.

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.s

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
- Currently, Azure confidential VM is not supported for image management.

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

Image lifecycle management using the Web Studio

Lifecycle of the image when you use the Web Studio is:

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.

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 also share image version specs across hosting units in both Azure and VMware environments, whether they are in the same hosting connection or not. In Azure, the sharing is achieved using the disk sharing capability of Azure Compute Gallery (ACG).

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 in your virtualization environment, whether in the same hosting connection or not.

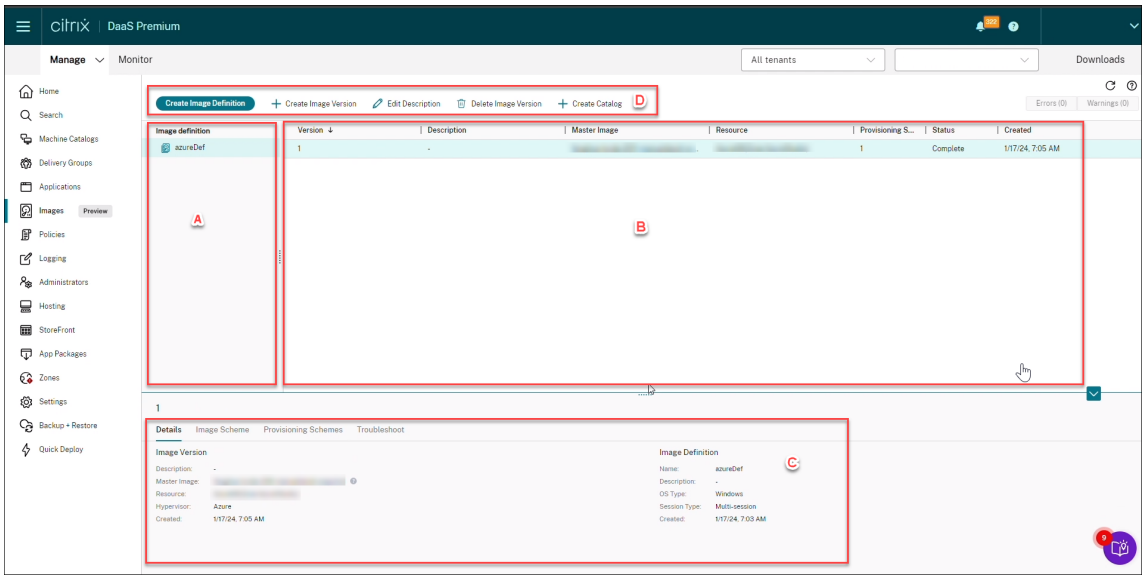
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 the Images node

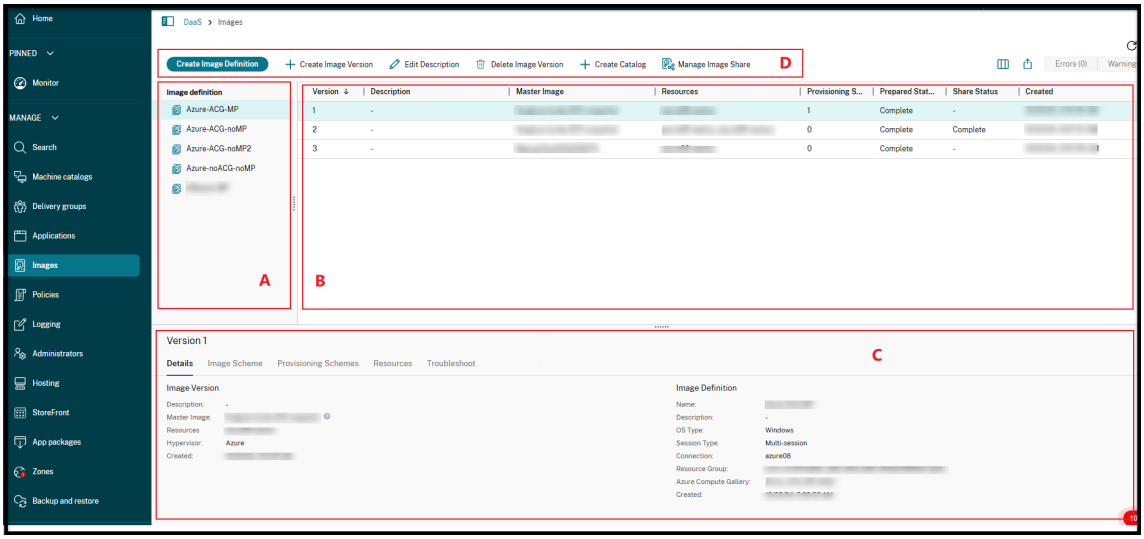
Use the **Images** node to create and manage MCS-prepared images. Its main view is divided into four parts:

- Without prepared image being shared across host unit



- With prepared image being shared across host unit:

© 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 of the selected image definition.
C	Details	• The **Details** tab displays detailed information about the selected image definition or 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** tab provides the error status of the selected image version.
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**.

Share prepared images across Azure subscriptions or tenants

To share a prepared image across subscriptions or tenants on the Azure platform, follow this example:

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

- **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.

Where to go next

Create prepared image machine catalogs
- Create a prepared image machine catalog in Azure
- Create a prepared image machine catalog in VMware
- Create a prepared image machine catalog in Red Hat OpenShift

Create prepared image machine catalogs

August 11, 2025

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Web Studio
- PowerShell commands

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

Currently, you can create prepared image machine catalogs in Azure, Red Hat OpenShift, and VMware virtualization environments.

More information

- Image management

Where to go next

- Create a prepared image machine catalog in Azure
- Create a prepared image machine catalog in VMware
- Create a prepared image machine catalog in Red Hat OpenShift
- Manage prepared image machine catalogs

Create a prepared image machine catalog in Azure

September 6, 2025

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Web 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 Web Studio

Create an image definition and initial image version

To create an image definition and the initial image version, do the following:

1. From Web 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 **Place image versions** in the 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.

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 **Version Description** page, enter a description for the initial image version created.
10. 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

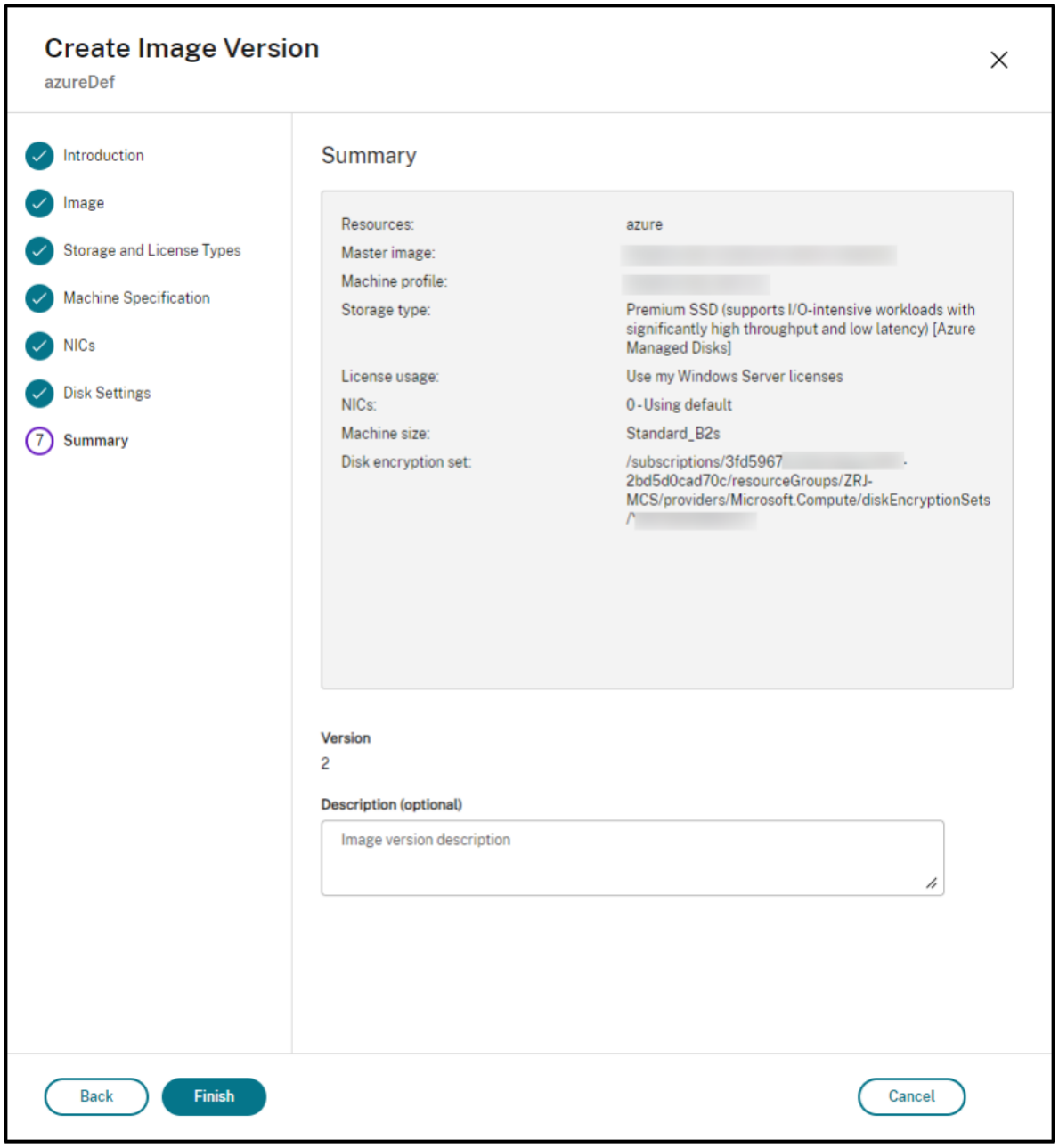
Image versions allow for the management of different iterations or updates to a particular image. This functionality enables you to maintain multiple versions of an image for different purposes.

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.

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

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. 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.

Shared prepared images

To share prepared images across different hosting units for Azure, follow these steps:

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.

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

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 **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 Master image type, follow the steps:
    a) Select Master image.
    b) Under the Master image, select an image. The blade lists all the images that belong to the same region as those of Resources.
    c) Click **Done**.
    d) For Prepared image type, select **Prepared image**.
    e) Under the **Prepared image**, select an image version of an image definition.
    f) Click the image version name. To view more details about the selected image version, click the version number, which is underlined.
    g) 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:

```
$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:

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

```
$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:

```
 $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\win2022-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. For example,

```
New-ProvImageVersionSpec
-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
    azureresourcegroup.resourcegroup\azure-vnet-eastus.
```

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

```
        virtualprivatecloud\dev.network" }
5
6  -ServiceOffering"XDHyp:\HostingUnits\azure\serviceoffering.folder\
       Standard_B2ms.serviceoffering" -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. For example,

```
1  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:

```
1  New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows -
       VdaSessionSupport MultiSession
2
3  $CustomProperties = @"
4  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
       instance">
5      <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
           Value="true" />
6      <Property xsi:type="StringProperty" Name="ResourceGroups" Value="rg
           " />
7      <Property xsi:type="StringProperty" Name="ImageGallery" Value="
           gallery" />
8  </CustomProperties>
9  "@
10
11 Add-ProvImageDefinitionConnection -ImageDefinitionName image1 -
       HypervisorConnectionName Azure28 -CustomProperties $CustomProperties
12
13 $imageVersion = New-ProvImageVersion -ImageDefinitionName image1 -
       Description "version 1"
14
15 $SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
       $imageVersion.ImageVersionUid `
16     -HostingUnitUid $hostingunit.HostingUnitUid `
17     -MasterImagePath "XDHyp:\HostingUnits\azure28\image.folder\abc.
           resourcegroup\def-snapshot.snapshot"
18
19 New-ProvImageVersionSpec -NetworkMapping @{
```

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

```
20  "0" = "XDHyp:\HostingUnits\azure28\virtualprivatecloud.folder\East US.
       region\virtualprivatecloud.folder\studio-mcs-infrastructure.
       resourcegroup\studio-mcs-vnet-eastus.virtualprivatecloud\mcs-dev.
       network"  }
21   -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.
       com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
       XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
       LicenseType`" Value=`"Windows_Server`" /></CustomProperties>" -
       ServiceOffering "XDHyp:\HostingUnits\azure28\serviceoffering.
       folder\Standard_B2s.serviceoffering" -SourceImageVersionSpecUid
       $SourceImageVersionSpec.ImageVersionSpecUid
22 Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx -
     HostingUnitName AzureWest
23 $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,

```
1 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,

```
1 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] [-
```

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

```
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```

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 `
     -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" -
```

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

```
      NetworkMapping @{
 8   "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
       azureresourcegroup.resourcegroup\azure-vnet-eastus.
       virtualprivatecloud\dev.network" }
 9    -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
10
11  Get-ProvTask -TaskId $Task.TaskId
12  $ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
13
14  Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
       .ProvisioningSchemeUid
```

More information

- Image management

Where to go next

- Manage prepared image machine catalogs

Create a prepared image machine catalog in Red Hat OpenShift

August 11, 2025

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Web 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

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

Use Web 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.
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.

© 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.

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.

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\YourNetworkAttachmentDefinition.network"  }
```

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

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 -
    SourceImageVersionSpecUid $masterImageVersionSpec.
    ImageVersionSpecUid -NetworkMapping @{
 "1" = "XDHyp:\HostingUnits\YourHostingUnitName\YourNamespaceName.
     namespace\YourNetworkAttachmentDefinition.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\YourNetworkAttachmentDefinition.network" }
```

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

More information

- Image management

Where to go next

- Manage prepared image machine catalogs

Create a prepared image machine catalog in VMware

April 17, 2026

Create prepared images and use the prepared images to create an MCS machine catalog using:

- Web 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 Web 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.
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.

© 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, 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.
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 con-

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

nections:

- 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**.

Known limitation: Custom storage policies are not preserved during cross-vCenter replication. The default storage policy of the target datastore is applied.

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

- 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 hosting 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.
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**

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

> 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.
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.

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

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
```

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
```

© 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. 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 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:

```
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
    >]
```

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 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:

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

```
$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
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme.ProvisioningSchemeUid
```

More information

- Image management

Where to go next

- Manage prepared image machine catalogs

Manage prepared image machine catalogs

May 5, 2025

You can update an existing MCS machine catalog with a different prepared image and manage the image definitions and versions using:

- Web Studio
- PowerShell

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

Use Web 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** on the left navigation pane and select a machine catalog that you want to update. Right-click and select **Change Prepared Image**.
2. On the **Image** page, select a prepared image.

   > **Note:**
   >
   > Applicable to Azure: 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. On the **Rollout strategy** page, select when you want to update this catalog with the selected prepared image.
4. On the **Summary** page, check the details. Click **Finish**.

You can see the history of image changes made to a catalog. To see the history, do the following:

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]
```

Or,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -
    ImageVersionSpecUid <Guid> [-DoNotStoreOldImage] [-RunAsynchronously
    ] [-PurgeJobOnSuccess]
```

Example of the complete set of Powershell commands to update a catalog:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "
    PreparationType -eq 'Mcs'"

Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
```

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:

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

- 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,

```
$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
```

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

7. Remove an image definition. For example,

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

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>
-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
```

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

```
17
18 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:

```
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>]
```

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

- Get image version details using the `Get-ProvImageVersion` command. For example:
  - 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,

```
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:

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

```
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

September 13, 2025

> **Important:**
>
> As of Citrix Virtual Apps and Desktops™ 7 2006, if your current deployment uses any of the following technologies, you can upgrade your deployment to the current release only after removing End of Life (EOL) items that use those technologies.
>
> - Personal vDisks (PvDs)
> - AppDisks™
> - Public cloud host types: Citrix CloudPlatform, Microsoft Azure Classic
>
> For details, see Remove PVD, AppDisks, and unsupported hosts.
>
> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

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

If you want to use public cloud host connections for your deployment, you need Hybrid Rights License to complete your fresh installation or upgrade to the current release.

When the installer detects one or more of the unsupported technologies or host connections without Hybrid Rights License, the upgrade pauses or stops. An explanatory message appears. The installer logs contain details. For more information, see Upgrade a deployment.

Introduction

Collections of physical or virtual machines are managed as a single entity called a machine catalog. All the machines in a catalog have the same type of operating system: multi-session OS or single-session OS, and Windows or Linux machines.

Web Studio guides you to create the first machine catalog after you create the site. After you create the first catalog, Web Studio guides you to create the first delivery group. Later, you can change the catalog you created, and create more catalogs.

> **Tip:**
>
> Upgrading an existing deployment enables the Machine Creation Services (MCS) storage optimization (MCS I/O) feature, no additional configuration is required. The Virtual Delivery Agent (VDA) and the Delivery Controller upgrade handle the MCS I/O upgrade.

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.

Consider:

- MCS supports a single system disk from the virtual machine image. It ignores the rest of the data disks attached to that image.
- If you use MCS to provision VMs, you provide a master image (or snapshot of an image) to create identical VMs in the catalog. Before you create the catalog, you first use the tools to create and configure the master image. This process includes installing a Virtual Delivery Agent (VDA) on the image. Then you create the machine catalog in Web Studio. You select that image (or snapshot), 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 for those machines.
- If you are creating a catalog using the PowerShell SDK directly, you can specify a hypervisor template (**VMTemplates**), rather than an image or a snapshot.

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

- Using a template to provision a catalog is considered an experimental feature. When using this method, virtual machine preparation might fail. As a result, the catalog cannot be published using the template.

When using MCS or Citrix Provisioning™ to create the first catalog, you use the host connection that you configured when you created the site. Later (after you create your first catalog and delivery group), you can change information about that connection or create more connections.

After you complete the catalog creation wizard, tests run automatically to ensure that it is configured correctly. When the tests complete, you can view a test report. Run the tests at any time from Web Studio.

> **Note:**
>
> MCS does not support Windows 10 IoT Core and Windows 10 IoT Enterprise. Refer to the Microsoft site for more information.

For technical details about the Citrix Provisioning tools, see Citrix Virtual Apps and Desktops Image Management.

RDS license check

Web Studio currently does not perform the check for valid Microsoft RDS licenses while creating a machine catalog that contains Windows multi-session OS machines. To view the status of the Microsoft RDS license for a Windows **multi-session OS machine**, go to Citrix Director. View the status of the Microsoft RDS license in the **Machine Details** panel. This panel is in the **Machine Details and the User Details** page. For more information, see Microsoft RDS license health.

VDA registration

A VDA must be registered with a Delivery Controller™ 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 an administrator can troubleshoot. Web Studio provides troubleshooting information in the catalog creation wizard, and after you add machines from a catalog to a delivery group.

After you add existing machines using the wizard, 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, either remove that machine, or add the machine. For example, if a message indicates that information might not be obtained about a machine, add the machine anyway.

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

For more information, see:

- CTX136668 for VDA registration troubleshooting guidance
- VDA versions and functional levels
- VDA registration methods

MCS catalog creation summary

Here's a brief overview of default MCS actions after you provide information in the catalog creation wizard.

- If you selected a master 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.
- 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, a master 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 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 difference 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 via the delivery controller.

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.

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

- Disk0 = Diff Disk: contains the OS when copied from the Master Base Image.
- 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 master 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.
  - 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.

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

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 in Web Studio 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.

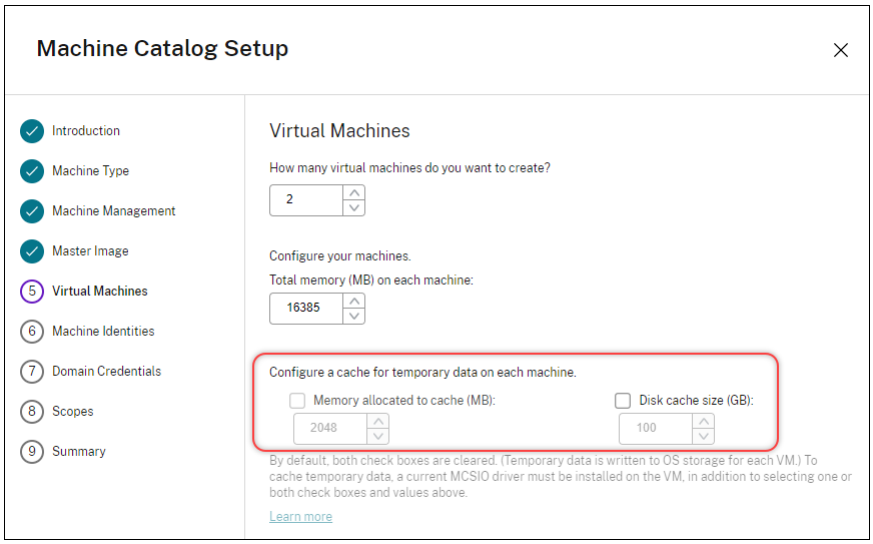
Enabling MCS storage optimization updates To enable MCS I/O storage optimization functionality, upgrade the Delivery Controller and the VDA to the latest version of Citrix Virtual Apps and Desktops.

> **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.

When enabling the MCS storage optimization update, consider the following:

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

- When creating a machine catalog, the administrator can configure the RAM and disk size.



- Updating an existing machine catalog to a new VM snapshot containing a VDA configured for version 1903 results in the following behavior: the new snapshot continues to use the existing catalog's MCS I/O setting for RAM and disk size. The existing raw disk is formatted.

> **Important:**
>
> MCS storage optimization changed with Citrix Virtual Apps and Desktops version 1903. This release supports file-based write cache technology, providing better performance and stability. The new functionality provided by MCS I/O might require a higher write cache storage requirement compared to previous Citrix Virtual Apps and Desktops releases. Citrix recommends that you reevaluate the disk size to ensure that it has sufficient disk space for the allocated workflow and extra pagefile size. The pagefile size is typically related to the amount of system RAM. If the existing catalog disk size is insufficient, create a machine catalog and allocate a larger write cache disk.

Assign a specific drive letter to MCS I/O write-back cache disk

You can assign a specific drive letter to the 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 the MCS I/O write-back cache disk. To assign drive letter to MCS I/O write-back cache disk, you can use PowerShell commands. The supported hypervisors are Azure, GCP, VMware, SCVMM, and XenServer.

> **Note:**
>
> This feature requires VDA version 2305 or later.

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

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 write-back cache disk

To assign a drive letter to a write-back cache disk:

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_d3e2d6352xxxxxxxx2130aa145ec77.
   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" Value="
   Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
   " />
```

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

```
<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. For information, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Prepare a master image

For information about creating connections hosts, see Connections and resources.

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 use different terms.
- Ensure that the host 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.

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 to allow access to the newest features. Failure to install a VDA on the master image causes the catalog creation to fail.
- 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).

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

- 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, plus 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 using Web 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. If you specify a master image rather than a snapshot when creating a catalog, Web Studio creates a snapshot. You cannot name it.

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)

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

- 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:

- 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.

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

> **Note:**
>
> - MCS doesn't support Microsoft Office activation using MAK.
> - 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:
  1. Add the registry DWORD value `Manual` under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfor\Activation`.
  2. 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:
   a) Add the registry DWORD value `Manual` under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfor\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.

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

- 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`, `WindowsActivationS`, `WindowsActivationStatusErrorCode`, and `WindowsActivationStatusError`.

You can check the error and verify the steps to resolve the issue.

Create a machine catalog using Web Studio

Before creating a catalog:

- Review this section to learn about the choices you make and the information you supply.
- Ensure that you have created a connection to the hypervisor, cloud service, and other resources that hosts your machines.
- If you have created a master image to provision machines, ensure that you have installed a VDA on that image.

To start the catalog creation wizard:

1. 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.
2. If you already created a catalog and want to create another, follow these steps:
   a) Sign in to Web Studio, select **Machine Catalogs** in the left pane, and then select **Create Machine Catalog** in the action bar.
   b) To organize catalogs using folders, create folders under the default **Machine Catalogs** folder. For more information, see Create a catalog folder.
   c) 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 following items. The wizard pages that you see differ, depending on the selections you make.

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

Operating system

Each catalog contains machines of only one type. Select one.

- **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. (See the Linux VDA documentation for details about that OS.)
- **Single-session OS:** A single-session OS catalog provides VDI desktops that you can assign to various different users.
- **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.

Machine management

This page does not appear when you are creating Remote PC Access catalogs.

The **Machine Management** page indicates how machines are managed and which tools you use to deploy machines.

Choose whether machines in the catalog are power managed through Web Studio.

- Machines are power managed through Web Studio, for example, VMs or blade PCs. This option is available only if you already configured a connection to a host.
- Machines are not power managed through Web Studio, for example, physical machines.

If you indicated that machines are power managed through Web Studio, choose which tool to use 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.

      > **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-`

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

> `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.

Desktop types (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 on. Select one of the following options:
  - **Yes, save changes on the local disk of the machine hosting virtual desktops.** (Persistent)
  - **No, 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.

- For **single-session OS** machines, you get the following options on the **Desktop Experience** page:
  - **I want users to connect to a new (random) desktop each time they log on.**
  - **I want users to connect to the same (static) desktop each time they log on.**

    For static desktops, 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 or full copy options are available for the Virtual machine copy mode in the **Virtual Machines** page.

If you select **Discard all changes and clear virtual desktops when the user logs off: Non-persistent**, you cannot configure the Virtual machine copy mode in the **Virtual Machines** page.

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

Image and machine profile

This page appears only when you are using MCS to create VMs.

1. Select an image type for the machine catalog, and then select an image. Two image types are available:

   - **Master image.** An image that has not yet gone through the image preparation process. The image preparation process is automatically initiated when catalog creation starts.

     > **Note:**
     >
     > - When you are using MCS, do not run Sysprep on master images.
     > - If you specify a master image rather than a snapshot, Web Studio creates a snapshot, but you cannot name it.

   - **Prepared image.** An image that has gone through the image preparation process and can be used for VM creation directly. Opting for prepared images rather than master images during catalog creation ensures faster and more reliable machine catalog creation, along with streamlined image lifecycle management.

     > **Note:**
     >
     > - VMs created using prepared images don't support hibernation.
     > - Currently, creating catalogs using prepared images are available only in Azure and VMware environments.

   For more information about how to create prepared images, see Image management (preview).

   When selecting an image, you can add a note for the selected image if needed.

   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.

   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.

2. To use an existing VM as the machine profile, select **Use a machine profile**, and then select the VM.

   > **Note:**
   >
   > Currently, using machine profiles is restricted to Azure, AWS, GCP, and VMware VMs.

   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.

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

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 select the virtual machine folder location. If not specified, the system considers the folder of the selected machine profile as the default location.

3. For AWS deployments, you can select a launch template as the machine profile.
4. 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.

Machines

This page does not appear when you are creating Remote PC Access catalogs.

The title of this page depends on what you selected on the **Machine Management** page: **Machines**, **Virtual Machines**, or **VMs and users**.

When using MCS:

- 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 performing **Add machines**.
- Choose the amount of memory (in MB) each VM has.
- 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 your deployment contains more than one zone, you can select a zone for the catalog.
- If you are creating static desktop VMs, select a virtual machine copy mode. See Virtual machine copy mode.
- If you are creating random desktop VMs that do not use vDisks, you can configure a cache to be used for temporary data on each machine. See Configure cache for temporary data.

When using other tools:

Add (or import a list of) Active Directory machine account names. You can change the Active Directory account name for a VM after you add/import it. If you specified static machines on the **Desktop Experience** page, you can optionally specify the Active Directory user name for each VM you add.

After you add or import names, you can use the **Remove** button to delete names from the list, while you are still on this page.

When using other tools (but 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 Delivery Controller. For details, see VDA versions and functional levels.

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

Add SIDs while creating virtual machines

You can now add the parameter `ADAccountSid` to uniquely identify the machines while creating new virtual machines.

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

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.

VDA versions and functional levels

A catalog's functional level controls which product features are available to machines in the catalog. Using features introduced in new product versions require a new VDA. However, machines in that catalog with an earlier VDA version cannot register.

A menu near the bottom of the **Machines** (or **Devices**) page allows you to select the minimum VDA level. This sets the catalog's minimum functional level. By default, the most current functional level is selected for on-premises deployments. If you follow the Citrix recommendation to always install and upgrade VDAs and core components to the latest version, you don't need to change this selection. However, if you must continue using older VDA versions, select the correct value.

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

A Citrix Virtual Apps and Desktops release might not include a new VDA version, or the new VDA does not impact the functional level. In such cases, the functional level might indicate a VDA version that is earlier than the installed or upgraded components. Each release's What's new article indicates any change in the default functional level.

The selected functional level affects the list of machines above it. In the list, a tooltip next to each entry indicates whether the machine's VDA is compatible with the catalog at that functional level.

Messages are posted on the page if the VDA on each machine does not meet or exceed the minimum functional level selected. You can continue with the wizard. Those machines will likely not be able to register with a Controller later. Alternatively, you can:

- Remove the machines containing older VDAs from the list, upgrade their VDAs and then add them back to the catalog.
- Choose a lower functional level that prevents access to the latest product features.

A message is also posted if a machine was not be added to the catalog because it is the wrong machine type. Examples include attempting to add a server to a single-session OS catalog, or adding a single-session OS machine originally created for random allocation to a catalog of static machines.

> **Important:**
>
> At release 1811, an extra functional level was added: **1811 (or newer)**. That level is intended for use with future Citrix Virtual Apps and Desktops features. The **7.9 (or newer)** selection remains the default. That default is valid for all deployments now.
>
> If you select **1811 (or newer)**, any earlier VDA versions in that catalog are unable to register with a Controller. However, if the catalog contains only VDAs at version 1811 or later supported versions, they are all eligible to register. This includes catalogs containing VDAs configured for later Citrix Virtual Apps and Desktops releases, including version 1903 and other 19XX releases before the current release.

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 the following 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.

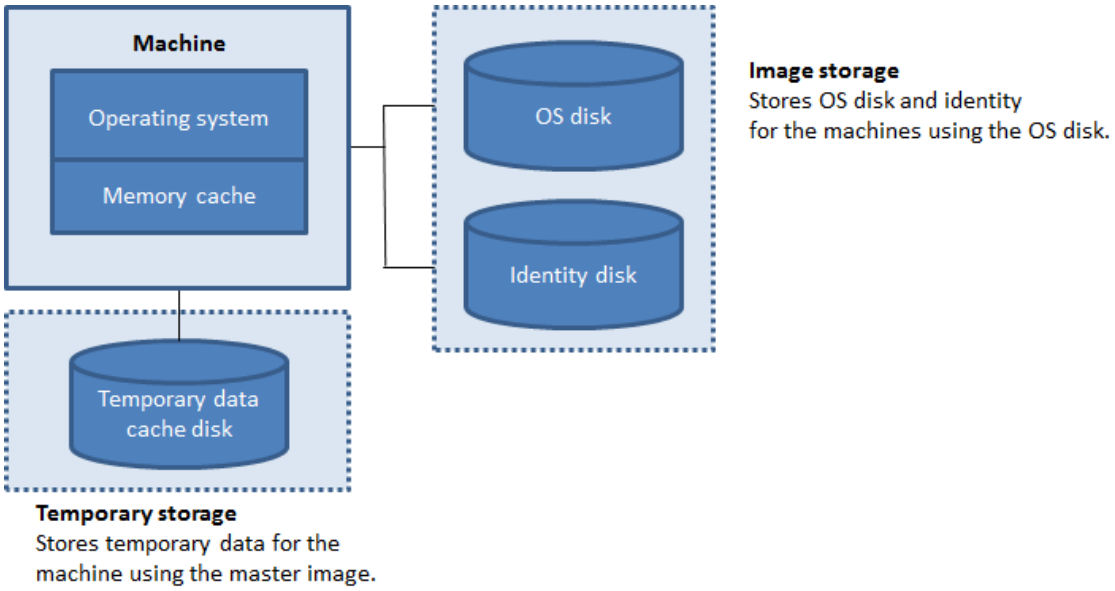
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Installing this driver is an option when you install or upgrade a VDA. By default, that driver is not installed.

- To enable drive letter assignment for disk caches, VMs must meet the following additional requirements:
  - Operating System: Windows
  - VDA version: 2305 or later

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.



- Configuring the write-back cache with a disk cache and no memory cache is removed. To enable a cache for temporary data, we recommend selecting **Disk cache size (GB)** and **Memory allocated to cache (MB)** and specifying a size greater than 0 for the memory cache. Temporary data is initially written to the memory cache. When the memory cache reaches its configured limit, the oldest data is moved to the temporary data cache disk.

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

- The memory cache is part of the total amount of memory on each machine. Therefore, if you enable the **Memory cache size (MB) (recommended)** checkbox, consider increasing the total amount of memory on each machine.
- If you keep the **Memory cache size (MB) (recommended)** checkbox cleared, temporary data is written directly to the disk cache, using a minimal amount of memory.
- 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.

- 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.
- If you clear both checkboxes, temporary data is not cached. It is written to the difference disk (located in the OS storage) for each VM. (This is the provisioning action in releases earlier than 7.9.)
- 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.

NIC (NICs)

This page does not appear when you are creating Remote PC Access catalogs.

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.

Machine accounts

This page appears only when creating Remote PC Access catalogs.

On the **Machine Accounts** page, specify the Active Directory machine accounts or Organizational Units (OUs) to add that correspond to users or user groups. Do not use a forward slash (/) in an OU name.

When adding OUs, you can do the following if the domain is not shown in the list:

- Search for it using an exact match.
- Browse all domains to find it.

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

You can choose a previously configured power management connection or elect not to use power management. If you want to use power management but a suitable connection hasn't been configured yet, you can create that connection later and then edit the machine catalog to update the power management settings.

Machine identities

This page appears only when using MCS to create VMs.

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.
- **Hybrid Azure Active Directory 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 Hybrid Azure Active Directory joined.

  > **Note:**
  >
  > - Before you can use hybrid Azure Active Directory 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.

> **Important:**
>
> - If you select **On-premises Active Directory** or **Hybrid Azure Active Directory 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 2311 or later of the VDA as the mini-

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

> mum functional level for the catalog. To make it available, update the minimum functional level.

If you create accounts, you must have permission to create computer accounts in the OU where the machines reside. Each machine in the catalog must have a unique name. Specify the account naming scheme for the machines that you want to create. For more information, see Machine account naming scheme.

> **Note:**
>
> Make sure that OU names do not use forward slashes (/).

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. The Web Studio interface 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, be aware of the following rules:

- The naming scheme must contain at least one wildcard. 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 (-).

Also, leave enough room for growth when specifying the naming scheme. Consider this example: If you create 1,000 machine accounts with the scheme "veryverylong#", the last account name created (veryverylong1000) contains 16 characters. Therefore, the naming scheme results in one or more machine names that exceed the maximum of 15 characters.

You can indicate whether the sequential values are numbers (0-9) or letters (A-Z):

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

- **0-9**. If selected, the specified wildcards resolve to sequential numbers.

  > **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.

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:
   - 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**.

> **Note:**
>
> If the identity type you selected in **Machine Identities** is **Hybrid Azure Active Directory joined**, the credentials you enter must have been granted the `Write userCertificate` permission.

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

Summary, name, and description

On the **Summary** page, review the settings you specified. Enter a name and description for the catalog. This information appears in Web Studio.

When you're done, click **Finish** to start the catalog creation.
When you're done, select **Finish** to start the catalog creation.

In **Machine Catalogs**, the new catalog appears with an inline progress bar.

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

MCS time synchronization

Time synchronization is determined by the master image and the type of machine identity joined catalog. You get the following time synchronization method according to the master image and the catalog:

Master image	Catalog	Resultant time synchronization method
NDJ	AD or Hybrid Azure AD	By default, NT5DS. You can disable MCS from changing time synchronization setting using registry settings in the master image
NDJ	NDJ or Azure AD	Same as the original time synchronization setting
AD or Hybrid Azure AD	AD or Hybrid Azure AD	Same as the original time synchronization setting
Azure AD	Azure AD	Same as the original time synchronization setting

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

> **Note:**
>
> The original time synchronization is controlled by the following registry setting and cannot be changed:
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config
>
> Value: MaxAllowedPhaseOffset, MaxNegPhaseCorrection, and MaxPosPhaseCorrection
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
>
> Value: Type

To disable MCS from changing the time synchronization setting, set the value of the following registry setting in the master image:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Name: TimeSyncMethodKeep
- Type: DWORD
- 0 (Or, value TimeSyncMethodKeep not configured): Does not keep the original time synchronization setting.
- 1: Keeps original time synchronization setting and default parameters values.

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.

- In Azure: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`
- In GCP: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`

Troubleshoot

> **Important:**
>
> After creating the machine catalog using Web Studio, you can no longer use the `Get-ProvTask` PowerShell command to retrieve the tasks associated with machine catalog creation. This restriction is a result of Web Studio deleting those tasks after machine catalog creation regardless of whether the catalog is created successfully.

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

Citrix recommends collecting logs to help the Support team provide solutions. When using Citrix Provisioning, use the following procedure to generate log files:

1. On the master image, create the following registry key with the value of 1 (as a DWORD (32-bit) value): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Shut down the master image and create a snapshot.
3. On the Delivery Controller, run the following PowerShell command: `Set-ProvServiceConfiguration -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Create a catalog based on that snapshot.
5. When the preparation VM is created on the hypervisor, log in and extract the following files from the root of C:\: Image-prep.log and PvsVmAgentLog.txt.
6. Shut down the machine, at which point it reports the failure.
7. Run the following PowerShell command to re-enable auto shutdown of the image preparation machines: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAu`
.

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 write-back cache disk:

1. Open the **PowerShell** window.

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

2. Run `asnp citrix*`.
3. Create an identity pool if not already created. For information, see Creating a Catalog.
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_d3e2d6352xxxxxxxx2130aa145ec77.
   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" 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>'
```

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

5. Finish creating the catalog.

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_NonMachineProfileWin19Machines.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
```

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

```
        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.

Where to go next

For information on creating specific cloud services catalogs, see:

- Create an AWS catalog
- Create a XenServer 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
- Create a VMware catalog

If this is the first catalog created, Web Studio guides you to create a delivery group.

To review the entire configuration process, see Install and configure.

You can create a Citrix Provisioning catalog using Web 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 environments, you can currently create the catalogs using only PowerShell commands. For more information, see Create Citrix Provisioning catalogs in Citrix Studio.

More information

- Create and manage connections and resources

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

- Create catalogs of different join types
- Manage machine catalogs

Create an AWS catalog

October 15, 2025

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to AWS virtualization environments.

> **Note:**
>
> Before creating an AWS catalog, you need to finish creating a connection to AWS. See Connection to AWS.

Limitation

From Citrix Virtual Apps and Desktops™ 2203 LTSR and later, MCS AWS plug-in makes `DescribeInstanceTypes` AWS API call and if that succeeds, then MCS uses the inventory name created from the API response.

Therefore, when you upgrade from Citrix Virtual Apps and Desktops 1912 to 2203 or later, disable the `DefineInstanceType` permission on AWS, and then update the existing catalog using `Set-ProvScheme` command to match the AWS naming scheme. Then, add the `DescribeInstanceType` permissions back after catalog update is complete and the service offering matches AWS naming scheme.

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.

Configure AWS tenancy

AWS provides the following tenancy options:

- Shared tenancy (the default type): Multiple Amazon EC2 instances from different customers might reside on the same piece of physical hardware.

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

- Dedicated tenancy: Your EC2 instances run only on hardware with other instances that you have deployed. Other customers do not use the same piece of hardware.

You can use MCS to provision AWS dedicated hosts by using PowerShell.

Configure AWS dedicated host tenancy using PowerShell

You can create a catalog of machines with host tenancy defined through PowerShell.

An Amazon [EC2] dedicated host is a physical server with [EC2] instance capacity that is fully dedicated, allowing you to 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.

The requirements for provisioning to AWS hosts include:

- 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.
- enable **auto-placement**.

To provision to a dedicated host in AWS using PowerShell, use the **New-ProvScheme** cmdlet with the parameter `TenancyType` set to *Host*.

Refer to the Citrix Developer Documentation for more information.

Capture machine properties from machine profiles

When creating a catalog to provision AWS machines using MCS, you can use a machine profile to preset certain machine property settings.

To do so, follow these steps:

1. Store the machine profiles in the same availability zone as the resources where you are creating this catalog.
2. On the **Machine Template** page of the catalog creation wizard, select **Use a machine profile**. Machine profiles that are in the same available zone as the resources you selected are shown.
3. Select a machine profile as needed.

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

Tag AWS operational resources

When creating a catalog to provision machines in AWS by using MCS, you can control whether to apply the IAM role and tag properties to those machines. You can also control whether to apply machine tags to 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
- S3 buckets
- S3 objects
- Launch templates
- AMIs

Tag operational resources using Web Studio

When creating a catalog to provision machines in AWS by using MCS, you can control whether to apply machine tags to operational resources by selecting the **Apply machine tags to operational resources** option on the **Machine Template** page.

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 instance and AMI.

Tag operational resources using PowerShell

To use PowerShell to tag resources:

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

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>
```

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 AWS EC2 console, you cannot see **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.

Create a catalog using a machine profile

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 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.
> - MCS provisions VMs with Identity disks of GP3 volume type. As GP3 volume type is the cheapest option offered by AWS, this feature minimizes cost. The implementation is ap-

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

> plicable only to the VMs added to a new catalog and new VMs added to an existing catalog. Existing VMs created before this feature will continue to have ID disks with GP2 volume type, unless the ID disk is reset.

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.

  > **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 `AwsCaptureInstancePro` or specify a machine profile.

The important considerations after creating an MCS machine catalog:

- You cannot change a catalog from machine profile-based to non-machine profile-based catalog.

Create a machine catalog using a machine profile

To create a machine catalog using a machine profile:

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,

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
      Domain abcdf -NamingSchemeType Numeric
```

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

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. For more information, see Citrix PowerShell SDK.

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-0
   xxxxxxxx).vm"
```

Create a catalog with launch template version

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

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

- Security Groups
- 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" `
-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 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
```

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

7. Complete creating the catalog. For more information, see Citrix PowerShell SDK

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-08
   xxxxxxxxx).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 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, you can create an MCSIO enabled non-persistent catalog.

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.
- `WriteBackCacheDriverLetter`: Specifies the drive letter to assign for the cache storage disk. 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 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.

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'  }
```

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

```
5
6  $SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-east-1a.
       availabilityzone\private.securitygroup' )
7  $ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
       Instance.serviceoffering'
8  $CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,
       false'
9
10
11 $provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
       -HostingUnitUid $HostingUnitUid `
12 -IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
13 - MasterImageVM $MasterImageVM `
14 -NetworkMap $NetworkMap `
15 -ServiceOffering $ServiceOffering `
16 -SecurityGroup $SecurityGroup `
17 -CustomProperties $CustomProperties `
18 -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, 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:

- 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)

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

- 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:

  1. Create a new snapshot of that volume.
  2. Create a new volume from that snapshot
  3. 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.
- 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.

© 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 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 cannot 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.

VMs added to the created catalog have NitoTPM and UEFI secure boot enabled.

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

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

(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:

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

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

Filter VM instances

An AWS EC2 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 EC2 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:

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

```
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:

```
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
```

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

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
    -015xxxxxxxxx" -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.

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.

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

- 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,false;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
```

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, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- To manage catalogs, see Manage machine catalogs and Manage an AWS catalog

More information

- Create and manage connections and resources
- Connection to AWS

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

- Create machine catalogs

Create an Azure Local catalog

September 6, 2025

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Azure Local environments.

> **Note:**
>
> Before creating an Azure Local machine catalog, you need to finish creating a connection to Azure Local. See Connection to Azure Local.

Create a catalog using Web Studio

There can be VMs created on Azure Local, which are non-MCS provisioned VMs. In such cases, you can use Web Studio to power manage those VMs by importing the VMs.

To create a catalog by importing the VMs created on Azure Local outside Citrix®:

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 the VMs created on Azure Local outside Citrix.

Where to go next

- If this is the first catalog created, Web Studio guides you to create a delivery group
- For power managing Azure Local VMs, see Power manage Azure Local VMs.

More information

- Create and manage connections and resources
- Connection to Azure Local
- Create machine catalogs

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

Create a XenServer® catalog

September 6, 2025

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to XenServer 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 XenServer connection

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.

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. Clear 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.

Limitations

- If a Citrix Virtual Apps and Desktops deployment with its VMs hosted on Citrix Hypervisor 8.2 Cumulative Update 1 uses multiple GFS2 SRs in a single MCS catalog, the VMs in the catalog cannot access the VDIs during deployment. The error "VDI is currently in use"is reported.
- Citrix Hypervisor 8.2 Cumulative Update 1 doesn't support MCS full clone VMs with GFS2 SRs.

For more information, see Constraints.

These constraints do not apply to XenServer 8 and later.

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

Create a machine catalog using a machine profile

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.

> **Note:**
>
> Currently, you can use only a VM as a machine profile input.

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`
- `VMMemory`
- `NetworkMapping`

To 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:

```
1 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.

```
1 $password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
2 New-AcctIdentity -IdentityPoolName "ExampleIdentityPool" -Count 10
     -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. Run the `New-ProvScheme` command to create a catalog. For example:

```
1 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">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
```

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

```
3 </CustomProperties>'
4 -MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
     vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
     " -Scope @() -SecurityGroup @()
5 -MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
     ExampleMachineProfile.vm"
```

6. Register provisioning scheme as a broker catalog. For example:

```
1 $ConfigZone = Get-ConfigZone | Where-Object {
2   $_.Name -eq "xxxxxx"  }
3
4 New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
     Description "Machine profile catalog" -ProvisioningSchemeId
     fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
     SessionSupport MultiSession -PersistUserChanges Discard -
     ZoneUid ($ConfigZone.Uid)
```

7. Add VMs to the catalog.

To update a catalog with a new machine profile:

1. Run the `Set-ProvScheme` command. For example:

```
1 Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
     MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
     ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
     snapshot"
```

   For more information on the Set-ProvScheme command, see Set-ProvScheme.

> **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.

Where to go next

- If this is the first catalog created, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- To manage catalogs, see Manage machine catalogs and Manage a XenServer catalog

More information

- Create and manage connections and resources

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

- Connection to XenServer
- Create machine catalogs

Create a Google Cloud Platform catalog

September 26, 2025

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.

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.

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

Create a machine catalog

You can create a machine catalog in two ways:

- Create a machine catalog using Web Studio
- Create a machine catalog using PowerShell

Create a machine catalog using Web Studio

> **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.

Follow the guidance in Create machine catalogs. The following description is unique to Google Cloud catalogs.

1. Sign in to Web Studio and select **Machine Catalogs** in the left pane.
2. Select **Create Machine Catalog** in the action bar.
3. On the **Operating System** page, select **Multi-session OS** and then select **Next**.
   - Citrix Virtual Apps and Desktops™ also supports single-session OS.
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) To inherit machine properties from a machine profile, select **Use a machine profile** and select a profile 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.

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

> - If you select an instance template as the machine profile, then all 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 Types** 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 https://cloud.google.com/compute/docs/disks/.

7. On the **Virtual Machines** page, specify how many VMs you want to create, view the detailed specification of the VMs, and then select **Next**. If you 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.

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:

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

- 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.

- 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.

9. On the **Computer Accounts** 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 **Summary** page, confirm the information, specify a name for the catalog, and then select **Finish**.

    > **Note:**
    >
    > Starting with version 2402, GCP catalog names must comply with these rules:
    >
    > - Start with a lowercase letter.
    > - Include only lowercase letters (a-z), numbers, and hyphens.
    > - End with either a lowercase letter or a number.

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

> When you attempt to rename existing GCP catalogs that don't comply with these rules, error messages appear and guide you to rename them according to the updated rules.

Machine catalog creation might take a long time to complete. To verify that the machines are created on the target node groups, go to the Google Cloud console.

Import manually created Google Cloud machines

You can *create a connection to Google Cloud* and then *create a catalog containing Google Cloud machines*. Then, you can manually power cycle Google Cloud machines through Citrix Virtual Apps and Desktops. With this feature, you can:

- Import manually created Google Cloud multi-session OS machines into a Citrix Virtual Apps and Desktops machine catalog.
- Remove manually created Google Cloud multi-session OS machines from a Citrix Virtual Apps and Desktops catalog.
- Use existing Citrix Virtual Apps and Desktops 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 Virtual Apps and Desktops provisioning workflow, nor the removal of any existing feature. We recommend that you use MCS to provision machines in Web 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:

1. 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.
2. You must create two firewall rules, one each for ingress and egress. These firewall rules are used during the image mastering process.

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

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 Virtual Apps and Desktops. 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:

1. **compute.firewalls.list** - This permission is mandatory. It allows MCS to retrieve the list of firewall rules present on the Shared VPC.
2. **compute.networks.list** - This permission is mandatory. It allows MCS to identify the Shared VPC networks available to the service account.
3. **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.
4. **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:
  - Allows access to all Shared VPCs within the host project.
  - Requires the permissions #3 and #4 must be assigned to the service account.
- Subnet-level permission:
  - Allows access to specific subnets within the Shared VPC.
  - Permissions #3 and #4 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:**

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

> For more information about the differences between project-level and subnet-level permissions, see the Google Cloud documentation.

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:

```
"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."
```

Configuring the shared VPC

Before adding the Shared VPC as a host connection in Web Studio, complete the following steps to add service accounts from the project you intend to provision into:

1. Create an IAM role.
2. Add the service account used to create a CVAD host connection to the Shared VPC host project IAM role.
3. Add the Cloud Build service account from the project you intend to provision into to the Shared VPC host project IAM role.
4. Create firewall rules.

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

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**.

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**.

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

b) Select **CREATE**.

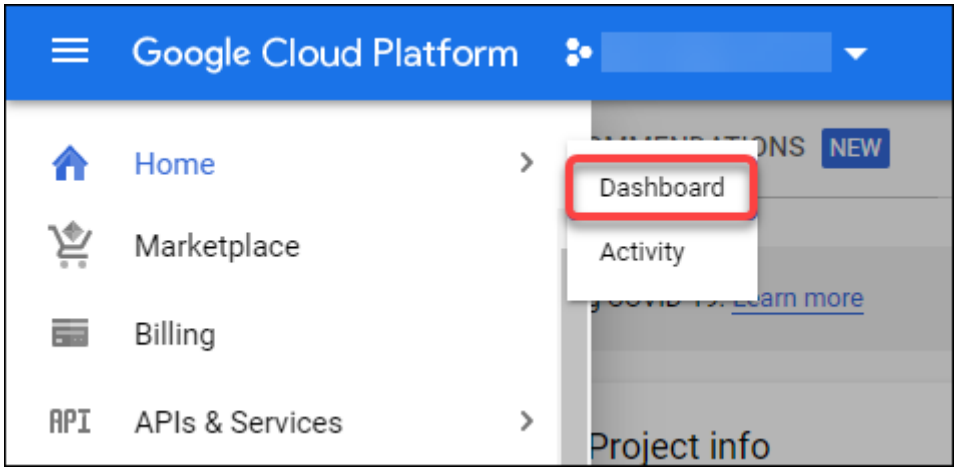
Add a service account to the host project IAM role After creating an IAM role, do the following steps to add a service account for the host project:

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**.

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 what the project ID number is for your project by selecting **Home** and **Dashboard** in the Google Cloud console:



Find the **Project Number** below the **Project Info** area of the screen.

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.

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

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 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.
   - **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 steps 1–4 to create another rule. For **Direction of traffic**, select **Egress**.

Add a connection Add a connection to the Google cloud environments. See Add a connection.

Enable zone selection

Citrix Virtual Apps and Desktops 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

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

Reserving 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.

Creating 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 After setting the node affinity label, configure the machine catalog.

Customer Managed Encryption Keys (CMEK)

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 Virtual Apps and Desktops account must have the correct permissions in the project where the key is stored. 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.

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

> **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.

Assign permissions to Citrix Virtual Apps and Desktops 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 permissions One option is to provide Citrix Virtual Apps and Desktops 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 Virtual Apps and Desktops. This allows you to browse regional keys in the relevant project in the inventory.

Resource Level Permissions For the other option, resource level permissions, in the Google Cloud console, browse to the `cryptoKey` you use for MCS provisioning. Add Citrix Virtual Apps and Desktops 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 Virtual Apps and Desktops 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, described below.

Provisioning with CMEK using custom properties

When creating your Provisioning Scheme via PowerShell, specify a `CryptoKeyId` property in `ProvScheme CustomProperties`. For example:

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

```
'<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`

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"/>`.

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.

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:

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

```
1 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).
2 We're aware that this can make things untidy, but we have no immediate
    plans to change this.
3 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 Virtual Apps and Desktops 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 Virtual Apps and Desktops 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.

Create a machine catalog using PowerShell

This section details how you can create catalogs using PowerShell:

- Create a catalog with persistent write-back cache disk
- Improve boot performance with MCSIO
- Create a machine catalog using a machine profile
- Create a machine catalog with machine profile as an instance template
- Use PowerShell to create a catalog with shielded VM
- Create Windows 11 VMs on the sole-tenant node

Create a catalog with persistent write-back cache disk

To configure a catalog with persistent write-back cache disk, use the PowerShell parameter `New-ProvScheme CustomProperties`.

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

> **Tip:**
>
> Use the PowerShell parameter here 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.

Setting the `PersistWBC` property to **`true`** does not delete the write-back cache disk when the Citrix Virtual Apps and Desktops administrator shuts down the machine from the management interface.

Setting the `PersistWBC` property to **`false`** deletes the write-back cache disk when the Citrix Virtual Apps and Desktops 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`**:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
     benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>
```

> **Note:**
>
> 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

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

> 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\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-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 ``````<!--NeedCopy
   -->
````````Groups" Value="benvaldev5RG3" />
```

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

```
<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`"
   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\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

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 `CryptoKeyIs` 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

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

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 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 must 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 New-ProvScheme 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.template
   ```

   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. For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

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

Change the machine profile of an existing machine catalog to be an instance template

The detailed steps to change the machine profile of an existing machine catalog to be an instance template are:

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/.

Use PowerShell to 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.

To create an MCS machine catalog with shielded VM using machine profile workflow.

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.
   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
```

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

3. Finish creating the machine catalog.

To update 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:

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.

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

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.

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
```

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

> **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.

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 the Web 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 the Web Studio, see Create a machine catalog using Web 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

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

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

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 Web Studio or PowerShell commands.
3. If using Web 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" `
```

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

```
-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):

```
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" `
-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.

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

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:

   ```
   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.

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

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 using Web Studio or use PowerShell commands.

Using Web 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 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
```

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

Where to go next

- If this is the first catalog created, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- 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

May 5, 2025

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:

- Web Studio
- PowerShell commands

Create a machine catalog using Web 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**.

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

3. On the **Virtual Machines** page, add machines and their Active Directory machine accounts. You can do either of the following:

    - 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:

```
1 New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
     "103.14.252.249" -AllocationType "Random" -IsRemotePC $False -
     MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
     BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
     Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
     -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
     "103.14.252.249" -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, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- 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

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

Create a Microsoft Azure catalog

April 2, 2026

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to Microsoft Azure Resource Manager cloud environments.

> **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:

- Create a machine catalog using an Azure Resource Manager image in Web Studio
- Create a machine catalog using PowerShell

Create a machine catalog using an Azure Resource Manager image in Web Studio

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 the Azure Resource Manager. For general information about images, see Create machine catalogs.

> **Note:**
>
> 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

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

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 randomly generated. For example, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

In the machine catalog creation wizard:

- The **Machine Type** and **Machine Management** pages do not contain Azure-specific information. Follow the guidance in the Create machine catalogs article.
- On the **Image** page, choose an image that you want to use as the template for creating machines in this catalog.

  If you select **Master image** as the image type to use, click **Select an image** and follow these steps to select a master image as necessary:

  1. (Applicable only to connections configured with shared images within or across tenants) Select a subscription where the image resides.
  2. Select a resource group.
  3. Navigate to the Azure VHD, the Azure Compute Gallery, or the Azure image version. Add a note for the selected image if needed.

  When selecting an image, consider the following:

  - Verify that a Citrix VDA is installed on the image.
  - If you select a VHD attached to a VM, you must shut down the VM before proceeding to the next step.

  > **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.
  > - 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. Trusted Launch is not supported for Shared Image Gallery. For information about Azure Trusted Launch, see https://docs.microsoft.com/en-us/azure/virtual-machin

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

> es/trusted-launch.
> - 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.
> - When you select a master image for machine catalogs in Azure, MCS identifies the OS type based on the master image and machine profile you select. If MCS can't identify it, select the OS type that matches the master image.
> - 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.

If you select **Prepared image** as the image type to use, click **Select an image** and select a prepared image as necessary.

To ensure successful VM creation, verify that the image has Citrix VDA 2311 or later installed and MCSIO is present on the VDA.

Once you select an image, the **Use a machine profile (mandatory for Azure Active Directory)** checkbox is automatically selected. Click **Select a machine profile** to browse to a VM or an ARM template spec from a list of resource groups. VMs in the catalog can inherit configurations from the selected machine profile.

Validate the ARM template spec to make sure whether it can be used as a machine profile to create a machine catalog. 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>`

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

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)
- Tags placed on the VM

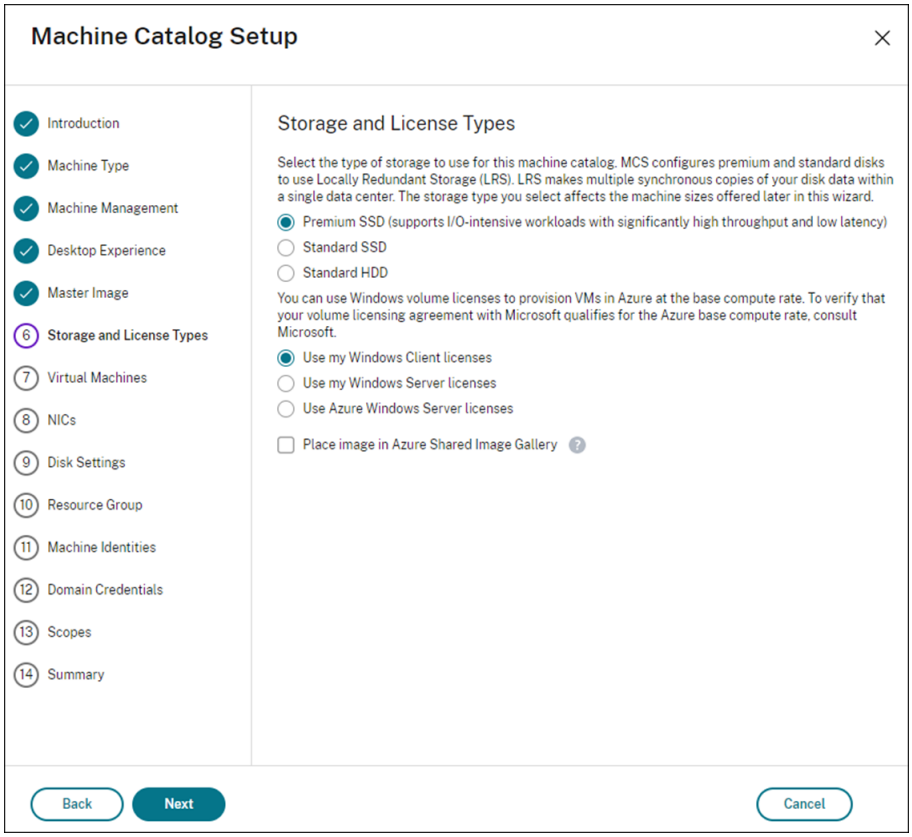
After you create the catalog, you can view the configurations that the image inherits from the machine profile. On the **Machine Catalogs** node, select the catalog to view its details in the lower pane. Then, click the **Template Properties** tab to view machine profile properties. The **Tags** section 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 dedicated 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 VMs. 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 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.

- The **Storage and License Types** page appears only when you use an Azure Resource Manager image.

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



You have the following storage types to use for the machine catalog:

- **Premium SSD**. Offers a high-performance, low-latency disk storage option suitable for VMs with I/O-intensive workloads.
- **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.
- **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. Be aware of the following considerations 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.

> **Note:**
>
> The identity disk is always created using Standard SSD irrespective of the storage type that

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

> you choose.

The storage type determines which machine sizes are offered on the **Virtual Machines** page of the wizard. MCS configures premium and standard disks to use Locally Redundant Storage (LRS). LRS makes multiple synchronous copies of your disk data within a single data center. Azure ephemeral OS disks use the local disk of the VMs to store the operating system. For details about Azure storage types and storage replication, see the following:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- 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.

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/.

© 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.

  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>'
```

  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="
```

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

```
        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>'
```

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

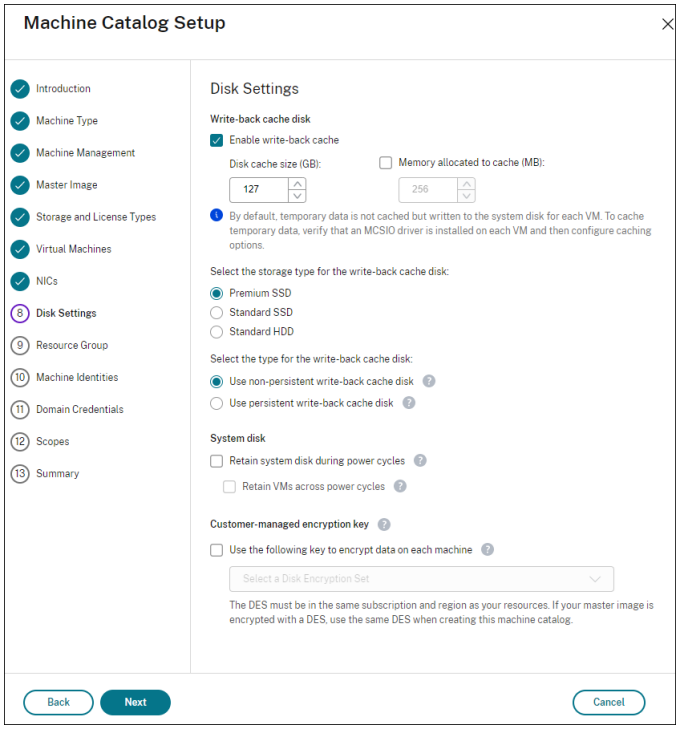
Azure Compute Gallery (formerly Azure Shared Image Gallery) is a repository for managing and sharing images. It lets you make your images available throughout your organization. We recommend that you store an image in SIG when creating large non-persistent machine catalogs because doing that enables 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 Compute 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.

> **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.

- On the **Virtual Machines** page, indicate how many VMs you want to create. You must specify at least one and select a machine size. After catalog creation, you can change the machine size by editing the catalog.
- The **NICs** page does not contain Azure-specific information. Follow the guidance in the Create machine catalogs article.
- 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. These settings apply to both Azure and GCP environments.

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



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
- 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

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

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.

- 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 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 savings**. 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.

- On the **Resource Group** page, choose whether to create resource groups or use existing groups.

  - If you choose to create resource groups, select **Next**.

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

- If you choose to use existing resource groups, select groups from the **Available Provisioning Resource Groups** list. **Remember**: 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.

- On the **Machine Identities** page, choose an identity type and configure identities for machines in this catalog. If you select the VMs as **Azure Active Directory joined**, you can add them to an Azure AD security group. Detailed steps are as follows:

  1. From the **Identity type** field, select **Azure Active Directory joined**. The **Azure AD security group (optional)** option appears.
  2. Click **Azure AD security group: Create new**.
  3. Enter a group name, and then click **Create**.
  4. Follow the onscreen instructions to sign in to Azure.
     If the group name doesn't exist in Azure, a green icon appears. Otherwise, an error message appears requesting you to enter a new name.
  5. Enter the machine account naming scheme for the VMs.

  After catalog creation, Citrix Virtual Apps and Desktops™ accesses Azure on your behalf 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.

  Adding VMs with a different naming scheme to this catalog requires you to sign in to Azure. Citrix Virtual Apps and Desktops can then access Azure and create a dynamic membership rule based on the new naming scheme.

  When deleting this catalog, deleting the security group from Azure also requires signing in to Azure.

- The **Domain Credentials** and **Summary** pages do not contain Azure-specific information. Follow the guidance in the Create machine catalogs article.

Complete the wizard.

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.

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

- 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 temporary disk is used for write-back cache while creating machine catalog.

Scenario	Outcome
All conditions to use 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.

Create an Azure template spec

You can create an Azure template spec in the Azure portal and use it in Web 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 just 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, change 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\bggTemplateSpec.templatespec
```

- To get information about the template spec version, run:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
```

Use 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 the Web Studio or PowerShell commands.

- For Web Studio, see Create a machine catalog using an Azure Resource Manager image in Web Studio
- For PowerShell, see Use template spec in creating or updating a catalog using PowerShell

Azure server-side encryption

Citrix Virtual Apps and Desktops 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:

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

- 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:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

Select a DES from the list. The DES you select must be in the same subscription and region as your resources.

See Creating a machine catalog using customer-managed key.

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

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 host is:

- Not supported for all Azure machine sizes
- Incompatible with Azure disk encryption

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>
```

3. Create a VM or a template spec, as an input for machine profile, in 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

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

- Cache Disk: Gets encrypted through Customer-managed key and Platform-managed key

You can create the machine catalog using Web 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.vm).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_templatespec.templatespec\EncryptionAtHost.
   templatespecversion).AdditionalData
```

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 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 Web Studio and PowerShell commands. See Create a machine catalog with double encryption for PowerShell commands.
> - You can use a 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.

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

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 DiskEncryptionSet 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.

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.

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 ephemeral disks

An Azure ephemeral disk allows you to repurpose the cache disk or temporary 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 disks.

> **Note:**
>
> Persistent catalogs do not support ephemeral OS disks.

Ephemeral OS disks require that your provisioning scheme uses managed disks and a Shared Image Gallery.

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

Storing an ephemeral OS temporary disk

You have the option of storing an ephemeral OS disk on the VM temp disk or a resource 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 or resource 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 VM's temporary (resource) 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.
- The PowerShell parameters (`UseWriteBackCache` and `UseEphemeralOsDisk`) fail with proper error messages if you set them to **true** in `New-ProvScheme` or `Set-ProvScheme`.
- For existing machine catalogs created with both features enabled, you can still:
  - update a machine catalog.
  - add or delete VMs.
  - delete a machine catalog.

Azure Compute Gallery

Use Azure Compute Gallery (formerly Azure 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. The shared image 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.

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

- *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 published image.

> **Note:**
>
> Shared Image Gallery functionality is only compatible with managed disks. It is not available for legacy machine catalogs.

For more information, see Azure Compute Gallery overview.

For information on creating or updating a machine catalog using Azure Compute Gallery image using PowerShell, see Create or update a machine catalog using an Azure Compute Gallery image.

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.

Important considerations for confidential VMs

The important considerations for supported VM sizes and creating machine catalog with confidential VMs are as follows:

- Supported VM sizes: Confidential VMs support the following VM sizes:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Create machine catalogs with confidential VMs.
  - You can create a machine catalog with Azure Confidential VMs using Web Studio and PowerShell commands.
  - 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. The security types are:

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

- **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`.

- 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.

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

> **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.

     > **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.

Create confidential VMs using Web 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 Web 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

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

healthy way. This monitoring is called **Boot Integrity Monitoring**. For more information on Boot Integrity Monitoring, see Boot integrity monitoring overview.

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

Required permissions:

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 installed. (link to the content below)
2. Create an MCS machine catalog using the machine profile input using the Web Studio 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 installed Create a VM or template spec as a machine profile input with integrity monitoring enabled, which implies GuestAttestation extension is installed.

To create a VM with integrity monitoring enabled, do the following:

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

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:

- 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

Azure Marketplace

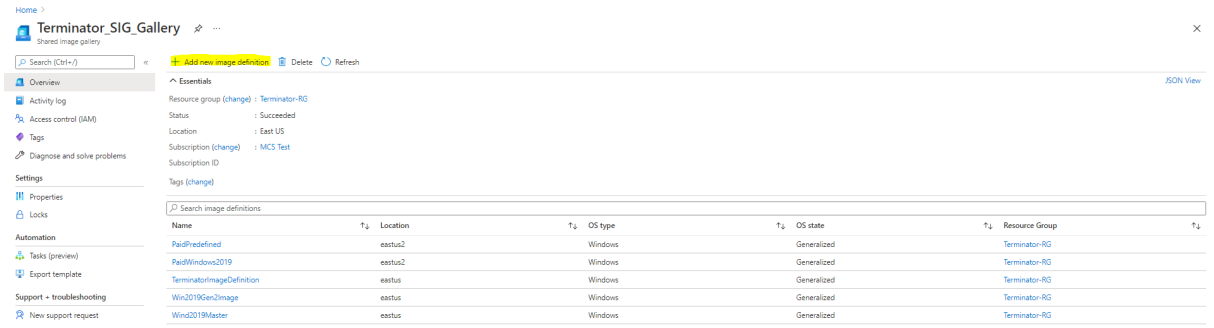
Citrix Virtual Apps and Desktops supports using a master image on Azure that contains plan information to create a machine catalog. For more information, see Microsoft Azure Marketplace.

> **Tip:**
>
> Some images found on the Azure Marketplace, like the standard Windows Server image, do not append plan information. Citrix Virtual Apps and Desktops feature is for paid images.

Ensure that the image created in Shared Image Gallery contains Azure plan information

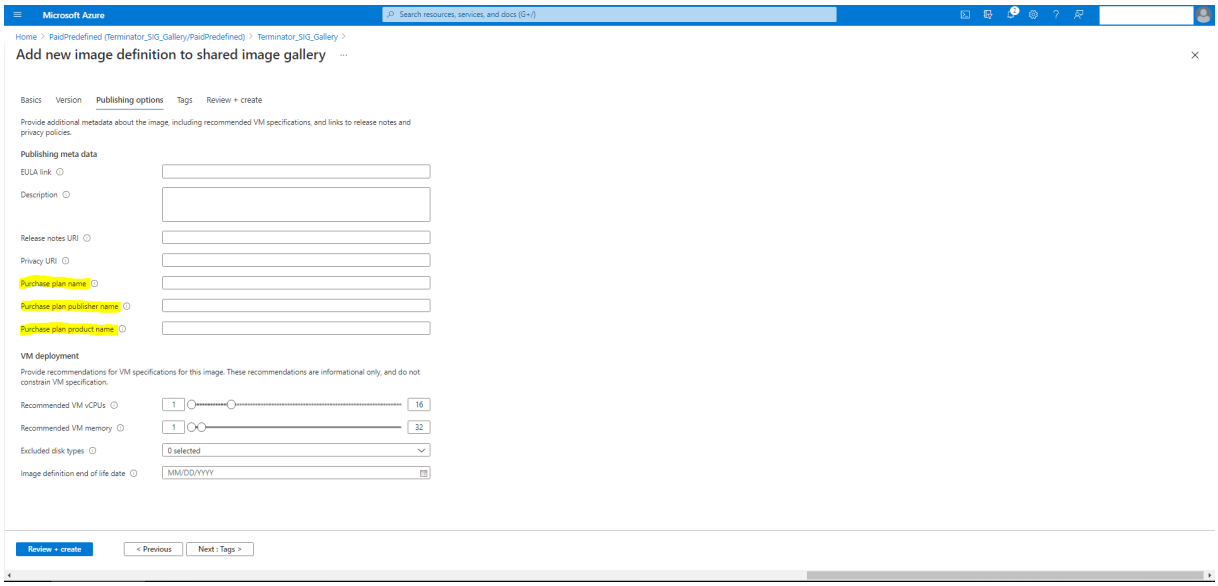
Use the procedure in this section to view Shared Image Gallery images in Web Studio. These images can optionally be used for a master image. To put the image into a Shared Image Gallery, create an image definition in a gallery.

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



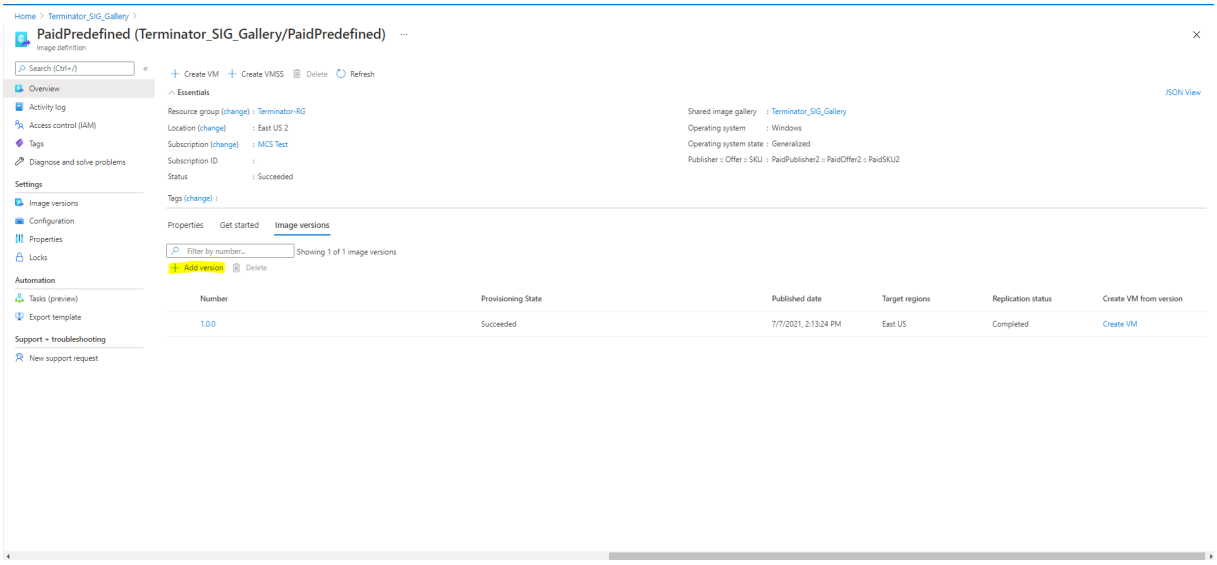
In the **Publishing options** page, verify the purchase plan information.

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.

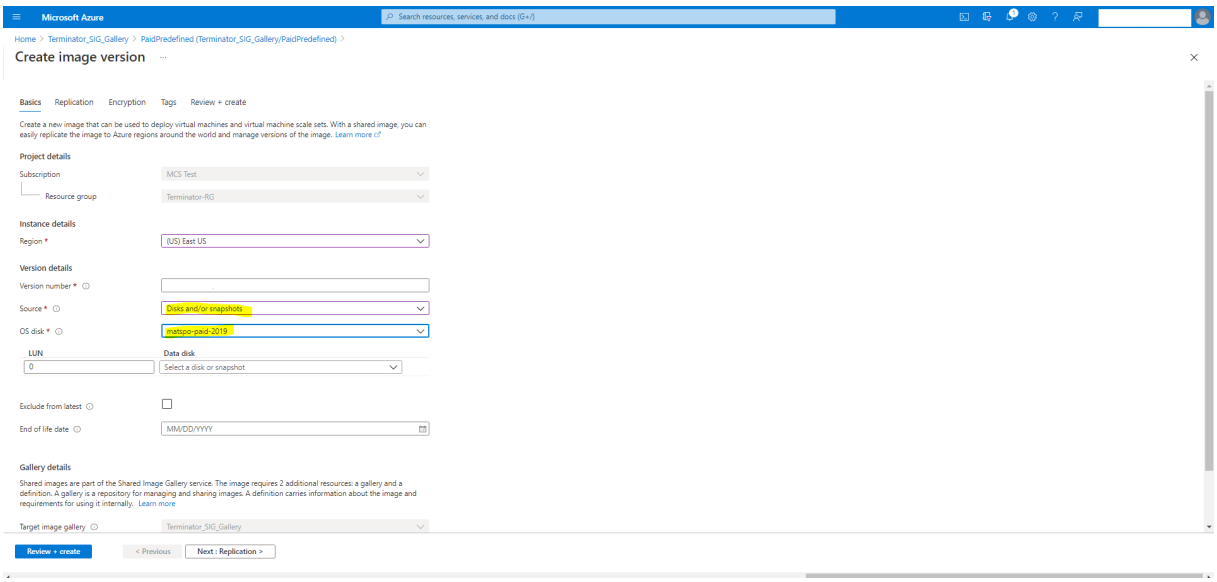


After verifying the purchase plan information, create an image version within the definition. This is used as the master image. Click **Add version**:

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



In the **Version details** section, select the image snapshot or managed disk as the source:



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.

This feature is applicable to persistent and non-persistent machine catalogs.

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

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.

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 Web Studio or PowerShell commands.

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 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.

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

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.

   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`.

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

- 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.
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.

Create a machine catalog using PowerShell

This section details how you can create catalogs using PowerShell:

- Create a catalog with non-persistent write-back cache disk
- Create a catalog with persistent write-back cache disk
- Improve boot performance with MCSIO

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

- Use template spec in creating or updating a catalog using PowerShell
- Machine catalogs with Trusted Launch
- Use machine profile property values
- Create a machine catalog with customer-managed encryption key
- Create a machine catalog with double encryption
- Create a catalog with an Azure ephemeral disks
- Azure dedicated hosts
- Create or update a machine catalog using an Azure Compute Gallery image
- Configure Shared Image Gallery
- Provision machines into specified Availability Zones
- Storage types
- Create a catalog using Azure Spot VMs
- Configure backup VM sizes
- Copy tags on all resources
- Provision catalog VMs with Azure Monitor Agent installed

Create a 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 property `UseTempDiskForWBC` 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"/> `
</CustomProperties>'
```

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

> **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 catalog with persistent write-back cache disk

To configure a catalog with persistent write-back cache disk, use the PowerShell parameter `New-ProvScheme CustomProperties`. 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.

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" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
</CustomProperties>
```

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 Virtual Apps and Desktops administrator shuts down the machine using Web Studio.

Setting the `PersistWBC` property to **false** deletes the write-back cache disk when the Citrix Virtual Apps and Desktops administrator shuts down the machine using Web Studio.

> **Note:**
>
> If the `PersistWBC` property is omitted, the property defaults to **false** and the write-back cache is deleted when the machine is shutdown using Web Studio.

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">
```

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

```
<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>
```

> **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\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-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

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

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 ``````<!--NeedCopy-->
````````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`" 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\W10MCSIO-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualprivatecloud\adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

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 the Web Studio or PowerShell commands.

For Web Studio, see Create a machine catalog using an Azure Resource Manager image in Web Stu-

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

dio

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>
[-LoggingId <Guid>]
[-BearerToken <String>][-AdminAddress <String>]
[<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]
[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
    String>] [<CommonParameters>]
```

Machine catalogs with Trusted Launch

To successfully create a machine catalog with Trusted Launch, use:

- 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

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

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 Virtual Apps and Desktops 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
```

Following are the 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.
- *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.

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

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 the Web Studio or PowerShell commands.
   - If you want to use Web Studio, see Create a machine catalog using an Azure Resource Manager image in Web 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. For the complete list of commands to create a catalog, see Creating a catalog.

     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>\<machine profile vm.vm>"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
```

     Example of `New-ProvScheme` with template spec as machine profile input:

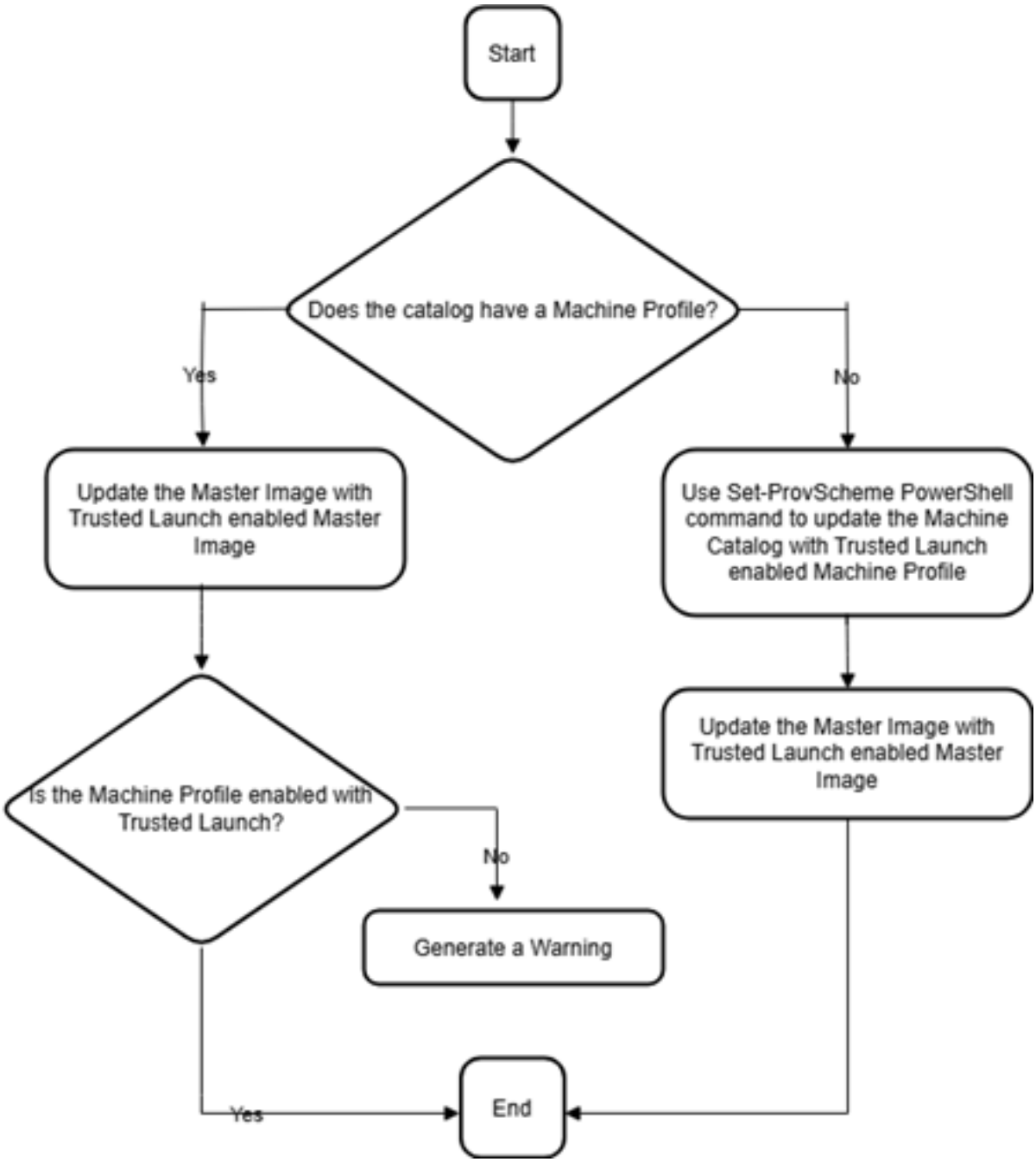
```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    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:

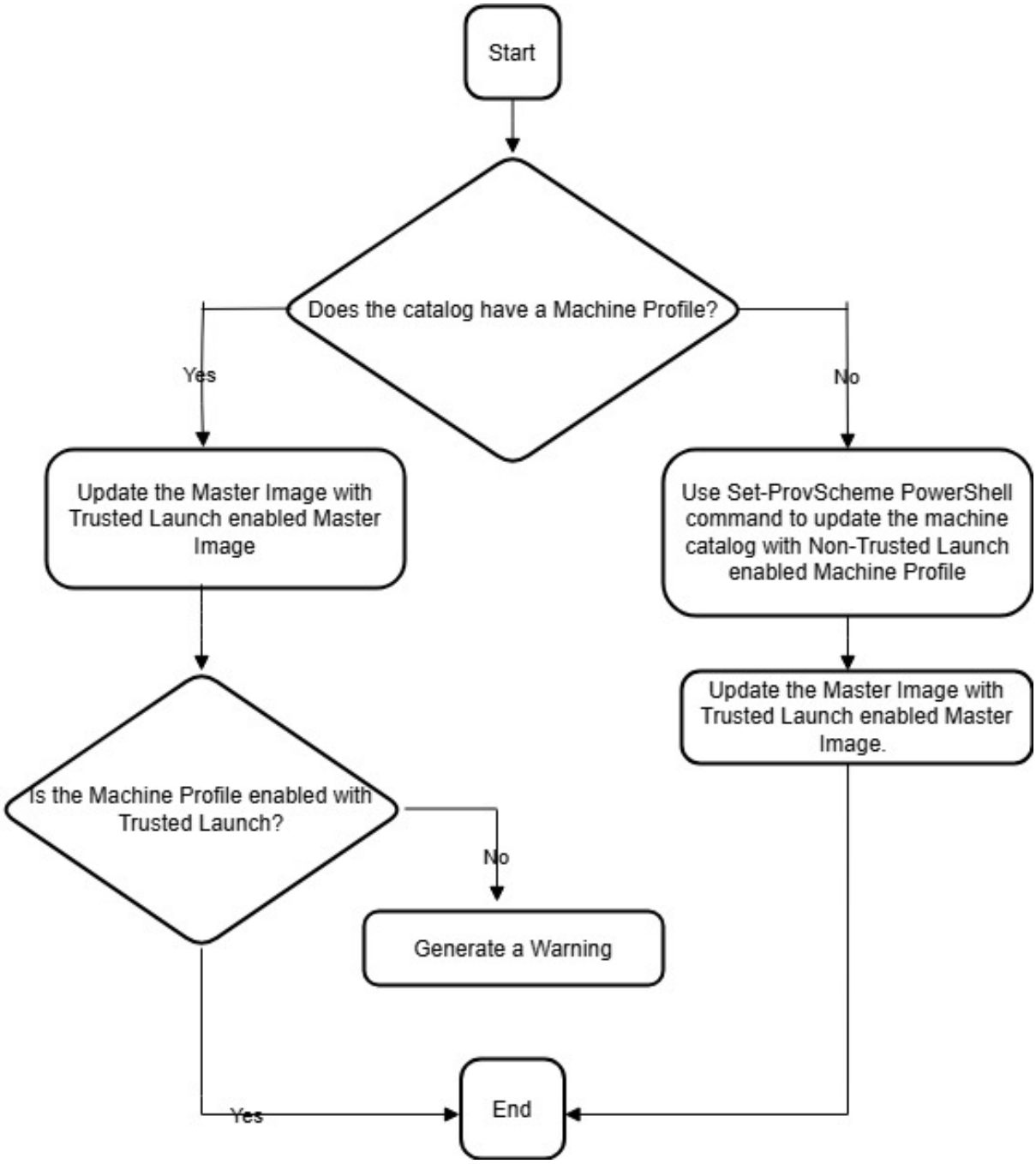
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For persistent machine catalog:



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:

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

Scenario	Error
If you select a machine profile while creating an unmanaged catalog	`MachineProfileNotSupportedForUnmanagedCata`
If you do not select a machine profile while creating a managed catalog with a master image source with Trusted Launch as the security type	`MachineProfileNotFoundForTrustedLaunchMaste`
If you select a machine profile with a security type different from the security type of the master image	`SecurityTypeConflictBetweenMasterImageAndMa`
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/
     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
  ```

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

```
<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>"/>
</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

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mp.vm"
```

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

```
-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.

```
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

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

```
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" 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>
```

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
- 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.

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

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:

   - 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.

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

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:
        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.

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 Required Azure permissions and the following permissions to use Azure Monitor:

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

  - `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 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 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 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 PoSH 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.

To 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 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.

     > **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:

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

```
{

"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
 }

 }
 ,
 {

    "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>"
      }

     }
```

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 the Web Studio.
     b) Proceed with the next steps to create the catalog.

   - To update an existing MCS catalog, use the following PoSH commands:

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

- To have the new VMs get the updated machine profile template, run the following command:

```
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:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-
   catalog -StartsNow -DurationInMinutes -1
```

3. Power on catalog VMs.
4. Go to 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 machine catalog with customer-managed encryption key

The detailed steps on how to create a machine catalog with customer-managed encryption key are:

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:

© 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=`"StorageAccountType`"
    Value=`"Standard_LRS`" />
<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
-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>\<machine profile vm.vm>"
-CustomProperties $customProperties
```

11. Finish creating the machine catalog.

Create a machine catalog with double encryption

You can create and update a machine catalog with double encryption using Web Studio and PowerShell commands.

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

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

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 DiskEncryptionSets 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 Web Studio, do one of the following in addition to the steps in Create machine catalogs.
     - If you do not use 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 menu. Continue creating the catalog.
     - If using machine profile workflow, on the **Image** page, select a master 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 you selected.
   - If using PowerShell commands, do one of the following:

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

- 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"
```

- 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
```

5. Finish creating a catalog using remote PowerShell SDK. For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. All machines created in the catalog are double encrypted by the key associated with the DES you selected.

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

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/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 the Web Studio:
  1. Navigate to **Machine Catalogs**.
  2. Select the catalog you want to verify. Click the **Template Properties** tab located near the bottom of the screen.
  3. 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.
  4. 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 PowerShell command:
  1. Open the **PowerShell** window.
  2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
  3. Use `Get-ProvScheme` to get the information of your machine catalog. For example:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

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

4. Retrieve the DES Id custom property of the machine catalog. For example:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions
   /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
   -RG/providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
```

5. In the Azure Portal, verify that the encryption type of the DES associated with the DES Id is platform-managed and customer-managed keys.

Create a catalog with an Azure ephemeral disks

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"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
 ,
            {

```

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

```
                    "Name": "SharedImageGalleryReplicaMaximum",
                    "Value": "10"
                }
    ,
                {

                    "Name": "LicenseType",
                    "Value": "Windows_Server"
                }
    ,
                {

                    "Name": "UseEphemeralOsDisk",
                    "Value": "true"
                }

            ],
```

Configure an ephemeral disk for a catalog

To configure an Azure ephemeral OS disk for a 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`.

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>'
```

Important considerations for ephemeral disks

To provision ephemeral OS disks using `New-ProvScheme`, consider the following constraints:

- The VM size used for the catalog must support ephemeral OS disks.

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

- 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 issues when:

- Creating the provisioning scheme.
- Modifying the provisioning scheme.
- Updating the image.

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:

```
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.

Create or update a machine catalog using an Azure Compute Gallery image

When selecting an image to use for creating a machine catalog, you can select images you created in the Azure Compute Gallery.

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

For these images to appear, you must:

1. Configure a Citrix Virtual Apps and Desktops site.
2. Connect to the Azure Resource Manager.
3. In the Azure portal, create a resource group. For details, see Create an Azure Compute Gallery using the portal.
4. In the resource group, create an Azure Compute Gallery.
5. In the Azure Compute Gallery, create an image definition.
6. In the image definition, create an image version.

Use the following PowerShell commands to create or update a machine catalog using an image from Azure Compute Gallery:

1. Open a PowerShell window.
2. Run `asnp citrix*` to load the Citrix-specific PowerShell modules.
3. Select a resource group, and then list all galleries of that resource group.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup")
```

4. Select a gallery, and then list all image definitions of that gallery.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery")
```

5. Select one image definition, and then list all image versions of that image definition.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery\sigtestimage.
    imagedefinition")
```

6. Create and update an MCS catalog using the following elements:

   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

   For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

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

Configure Shared Image Gallery

Use the `New-ProvScheme` command to create a provisioning scheme with Shared Image 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 Shared Image Gallery feature:

`UseSharedImageGallery`

- Defines whether to use the Shared Image Gallery to store the published images. If set to **True**, the image is stored as a Shared Image 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**.

`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.
- If the property is not defined, the default value is 100.
- If the property is not defined, the default value is 100.

> **Tip:**
>
> When using Shared Image 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 Shared Image Gallery replica ratio and replica max

The existing machine catalog uses Shared Image Gallery. Use the `Set-ProvScheme` command to update the custom properties for all existing machines in the catalog and any future machines:

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

```
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>'
```

Use Case: Converting a snapshot catalog to a Shared Image 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 Shared Image 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 Shared Image 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 a Shared Image 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 a Shared Image 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 Shared Image 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 Shared Image Gallery assets (gallery, image, and version) are automatically cleaned up within a few hours.

Provision machines into specified Availability Zones

You can provision machines into specific Availability Zones in Azure environments. You can achieve that using the 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.

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

Configure Availability Zones through PowerShell

Using PowerShell, you can view the 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
```

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.

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.

> **Tip:**
>
> `StorageType` is configured for an OS type and storage account. `WBCDiskStorageType`

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

> 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

To configure storage types for VM, use the `StorageType` parameter in `New-ProvScheme`. Set the value of the `StorageType` parameter to one of the supported storage types.

The following is an example set of the `CustomProperties` parameter in a provisioning scheme:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
     Windows_Client" />
5 </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 `-StartsNow` and `-DurationInMinutes -1` parameters, and you can change existing machine from LRS to ZRS storage.

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.

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

- 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
- **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.

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

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

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 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.

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

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.

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 NIC(s).
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",
   ```

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

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.

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 I/O 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.
- 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.

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

> 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_9473d7c8a6174b2c8284c7d3efeea88f.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"/> `
<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`

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

- `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" />
<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 IO driver automatically redirects the page file to a correct disk drive and not `C:`.

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.

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

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).
   - For creating a VM using 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.

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

> - Maximum price is the price 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:

   ```
   (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:

  1. Find the VM in the Azure Portal.

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

2. Go to the **Overview** page.
3. 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.

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 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 falls back on the backup VM sizes. You can provide a list of backup VM sizes using a custom property `BackupVmConfiguration` while creating or updating an MCS machine catalog. MCS tries to fall back on the backup VM sizes in the order that is provided by you in the list.

When MCS uses a particular backup configuration for the VM, it continues to use that configuration until the next shutdown. On the next power-on, MCS tries to boot the primary VM configuration. In case of failure, MCS again tries to boot a backup VM size configuration as per the list.

This feature is supported for:

- a catalog that uses a machine profile
- persistent and non-persistent MCS machine catalogs
- Azure environments currently

Important considerations

- You can provide more than one backup VM size in the list.
- The list must be unique.
- You can add the instance type property for each of the VMs in the list. The type is either **Spot** or **Regular**. If the type is not specified, then MCS considers the VM to be **Regular**.
- You can change the backup VM size list of an existing catalog using the `Set-ProvScheme` PowerShell commands.
- You can update the existing VMs created from the provisioning scheme associated with the catalog using `Set-ProvVMUpdateTimeWindow` command.
- 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. If the

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

`Set-ProvVm` command is used on a VM, the VM continues to use the backup VM size list set on that particular VM even if the list on the provisioning scheme is later updated. You can use `Set-ProvVM` with `-RevertToProvSchemeConfiguration` to make the VM use the backup list on the provisioning scheme.

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`

> **Note:**

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

> `StartsNow` indicates the scheduled start time. `DurationInMinutes` is the schedule's time window.

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:

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.

```
1   "tags": {
2
3  "TagC": "Value3"
4   }
5  ,
```

> **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.

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:

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

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
```

3. Turn off the VM on which you want to apply the updates.
4. Request 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`:

```
$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" `
```

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

```
-MasterImageVM "XDHyp:\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.manageddisk" `
-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
```

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.manageddisk" `
-CustomProperties $customProperties `
-NetworkMapping $networkMapping `
-UseWriteBackCache `
-WriteBackCacheDiskSize 30
```

You can also update an existing catalog using the `Set-ProvScheme` command to update the `PersistWBC` custom property.

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

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.

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.

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

- 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>"
```

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.

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:

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

```
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:
  - 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>
```

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

Where to go next

- If this is the first catalog created, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- 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 System Center Virtual Machine Manager catalog

September 13, 2025

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.

Create a master VM

1. Install a VDA on the master VM, and select the option to optimize the desktop to improve performance.
2. Take a snapshot of the master VM to use as a backup.
3. Create virtual desktops.

MCS on SMB 3 file shares

For machine catalogs created with MCS on SMB 3 file shares for VM storage, ensure that credentials meet the following requirements. These requirements ensure that calls from the Controller's Hypervisor Communications Library (HCL) connect successfully to SMB storage:

- VMM user credentials must include full read write access to the SMB storage.

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

- Storage virtual disk operations during VM life cycle events are performed through the Hyper-V server using the VMM user credentials.

When you use SMB storage, enable the Authentication Credential Security Support Provider (CredSSP) from the Controller to individual Hyper-V machines. Use this process for VMM 2012 SP1 with Hyper-V on Windows Server 2012. For more information, see CTX137465.

The HCL uses `CredSSP` to open a connection to the Hyper-V machine. This feature passes Kerberos-encrypted user credentials to the Hyper-V machine. The **PowerShell** commands in the session on the remote Hyper-V machine run with the credentials provided. In this case, the credentials of the VMM user, so that communication commands to storage work correctly.

The following tasks use PowerShell scripts that originate in the HCL and are then sent to the Hyper-V machine to act on the SMB 3.0 storage.

- **Consolidate master image**: A master image creates an MCS provisioning scheme (machine catalog). It clones and flattens the master VM ready for creating VMs from the new disk created (and removes dependency on the original master VM).

  ConvertVirtualHardDisk on the root\virtualization\v2 namespace

  Example:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2
    ";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
```

- **Create difference disk:** Creates a difference disk from the master image generated by consolidating the master image. The difference 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 Controller, 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

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

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 finishes uploading the identity disk to the Hyper-V machine, the remote PowerShell session copies the identity disks to SMB storage. It then deletes it from the Hyper-V machine.

The identity disk folder is recreated if it is deleted so that it is available for reuse.

- **Download identity disks:** As with uploads, the identity disks pass though the Hyper-V machine to the HCL. The following process creates a folder that only has VMM user permissions on the Hyper-V server if it does not exist.

1. The Hyper-V machine copies the disk from the SMB storage to the local Hyper-V storage through a PowerShell script. This script runs 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.
- You can configure VTPM from the Hyper-V console and not from the SCVMM console.
- 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

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

- 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)` -PersonalvDiskStoragePath
 @()` -RootPath $RootPath ` -StoragePath @($StoragePath)` -
NoVmTagging
```

- You can update an existing catalog using the `Set-ProvScheme` command.
- You can update the memory and disk cache sizes after creating the MCS catalogs when MCSIO is enabled.

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.
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:

```
1 New-ProvScheme -HostingUnitName "<hostingunit name>"
2 -IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<
     path to the checkpoint/snapshot>"
3 -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.

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

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 Web studio or PowerShell commands.

Remove a VM using Web 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
- Delete machines without hypervisor access

Where to go next

- If this is the first catalog created, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- 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

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

Create a Nutanix catalog

January 16, 2026

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

Limitations

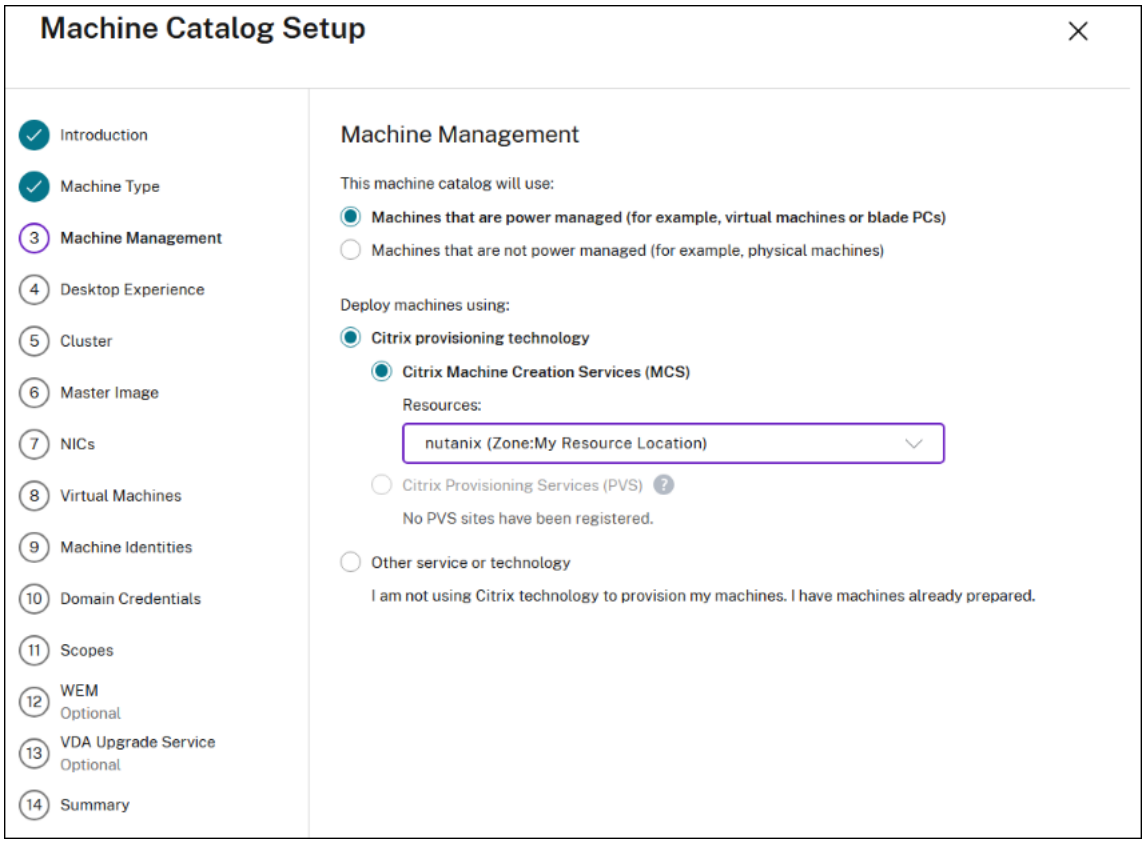
- Attaching multiple NICs to the same subnet is not supported.
- Categories are not inherited from the Nutanix template version used as the MCS master image.
- Due to Nutanix limitation, each MCS provisioned machine catalog can only be assigned with NICs in a single type of network among Overlay networks, 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 **&**.

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

Create a machine catalog using Studio

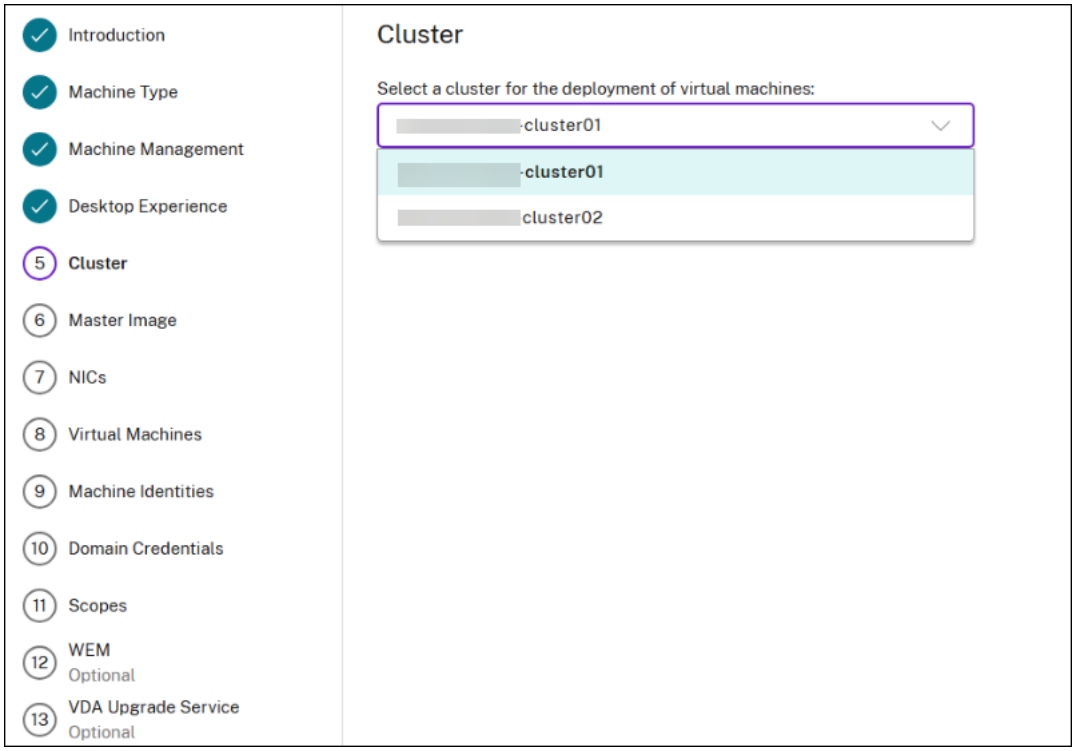
In the Machine Catalog Setup wizard:

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**.



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.

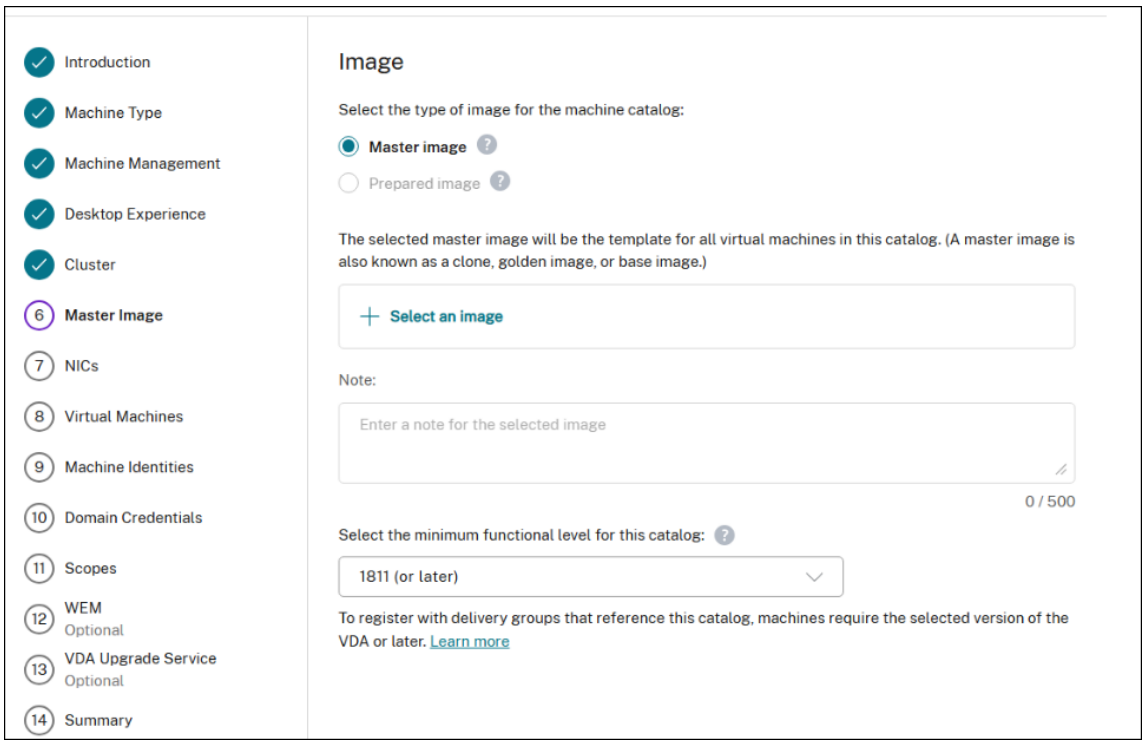
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. On the **Master Image** page, click **Select an Image** and select a master image (template version). You can filter machine templates by name.

> **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.

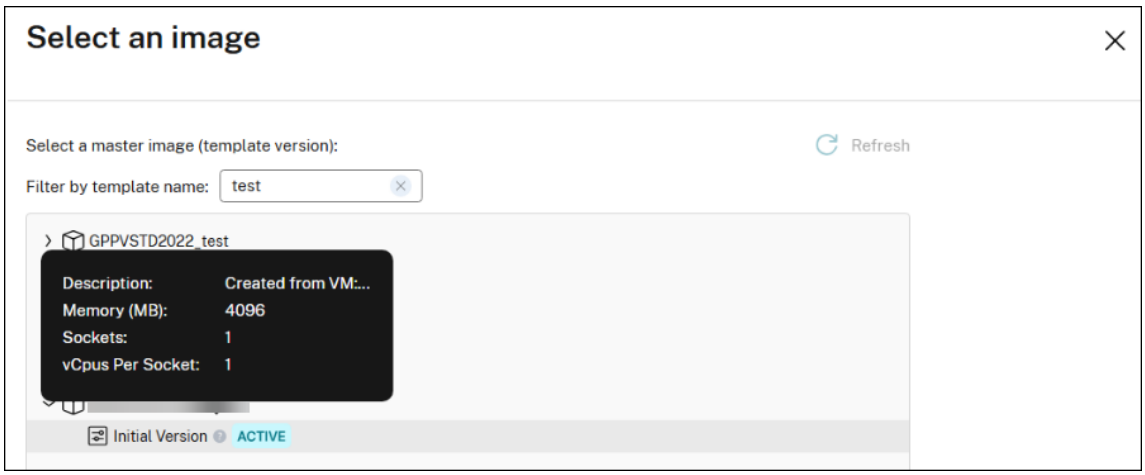
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Filter machine templates by name:

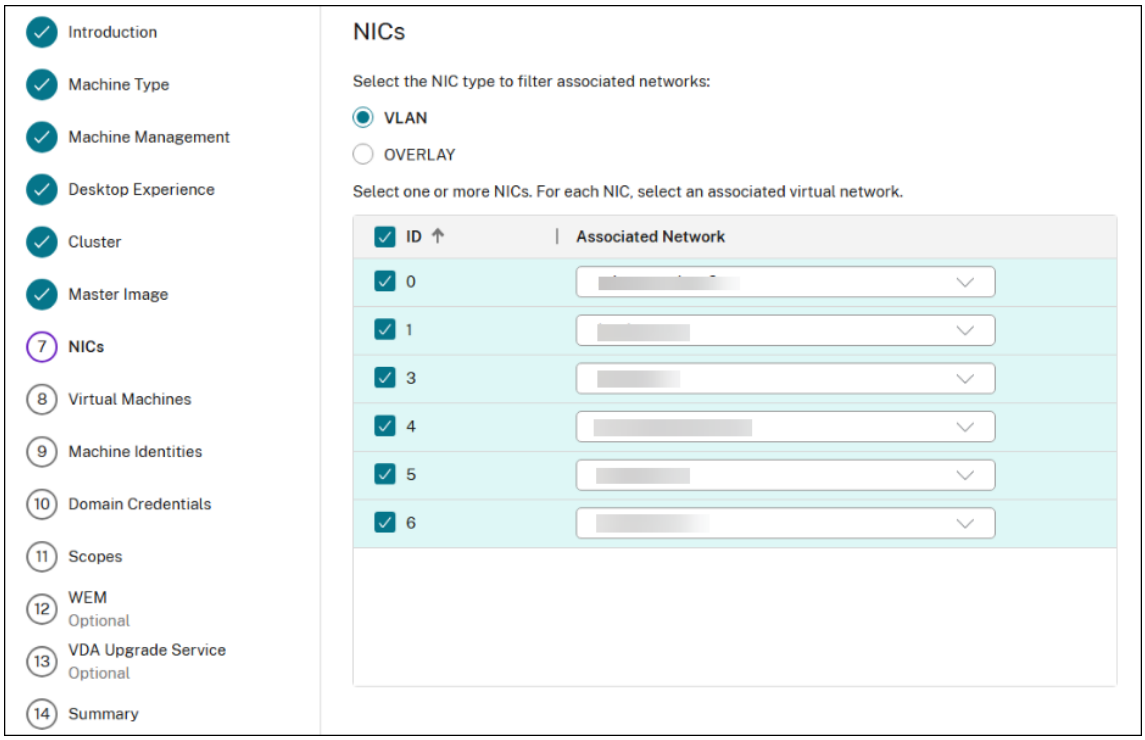
See description of a template:

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



6. On the **NICs** page:

   - Select the NIC type to filter associated networks.
   - Select one or more NICs that the master image contains and then select an associated virtual network for each NIC.



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.

8. 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.

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:

```
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
```

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"    -
    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:

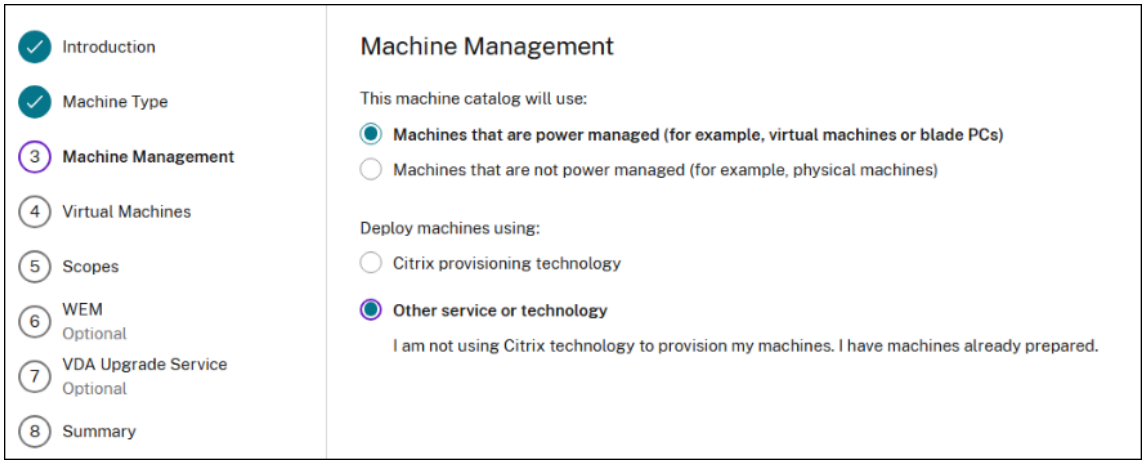
- Studio
- PowerShell

Create a machine catalog with existing machines (power managed) using Studio

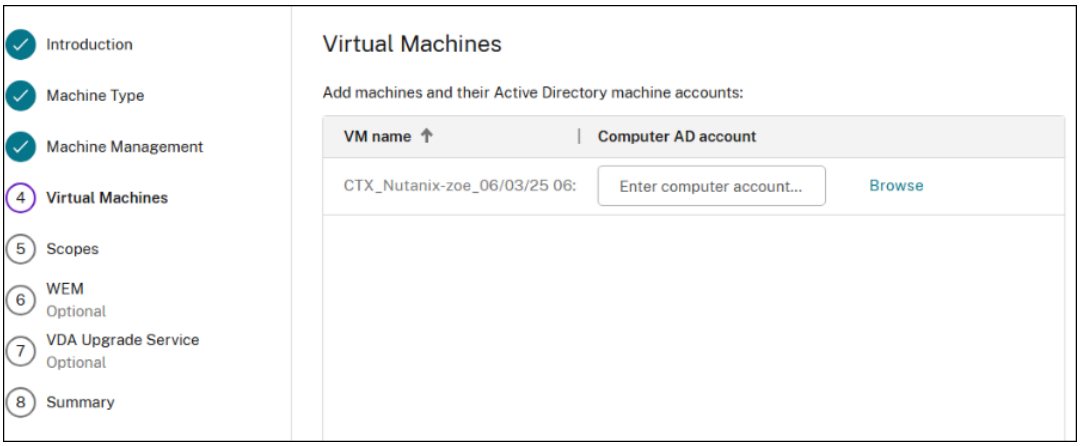
In the Machine Catalog Setup wizard:

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

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.
   - 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.



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.

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

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 "fb202053-8c35-4
    db2-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.
  - 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.

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

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, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- 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

Create a Red Hat OpenShift catalog

September 6, 2025

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.

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

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.

Create a catalog

You can create OpenShift catalogs to create, deliver, and power manage machines in your OpenShift environments.

- Create a catalog using Web Studio
- Create a catalog using PowerShell commands

Create a catalog using Web 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)**.

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

- 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.
   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.

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

4. Follow the on-screen instructions to complete the remaining steps, which don't include OpenShift-specific information.

Create a catalog using PowerShell commands

You can create an MCS machine catalog in the Red Hat OpenShift environment using 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
    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"
```

Create a provisioning scheme with persistent machines (without machine profile)

```
New-ProvScheme `
    -ProvisioningSchemeName "ProvisioningSchemeName" `
    -HostingUnitName "HostingUnitName" `
    -IdentityPoolName "IdentityPoolName" `
    -ProvisioningSchemeType "MCS" `
```

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

```
    -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:\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.vm"
```

Create new ProvVMs

```
New-ProvVM `
    ProvisioningSchemeName "ProvisioningSchemeName" `
    ADAccountName "MyDomain\vm001" `
    AdminAddress "MyDDC.MyDomain.Local"

Lock-ProvVM `
    -ProvisioningSchemeName "ProvisioningSchemeName" `
    -Tag "Brokered" `
    -VMID "TargetNamespace:vm001"
```

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"
```

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

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" `
    -MachineName "S-0-0-00-0000000000-0000000000-000000000-000000"
```

Where to go next

- If this is the first catalog created, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- For power management, see Power manage Red Hat OpenShift VMs

More information

- Create and manage connections and resources
- Connection to Red Hat OpenShift
- Create machine catalogs

Create a VMware catalog

September 13, 2025

Create machine catalogs describes the wizards that create a machine catalog. The following information covers details specific to VMware virtualization environments.

> **Note:**
>
> Before creating a VMware catalog, you need to finish creating a connection to VMware. See Connection to VMware.

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

Create a master VM

Use a master VM to provide user desktops and applications in a machine catalog. On your hypervisor:

1. Install a VDA on the master VM, selecting the option to optimize the desktop, which improves performance.
2. Take a snapshot of the master VM to use as a back-up.

> **Note:**
>
> You can use MCS to provision VMs in vSAN 8.0 environment.

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.

> **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 properties of a VMware template. You can create new a VMware template referencing stored properties of 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.

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

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:

1. Open a **PowerShell** window.
2. Run `asnp citrix*`.
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
-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
```

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

```
-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>"
-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 @()
-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.

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

- 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 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, NetworkMapping count should be same as the machine profile NIC count).
  - Multiple NICs cannot be mapped to the same network in the hosting unit.
  - `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.

Troubleshooting

If the catalog fails to create, see CTX294978.

Where to go next

- If this is the first catalog created, Web Studio guides you to create a delivery group
- To review the entire configuration process, see Install and configure
- To manage catalogs, see Manage machine catalogs and Manage a VMware catalog

More information

- Create and manage connections and resources
- Connection to VMware
- Create machine catalogs

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

Identity pools of different machine identity join types

September 6, 2025

Using MCS, you can provision machines as on-premises AD joined, hybrid Azure AD joined, or non-domain-joined.

For information about how to configure machine identities in the Web 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 Hybrid Azure Active Directory joined machine identity
- Identity pool of non-domain-joined machine identity

Identity pool of on-premises Active Directory joined machine identity

May 5, 2025

This article describes how to create identity pool of on-premises Active Directory joined machine identity.

Use Web Studio

The following information is a supplement to the guidance in Create machine catalogs.

1. On the **Machine Identities** page:
    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.
            - 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.

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

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:

```
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.

Identity pool of Microsoft Entra hybrid joined machine identity

April 2, 2026

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

This article describes how to create identity pool of:

Microsoft Entra hybrid joined catalogs
Microsoft Entra hybrid joined catalogs enrolled in Microsoft Intune

For information on requirements, limitations, and considerations, see Microsoft Entra hybrid joined.

Create Microsoft Entra hybrid joined catalogs

Use Web Studio

The following information is a supplement to the guidance in Create machine catalogs.

On the **Machine Identities** page of the catalog creation wizard:

- Select **Microsoft Entra hybrid joined**. The created machines are owned by an organization and are signed into with an Active Directory account that belongs to that organization.
- To enroll the created machines into Microsoft Intune (including Configuration Manager) for device management, select **Enroll the machines in Microsoft Intune with Configuration Manager**. To avoid errors during catalog creation, ensure that the master image meets the following requirements:
  - Has VDA version 2405 or later installed.
  - Has the **Configuration Manager client** installed with the site code unassigned. For more information, see this Microsoft article.

> **Note:**
>
> If you select **Microsoft Entra hybrid joined** as the identity type, each machine in the catalog must have a corresponding AD computer account.

Use PowerShell

The following are PowerShell steps equivalent to operations in Web Studio. For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

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.

To create an identity pool along with the accounts for Microsoft Entra hybrid joined catalogs:

© 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-d2f2-49
    d2-ab12-bae5bbd0df05"
New-AcctIdentity -IdentityPoolName "HybridAADJoinedCatalog" -Count 10 -
    ADUserName "corp\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
```

> **Note:**
>
> `$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.

View the status of the Microsoft Entra hybrid join process

In the Web Studio, the status of the Microsoft Entra hybrid 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

> **Note:**
>
> - You might experience delayed Microsoft Entra hybrid 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 the Web 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:

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

- Check if the machine account has been synced to Microsoft Entra ID through the Microsoft Microsoft Entra ID portal. If synced, **Not yet joined to Azure AD** 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 Microsoft Entra hybrid join is correctly pushed to the machine by querying the value of **DeviceKeyPairRestored** under **HKEY_LOCAL_MACHINE\SYSTEM\Cur**

  Verify that the value is 1. If not, possible reasons are:

  - `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 Microsoft Entra hybrid join.

- Check diagnostic messages by running the `dsregcmd /status /debug` command on the MCS-provisioned machine.

  - If Microsoft Entra hybrid 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:

    ```
    1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
          UserCertificate
    ```

    For more information about the user certificate issue, see CTX566696.

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

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 Web Studio and PowerShell.

Use Web 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.

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.

The difference between Microsoft Entra hybrid joined catalogs and co-management enabled ones lies in the creation of the identity pool. For example:

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "
    IntuneWithSCCM" IdentityType="HybridAzureAD" -IdentityPoolName "
    CoManagedCatalog" -NamingScheme "CoManaged-VM-##" -NamingSchemeType
    "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

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 Microsoft Entra hybrid join status

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

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 Microsoft Entra hybrid 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()
    ```

  - 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.

Identity pool of non-domain-joined machine identity

September 13, 2025

This article describes how to create identity pool of non-domain-joined catalogs using Citrix Virtual Apps and Desktops.

For information on requirements, limitations, and considerations, see Non-domain-joined.

Before you create the machine catalog, you need the following:

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

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**.
2. Create a hosting connection. See Create and manage connections section for details.

Using Citrix Virtual Apps and Desktops, you can create catalogs based on workgroups or 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.

Use Web 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 **Non-domain-joined**. The created machines are not joined to any domain.

> **Note:**
>
> The **Non-domain-joined** identity type requires version 2311 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

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"
```

All other commands used to create non-domain-joined catalogs are the same as for the traditional on-premises Active Directory joined catalogs.

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

Manage machine catalogs

September 13, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Introduction

You can add or remove machines from a machine catalog, rename, change the description, or manage a catalog's Active Directory computer accounts.

Maintaining catalogs can also include making sure that each machine has the latest OS updates. Including antivirus updates, operating system upgrades, or configuration changes.

- Catalogs containing pooled random machines created using Machine Creation Services™ (MCS) maintain machines by updating the master image used in the catalog and then updating the machines. This method enables you to efficiently update large numbers of user machines.
- For catalogs containing static, permanently assigned machines, and for Remote PC Access Machine catalogs, you manage updates to users' machines outside of Web Studio. Perform this task either individually or collectively using third-party software distribution tools.

For information about creating and managing connections to host hypervisors, see 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.

About persistent instances

When updating an MCS catalog created using persistent, or dedicated instances, any new machines created for the catalog use the updated image. Pre-existing instances continue to use the original instance. 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.

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

- For non-persistent disk catalogs, the machine image is updated the next time the machine is reset.
- With persistent machine catalogs, updating the image also updates the catalog instances that use it.
- 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 Web Studio
- Using PowerShell

Use Web Studio

This section details how you can manage catalogs using Web Studio:

- Manage machine catalogs
  - Introduction
  - About persistent instances
- Manage machine catalogs
- Use Web Studio
- View catalog details
  - Add machines to a catalog
  - Delete machines from a catalog
- Edit a catalog
- Rename a catalog
- Move a catalog to a different zone
- Delete a catalog
- Convert legacy MCS catalogs in Azure to machine profile-based catalogs
- Manage Active Directory computer accounts in a catalog
- Update a catalog
  - Update or create a master image
  - Change the master image
  - Roll back the master image
- Change the functional level or undo the change

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

- Clone a catalog
- Organize catalogs using folders
  - Create a catalog folder
  - Move a catalog
  - Manage catalog folders
- Upgrade VDAs
- Retry catalog creation
- Enroll non-MCS provisioned VDAs using tokens
- Use PowerShell
- Retrieve warnings and errors associated with a catalog
- Add descriptions to an image
- Reset OS disk
- Change the network setting for an existing provisioning scheme
- Manage versions of a machine catalog
- Convert a non-machine profile-based machine catalog to machine profile-based machine catalog
- Repair the identity information of active computer accounts
  - Conditions
  - Reset identity disk
- Change cache configuration on an existing machine catalog
  - Requirements
  - Change the cache configuration
- VDA Update Support via Local File Share Access
  - PowerShell cmdlets
  - Prerequisites
  - How to Set File Share Permissions
  - VDA Updates from a Local File Share
- Troubleshoot
- Where to go next

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.

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

4. Click a tab in the bottom details pane for more information about this catalog.

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
Machine Count	The machine count in the catalog and the 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 image update status of the catalog. Applicable only to non-persistent machine catalogs. Possible values include: Fully updated, Partially updated, Pending updates, Preparing

Add machines to a catalog

Before you start:

- Make sure that the virtualization host has sufficient processors, memory, and storage to accom-

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

modate 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 Web Studio to create Active Directory computer accounts for the additional machines, you must have appropriate domain administrator permission.

To add machines to a catalog:

1. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.
3. Select a machine catalog and then select **Add machines** in the action bar.
4. Select the number of virtual machines to add.
5. 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. Specify an account naming scheme, using hash marks to indicate where sequential numbers or letters appear. Do not use a forward slash (/) in an OU name. A name cannot begin with a number. 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.
6. If you use existing Active Directory accounts, either browse to the accounts or click **Import** and specify a .csv file containing account names. Make sure that there are enough accounts for all the machines you're adding. Web Studio manages these accounts. Either allow Web Studio to reset the passwords for all the accounts, or specify the account password, which must be the same for all 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 Web Studio.

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. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.

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

3. Select a catalog and then select **View Machines** in the action bar.
4. Select one or more machines and then select **Delete** in the action bar.

Choose whether to delete the machines being removed. If you choose to delete the machines, indicate if the Active Directory accounts for those machines are kept, disabled, or deleted.

Edit a catalog

1. On the **Description** page, change the catalog description.
2. Select **Machine Catalogs** in the left pane.
3. Select a catalog and then select **Edit Machine Catalog** in the action bar.
4. On the **Scopes** page, change the scopes.
5. 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 case of Nutanix hypervisors.

6. You might see other pages depending on the catalog type.

   For catalogs created using an Azure Resource Manager image, the following pages are visible. Keep in mind that 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.

- On the **Machine Profile** page, choose whether to use or change a machine profile.
- (Visible 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 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.

- On the **License Type** page, choose whether to change the Windows license or Linux license setting.

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.
- On the **Organizational Units** page, add or remove Active Directory OUs.

7. Click **Apply** to apply the changes you made and click **Save** to exit.

Rename a catalog

1. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.
3. Select a catalog and then select **Rename Machine Catalog** in the action bar.
4. Enter the new name.

Move a catalog to a different zone

If your deployment has more than one zone, you can move a catalog from one zone to another.

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

Moving a catalog to a different zone, other than the hypervisor containing the VMs in that catalog, affects performance.

1. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.
3. Select a catalog and then select **Move** in the action bar.
4. Select the zone where you want to move the catalog.

Delete a catalog

Before deleting a catalog, ensure that:

- All users are logged off and you don't run any disconnected sessions.
- 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 a delivery group. In other words, the delivery group does not contain machines from the catalog.

To delete a catalog:

1. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.
3. Select a catalog and then select **Delete Machine Catalog** in the action bar.
4. Indicate whether the machines in the catalog are deleted. If you choose to delete the machines, indicate whether the Active Directory computer accounts for those machines are retained, disabled, or deleted.

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 Azure Active Directory)** 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 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**.

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

6. Click **Apply**.

> **Note:**
>
> Currently, this feature is supported only for Azure, AWS, and VMware.

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 OS and multi-session OS 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. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.
3. Select a catalog and then select **Manage AD accounts** in the action bar.
4. 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. When entering a password, the password is changed on the accounts as they are imported. When deleting an account, choose whether the account in Active Directory is kept, disabled, or deleted.

Indicate if Active Directory accounts are retained, disabled, or deleted when you remove machines from a catalog or delete a catalog.

Update a catalog

We recommend that you save copies or snapshots of master images before updating the machines in the catalog. The database keeps a historical record of the master images used with each machine catalog. Roll back, or revert, machines in a catalog to use the previous version of the master image. Perform this task if users encounter problems with updates you deployed to their desktops. This minimizes user downtime. Do not delete, move, or rename master images. You cannot revert a catalog to use them.

After a machine is updated, it restarts automatically.

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

Update or create a master image

Before you update the machine catalog, either update an existing master image or create one on your host hypervisor.

1. On your hypervisor, take a snapshot of the current VM and give the snapshot a meaningful name. This snapshot can be used to revert (roll back) machines in the catalog, if needed.
2. If necessary, power on the master image, and log on.
3. Install updates or make any required changes to the master image.
4. Power off the VM.
5. Take a snapshot of the VM. Give it a meaningful name that is recognized when the catalog is updated in Web Studio. Although Web Studio can create a snapshot, Citrix recommends that you create it using the hypervisor management console. Then select that snapshot in Web Studio. This process enables you to provide a meaningful name and description rather than an automatically generated name. For GPU master images, you can change the master image only through the XenServer® console.

Change the master image

To prepare and roll out the update to all machines in a catalog:

1. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.
3. Select a catalog and then select **Change Master Image** in the action bar.
4. 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**.

5. On the **Rollout Strategy** page, choose when the machines in the machine catalog are updated with the new master 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.

6. Verify the information on the **Summary** page and then click **Finish**. Each machine restarts automatically after it is updated.

To track the update progress, locate the catalog in **Machine Catalogs** to view the inline progress bar and the step-by-step progress graph.

When updating a catalog using PowerShell SDK directly, rather than Web Studio, specify a hypervisor template (**VMTemplates**). Use this as an alternative to an image or a snapshot of an image.

To roll out a new master image to Azure based machine catalog:

1. From Web 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:

Updating images 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. Consider the following:

- New sessions cannot be launched until the update has completed on applicable machines.
- For single-session OS machines, machines are immediately updated when the machine is not in use, or when users are not logged in.
- For a multi-session OS with child machines, reboots do not occur automatically. To apply the updated master image, restart the machines using Studio, PowerShell, or Workspace. Restarting from the machines or the hypervisor 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 master image, you can roll it back. This process 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. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.
3. Select the catalog and then select **Roll Back Master Image** in the action bar.

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

4. Specify when to apply the earlier master image to machines, as described in the preceding section for the rollout operation.

The rollback is applied only to machines that need to be reverted. Machines that are not updated with the new or updated master image 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.

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. Citrix recommends 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 the Controller. This process lets Web Studio determine that the machines in the catalog need upgrading.

To change the functional level for a catalog:

1. Sign in to Web Studio.
2. Select **Machine Catalogs** in the left pane.
3. Select the catalog. The **Details** tab in the lower pane displays version information.
4. Select **Change Functional Level**. If Web Studio detects that the catalog needs upgrading, it displays a message. Follow the prompts. If one or more machines cannot be upgraded, a message explains why. To ensure that all machines function properly, Citrix recommends you resolve machine issues before clicking **Change** to proceed.

After the catalog change 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:**

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

> 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.

1. Sign in to Web Studio, and then 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 in the upper right of the action bar.

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 Web 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 **Machine Catalogs** node, you must add the `ContainsMachineCatalogs` metadata using the `Set-BrokerAdminFolderMetadata` cmdlet.

  Example:

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

```
Set-BrokerAdminFolderMetadata -AdminFolderId {
adminFolderUid }
 -Name ContainsMachineCatalogs -Value true
```

To create a catalog folder, follow these steps:

1. 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. 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 the below steps:

1. 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 onscreen instructions to complete the remaining steps.

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

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.

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 Web 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.
5. After you finish, select **Finish** to start the creation.

Enroll non-MCS provisioned VDAs using tokens

You can now generate and manage enrollment tokens for non-MCS-provisioned VDAs. This implementation allows VDA registration over WebSocket without provisioning the VDAs with MCS. This feature also supports Linux Virtual Delivery Agent, Citrix Virtual Delivery Agent for macOS, and non-domain joined VDAs with Citrix Virtual Apps and Desktops.

Before you begin

1. Configure your site. For more information, see Create a site.

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

2. Install TLS certificates on the Delivery Controllers. For more information, see Install TLS server certificates on Controllers.
3. Install root CA and intermediate CA on VDA to trust the Delivery Controller.
4. Enable WebSocket connection on the Delivery Controller. Run the following command on each Delivery Controller present on your site:

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
    -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -
   Force
```

> **Note:**
>
> Ensure that you restart the Delivery Controllers after enabling the WebSocket.

Generate enrollment tokens

After you decide to enable token-based enrollment for non-Citrix provisioned machines, you must first generate tokens on a per-machine catalog basis, and then share them with VDA installation administrators.

An enrollment token features:

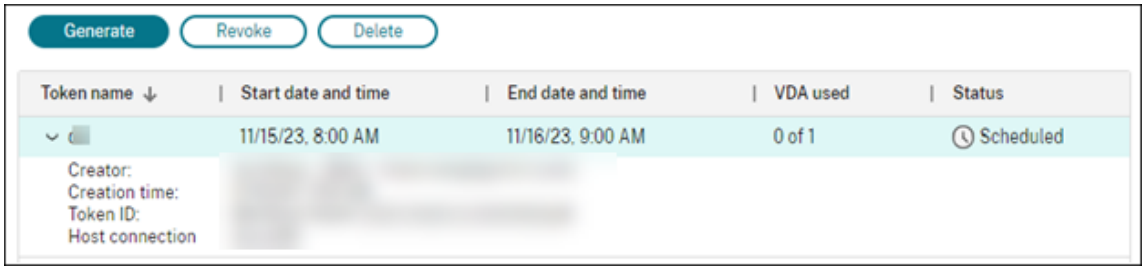
- Registration range: 1–5000 VDA machines
- Validity period: up to 14 days

To generate a token for a catalog using Web Studio, follow these steps:

1. In **Web Studio > 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.

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

A token record appears in the token list.



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.

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:

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

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
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 the Web 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:

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

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.
-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.

Use PowerShell

This section details how you can manage catalogs using PowerShell:

- Retrieve warnings and errors associated with a catalog
- Add descriptions to an image
- Reset OS disk
- Change the network setting for an existing provisioning scheme
- Manage versions of a machine catalog
- Convert a non-machine profile-based machine catalog to machine profile-based machine catalog
- Repair the identity information of active computer accounts
- Change cache configuration on an existing machine catalog
- VDA update support via local file share access

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.

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

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 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
- 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 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:

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

- 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
- 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
```

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. Use the following commands to add or view image descriptions:

- To add a note while creating a machine catalog with a master image, use the parameter `MasterImageNote` in the `NewProvScheme` command. For example:

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

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
    HostingUnitName <name> -IdentityPoolName <name> -MasterImageVM
XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.
    snapshot -MasterImageNote "Note"
```

- To update the master image associated with a machine catalog, use the parameter `MasterImageNote` in the `Publish-ProvMasterVMImage` command. For example:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name> -
    MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm name
    >.vm\base.snapshot -MasterImageNote "Note"
```

- To display the information for each image, use the Get-ProvSchemeMasterVMImageHistory command. For example:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall
```

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.

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, XenServer, Google Cloud. SCVMM, and VMware 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.

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

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:

     ```
     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.

   > **Note:**
   >
   > Do not take VMs out the of the maintenance mode or power them on until the completion of the reset process.

   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
     ```

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

- Provide the `-Confirm:$false` parameter:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Confirm:$false
```

- 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
```

5. Run `Get-ProvTask` to get the status of the tasks returned by `Reset-ProvVMDisk` command.

Change the network setting for an existing provisioning scheme

You can 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.

> **Note:**
>
> This feature is supported on Citrix Virtual Apps and Desktops 2203 LTSR CU3 and later versions.

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`.
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

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

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 (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:

```
(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 (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
```

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

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.

Convert a non-machine profile-based machine catalog to machine profile-based machine catalog

You can use a VM, template spec (in case of Azure), 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 unless overwritten by explicit custom property.

> **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\<ResourceGroupName>\<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:

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

```
Set-ProvScheme -ProvisioningSchemeName "my-prov-scheme" -
    MachineProfile "XDHyp:\HostingUnits\my-hosting-unit\my-
    template.template"
```

> **Note:**
>
> Set the `FolderID` as the custom property to avoid deriving `FolderID` from the VMware template.

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 for AWS, GCP, Azure, SCVMM, XenServer, and VMware 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

Reset identity disk

To reset identity disk:

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 are as follows:

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

- IdentityAccountName: The name of the identity account that must be repaired.
- PrivilegedUserName: User account that has write permission on identity provider (AD or AzureAD).
- 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 Hybrid AzureAD 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
```

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 cache configuration on 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.

VDA Update Support via Local File Share Access

Specify the VDA installer location through PowerShell cmdlets which reduces your effort from providing network rules to allow each VDA to go and fetch the new VDA installer from the Citrix Managed Azure CDN.

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

PowerShell cmdlets

Two new optional parameters added to **New-VusCatalogSchedule** and **New-VusMachineUpgrade** cmdlets that allow you to use installers from a local file share

- **VdaWorkstationPackageUri** - to specify the UNC path to the workstation OS VDA installer
- **VdaServerPackageUri** - to specify the UNC path to the server OS VDA installer

Prerequisites

- VUS Agent Installer that comes with VDA 2311
- VDA Upgrade Agent to version 7.40.0.35 or later (using the VDA installer version 2311 or later)
- Virtual Apps and Desktops Remote PowerShell SDK version 7.40 or newer (released on Jan 10, 2024 or later)

How to Set 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 file share permission**

  When the VDA machine is domain-joined, then the **Local System** account (VUA runs as Local System), uses computer credentials when accessing network shares.

  The least privilege permission can be set by granting the **Read** access to Domain Computers.

  1. Choose people on your network who you want to share the file with.
  2. Click **Advanced Sharing Settings** and turn on **File and Printer Sharing**.

- **Non-Domain Joined file share permission**

  When the VDA machine is non-domain joined, then the **Local System** account (VUA runs as Local System), uses **ANONYMOUS LOGON** when accessing network shares.

  1. Select a shared folder.
  2. Disable the password protection.
     a) Go to Folder **Properties**.
     b) Select **Network and Sharing Center**.
     c) Turn off **Password Protected Sharing**.
  3. Click **Advanced Sharing** to grant a share permission.
     a) Select **Permissions**.
     b) Grant a **Read** share permission to **ANONYMOUS LOGON**.

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

4. Select the **Security Tab** to grant folder permissions
   a) Click **Edit** to add permissions to the shared folder
   b) Select the shared folder to grant folder permissions to **ANONYMOUS LOGON**.
5. Click **Advanced** to turn on **File and Printer Sharing**.
6. Add the shared folder name to **Network Access Security Policy**.

> **Note:**
>
> Restart your machine for the change to take effect immediately.

VDA Updates from a Local File Share

1. Download the VDA installer and place it in the shared file.

   > **Note:**
   >
   > With Virtual Upgrade Service, you can select from either the Current Release track or the LTSR track.
   >
   > **For Example:** If the machine catalog is set to Current Release that is 2311, and the VDA version is 2305, you must upgrade the VDA to version 2311.

   a) Navigate to the **Downloads** page on our website.
   b) Select **Citrix Virtual Apps and Desktops** as the product.
   c) Select **Citrix Virtual Apps and Desktops 7 2311, All Editions**.
   d) Select the VDA installer from the **Components that are on product ISO but also packaged separately** expandable.

2. Select the relevant VDA installer based on the catalog type.

   - Download the **Multi-session OS VDA installer** if the catalog type is **multi session**
   - Download the **Single-session OS VDA installer** if the catalog type is **single session**
   - Download the **Single-session OS Core Services VDA installer** if the catalog type is **Remote PC Access**

> **Note:**
>
> The version of the file share installer has to **exactly** match the version of the latest installer version published by VUS to the cloud.

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 manage-

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

ment, 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.

   > **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 *
   ```

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

- 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.

> **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.

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

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

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:
        - Web Studio
        - PowerShell
    - VMware:
        - Web Studio
        - PowerShell
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]
```

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

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.

Where to go next

For information on managing specific cloud services catalogs, see:

- Manage an AWS catalog
- Manage a XenServer catalog
- Manage a Google Cloud Platform catalog
- Manage a Microsoft Azure catalog
- Manage a Microsoft System Center Virtual Machine Manager catalog
- Manage a VMware catalog

Manage an AWS catalog

September 6, 2025

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to AWS cloud environments.

> **Note:**
>
> Before managing an AWS catalog, you need to finish creating an AWS catalog. See Create an AWS catalog.

Remove tags

When you create a catalog or a VM, MCS- created tags are created on the following resources:

- Virtual machine

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

- Root disk volume
- Identity disk volume
- NIC
- Root disk image (AMI)
- Launch template
- Snapshot of AMI or root disk

You can remove VMs and machine catalogs from Citrix® database and remove MCS- created tags. You can use:

- `Remove-ProvVM` with `ForgetVM` parameter to remove VMs and MCS- created 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 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. 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 MCS- created tags from resources.
   - Run `Remove-ProvVM` with `ForgetVM` to remove VMs from Citrix database and 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™, however, 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 tags are now removed. Tags from the following resources are removed:

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

- Virtual machine
- Root disk volume
- Identity disk volume
- NIC

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. 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"
NIC	"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”: “”
VM in catalog	“XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “CitrixResource”: “” [when AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx”

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

Resource name	Tag
	[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”

More information

- Create and manage connections and resources
- Connection to AWS
- Create machine catalogs
- Create an AWS catalog
- Manage machine catalogs

Manage a XenServer® catalog

September 6, 2025

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to XenServer virtualization environments.

> **Note:**
>
> Before managing a XenServer catalog, you need to finish creating a XenServer catalog. See Cre-

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

> ate a XenServer catalog.

Identify resources created by MCS

Following are the tags that MCS adds to the resources. The tags in the table are represented as "key" :"value".

Resource name	Tag
Published base disk and its copy on each network or local storage	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ID disk	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OS disk	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Prep VM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM in catalog	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBC disk	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

More information

- Create and manage connections and resources
- Connection to XenServer
- Create machine catalogs
- Create a XenServer catalog
- Manage machine catalogs

Manage a Google Cloud Platform catalog

September 13, 2025

Manage machine catalogs describes the wizards that manage a machine catalog. The following information covers details specific to Google cloud environments.

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

> **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.

Manage machine catalog

To add machines to a catalog, update machines, and roll back an update, see Manage machine catalogs.

Power management

Citrix DaaS™ lets your power management of Google Cloud machines. Use the **Search** node in the left pane to locate the machine you want to power manage. The following power actions are available:

- Delete
- Start
- Restart
- Force Restart
- Shut Down
- 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 update supported by this feature is machine profile.

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

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

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,

```
`Set-ProvScheme  – ProvisioningSchemeName "my-catalog"  –
    MachineProfile "XDHyp:\HostingUnits\<hosting-unit>\
    machineprofileinstance.vm"
```

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
```

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:

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

```
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

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.

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" />
```

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

```
<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:

```
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. The tags in the table are represented as “key” :”value”.

Resource name	Tag
ID disk	“CitrixResource”: “internal”

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

Resource name	Tag
Image	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
OS disk	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
PrepVM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
Published snapshot	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
Storage bucket	“Citrixresource”: “internal”
Template	“CitrixResource”: “internal”
VM in catalog	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
WBC disk	“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. “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

September 6, 2025

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.

Power management

Citrix Virtual Apps and Desktops™ 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

September 13, 2025

> **Note:**
>
> Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

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.

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.

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

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 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 Restriction.

1. Add the custom property `StorageTypeAtShutdown`, set the value to Standard_LRS (HDD), and create a catalog using `New-ProvScheme`. For information on creating a catalog using PowerShell, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **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" />
</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" />
```

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

```
<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`.

2. Shut down the VM and check the storage type of the VM in the 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 Restriction.

Use `Set-ProvScheme` to add a VM to an existing catalog. The feature applies to new VMs added after running `Set-ProvScheme`. The existing machines are not affected.

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"
    />
```

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

```
<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>'

$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 Restriction.

You can 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.

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>'
   ```

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
   ```

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

6. Update the existing VMs to enable `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName -
    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  }
   }
```

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`

> **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

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

> takes effect.

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`

> **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:

© 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
```

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
```

> **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,

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

```
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
     ```

   > **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. 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, configuration update is not applied
     - you power on the machine, configuration update is applied
   - If the machine is powered on, and
     - you do not restart the machine, configuration update is not applied
     - you restart the machine, configuration update is applied

To cancel the configuration update:

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

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:

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog" -VMName "vm1","vm2"
    ```

    > **Note:**
    >
    > The VMs must be from the same catalog.

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 only to the Azure environment.

Currently, the properties that you can update are:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

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

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:

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

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. Check the configuration of the VM on which you want to apply the updates. For example:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -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 AzureCatalog -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 AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
```

> **Note:**
>
> The updates are not applied immediately.

3. Get the list of properties that are specified to be updated and the configuration version. For example:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    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 AzureCatalog -VMName machine1
```

Check the property value of `ProvVMConfigurationVersion`. The update is not yet applied. The VM is still in the old configuration.

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

5. Request scheduled update. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    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.

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 AzureCatalog -
    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 AzureCatalog
```

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 AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits\<hosting-unit>\
    machineprofile.folder\<resource-group>.resourcegroup\<template-
    spec>.templatespec\<template-spec-version>.templatespecversion"
```

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

> **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
    AzureCatalog -VMName machine1
```

> **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 AzureCatalog -
    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 AzureCatalog -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 AzureCatalog -VMName machine1
```

3. Request scheduled update for the VM. For example:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
```

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

4. Restart the VM. For example:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. Check the configuration version of the VM. For example:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

The `ProvVMConfigurationVersion` value is now the configuration version of the machine 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/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/
    testrsg/providers/Microsoft.Compute/diskEncryptionSets/test-
    diskEncryptionSet"/>
</CustomProperties>
"@
New-ProvScheme -CleanOnBoot `
-ProvisioningSchemeName $provisioningSchemeName `
-HostingUnitName $hostingUnitName `
-IdentityPoolName $identityPoolName `
-InitialBatchSizeHint $numberOfVms `
-masterImagePath $masterImagePath `
-NetworkMapping $networkMapping `
-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>'
```

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

```
4 Set-ProvScheme -ProvisioningSchemeName azure-catalog -
      CustomProperties $customProperties
5 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:

```
1 $customProperties = '<CustomProperties xmlns="http://schemas.
      citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
      org/2001/XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
      Value="" />
3 </CustomProperties>'
4 Set-ProvScheme -ProvisioningSchemeName azure-catalog -
      CustomProperties $customProperties
5 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 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`.
2. Run `Set-ProvScheme` to update the catalog with `DiskEncryptionSetId`.

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

> **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`:

```
$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 Web 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 will get errors while trying to add new VMs to the catalog.

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="" />
</CustomProperties>'
```

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

```
4 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`.
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`:

```
1 $customProperties = '<CustomProperties xmlns="http://schemas.
      citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
      org/2001/XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
      Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
      providers/Microsoft.Compute/diskEncryptionSets/
      diskEncryptionSet1" />
3 </CustomProperties>'
4 Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
      CustomProperties $customProperties
```

   Example when using MachineProfile:

```
1 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:

```
1 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.

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

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`, `WriteBackCacheDiskSiz` , and `UseWriteBackCache` are enabled.
- Ephemeral OS disk is not enabled.
- WBC is non-persistent: `PersistWBC` is **`false`**.
- `UseTempDiskForWBC` is null or false.
- 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>"
```

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

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 that the OS type is Windows; 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
```

Identify resources created by MCS

Following are the tags that MCS adds to the resources. The tags in the table are represented as “key” :”value”.

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

Resource name	Tag
ID disk	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
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”
PrepVM	“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
Storage account	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
VM in catalog	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
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

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

> 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 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:

```
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.

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

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 System Center Virtual Machine Manager catalog

May 5, 2025

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. The tags in the table are represented as "key" :"value".

Resource name	Tag
Prep 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

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

- 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

November 12, 2025

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

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.
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.

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

Option	Description
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.
Manage Tags	Create, edit, and delete tags. Select tags to apply to the catalog.
Move Machine Catalog	Move the catalog to another folder.

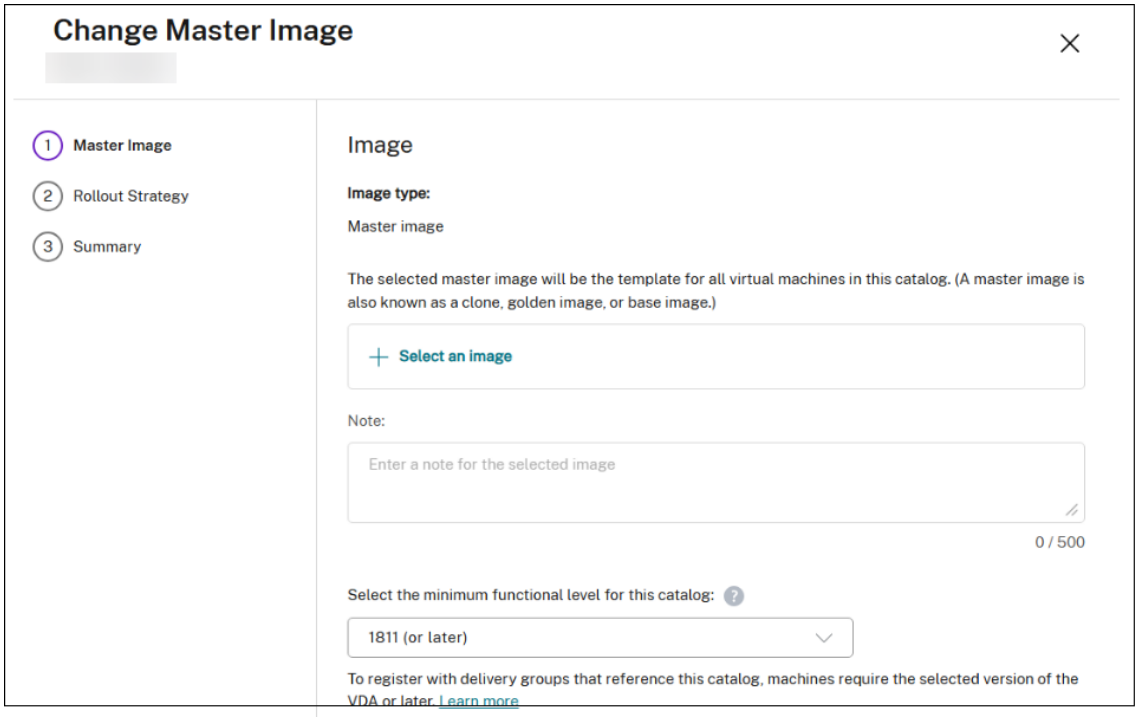
> **Note:**
>
> Currently, the **Clone** option is not available.

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**.

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



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.

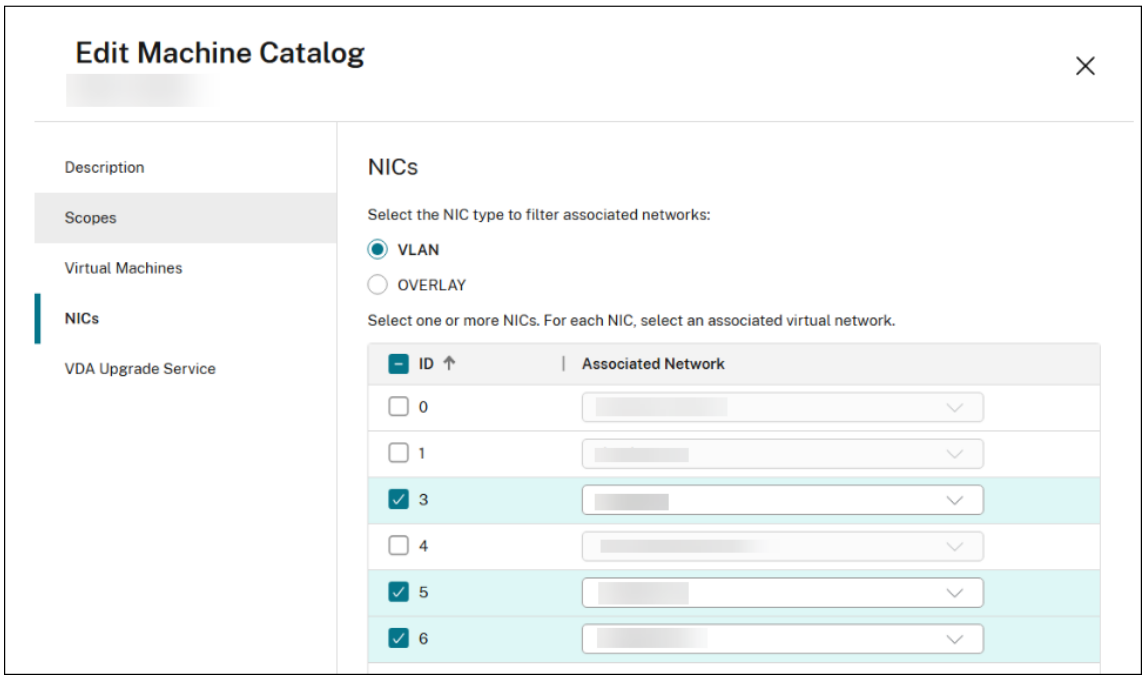
> **Note:**
>
> For an MCS provisioned non-persistent catalog with the Nutanix AHV Prism Central host connection plug-in, updating the master image to switch the boot configuration between Legacy and UEFI, prevents existing VMs from starting at their next boot.

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:
    a) Select an NIC type
    b) Select or clear the boxes to select NICs, and choose an associated virtual network for each NIC.

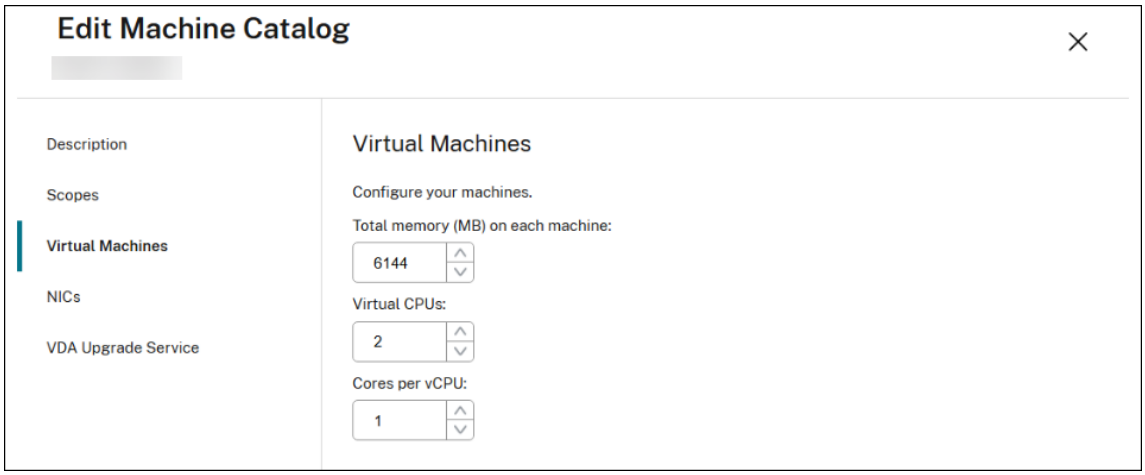
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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
```

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 Unit Name>\Clusters.folder\<Cluster
    Name>\<Network name>.network" }
  -ProvisioningSchemeName "<ProvisioningSchemeName>" -VMCpuCount 4
```

More information

- Create and manage connections and resources
- Connection to Nutanix
- Connection to Nutanix cloud and partner solutions
- Create machine catalogs
- Create a Nutanix catalog
- Manage machine catalogs

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

Manage a VMware catalog

September 6, 2025

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 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-2e83-4a37-9ea1-94
    f630687372" -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>"
```

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.

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

Find the folder ID in vSphere

Access Managed Object Browser (MOB) on any ESXi or vCenter server system to find the folder ID of the VMs.

The 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.

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. The tags in the table are represented as "key":"value".

Resource name	Tag
Prep 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

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

Power Management

September 6, 2025

With Citrix Virtual Apps and Desktops™, 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 AWS VMs
- Power manage Azure VMs

Power manage AWS VMs

May 5, 2025

For information on required permissions, see Required AWS permissions.

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.

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

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 on how to launch the instance, encrypt root EBS volume, and enable hibernation, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/. Use this instance as a master image to create an AMI.
3. 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.
   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.
4. Create an AMI from that instance. For information on creating an AMI from an instance, see Create an AMI from an Amazon EC2 Instance.
5. Create a machine catalog using `New-ProvScheme` command. Set the `AwsCaptureInstancePropert` custom property as **True**. For information on enabling AWS instance properties in Web Studio, see **Applying AWS instance properties and tagging operational resources in Web Studio**.

```
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" }
```

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

```
6
7 -ProvisioningSchemeName $catalog_name
8 -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.

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,

```
1 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.

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

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.

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 VM from the running state.
2. Resume VM from the suspended state.
3. Restart VM from the suspended state.

Power manage Azure Local VMs

September 6, 2025

Citrix Virtual Apps and Desktops™ lets you do power management of Azure Local 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

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

- Force Shutdown
- Restart

> **Note:**
>
> Reset, Suspend, and Resume power actions are not supported.

Power manage Azure VMs

December 17, 2025

For information on required permissions, see Required Azure permissions.

Azure on-demand provisioning

With Azure on-demand provisioning, VMs are created only when Citrix Virtual Apps and Desktops™ 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 Virtual Apps and Desktops initiates a power-on action for it. 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 isn't visible in the Azure portal. There's a significant storage cost saving if you routinely shut down machines (for example, outside of working hours).
- 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 on-demand provisioning feature ("legacy"catalogs) is deprecated. Therefore, recreate Azure legacy catalog VMs. The catalogs are then provisioned as

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

> on-demand that saves storage cost.

Preserve 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 isn't 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 isn't 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"
   />
<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`" /><
```

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

```
        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" }

-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. Do not 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 can't 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.

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

- On shutdown, the VM remains off with the incorrect storage type.

To create a machine catalog:

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.
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. For information on how to create a catalog using the Remote PowerShell SDK, see https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-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:

```
    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`" />
```

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

```
6     </CustomProperties>"
```

To apply the change done in Set-ProvScheme to the existing VMs, run the `Set-ProvVMUpdateTimeWindow` command with `-StartsNow` and `-DurationInMinutes -1` parameters.

1. Run `Set-ProvVMUpdateTimeWindow` command with `-StartsNow` and `-DurationInMinutes -1` parameters command. For example:

```
1  Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
       VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

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.

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.

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

- 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:

  1. Open the Azure Portal. Choose a VM whose configuration you want to use in the template. Select **Export template** in the left pane.
  2. Clear the **Include parameters** checkbox. Copy the context and save it as a JSON file, for example, `VMExportTemplate.json`.
  3. 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 supported VM size in the template file. However, you can also specify the machine size while creating the catalog.
  4. 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.
  5. Select **Azure Portal > Template specs > Import template > Choose local template file** to import this template file as an ARM template spec.
  6. 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.

For more information, see the Microsoft document.

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

Create and manage a hibernation-capable machine catalog

To create hibernation-capable VMs, you can create and manage a hibernation-capable machine catalog using:

- Web Studio, or
- PowerShell commands

Create a catalog using Web Studio

1. Select **Create Machine Catalog**. The catalog creation wizard opens.
2. On the **Machine Type** page, select the **Single-session OS** machine type for this catalog.
3. 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)**.
4. On the **Desktop Experience** page, select the random or static desktop experience as needed.
5. 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, the blade lists all the images that belong to the same region as those of Resources.

6. On the **Storage and License Types** page, select the storage and license to use for this catalog.
7. 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.

8. On the **NICs** page, add the NICs you want the VMs to use.
9. On the **Disk Settings** page, select the storage type and size of the write-back cache disk.
10. On the **Resource Group** page, select the resource group to provision VMs.
11. On the **Machine Identities** page, select **Create new Active Directory accounts**. Then, specify an account naming scheme.
12. On the **Domain Credentials** page, click **Enter credentials**. Enter your domain credentials to perform account creation in the target Active Directory domain.

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

13. 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**.

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 the Web 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 Web 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 New-ProvScheme.

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,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
    ("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.
    folder") | select Name, AdditionalData | ConvertTo-Json
```

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

- For the machine profile, run the following command and check whether the property `supportsHibernation` is **True**. For example,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -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 Web 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`.

```
(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
```

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

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:

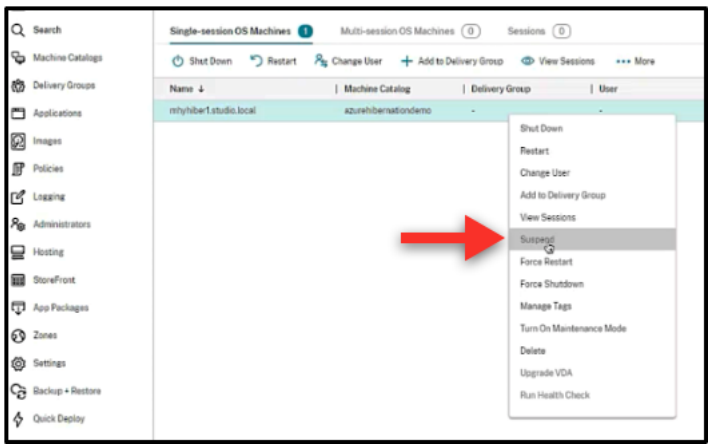
- Suspend
- Resume

Suspend You can suspend a VM using one of the following ways:

- **Manually** using Web Studio
- **Automatically** using the timeout policy: For more information, see Miscellaneous settings.

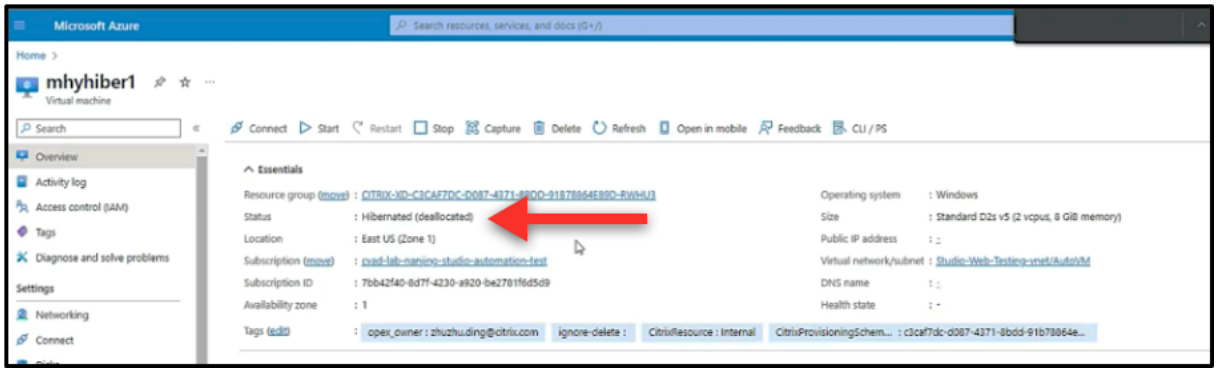
To manually suspend a VM:

1. Right-click the VM, and select **Suspend**. Click **Yes** to confirm the action. The **Power State** changes from **Suspending** to **Suspended**.



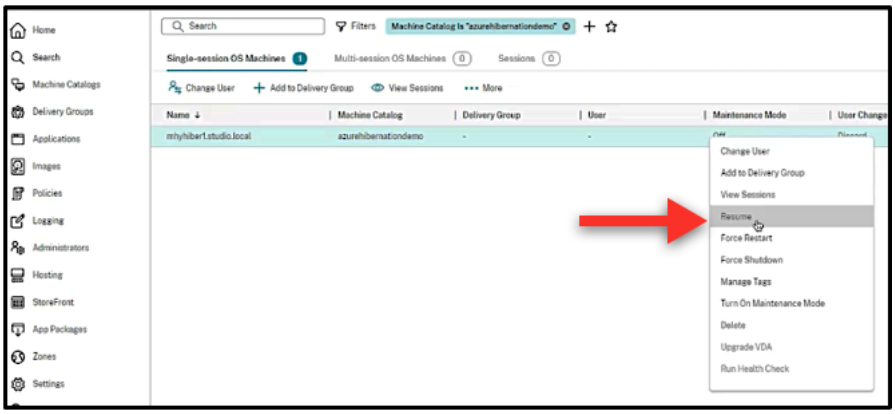
You can check the status of the VM in the Azure portal.

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

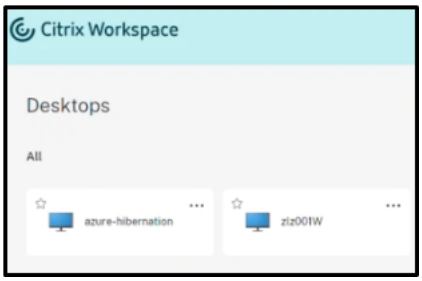


Resume To resume a hibernated VM, use one of the following ways:

- **Manually**:
  - Administrators can resume the VM using the Web Studio.



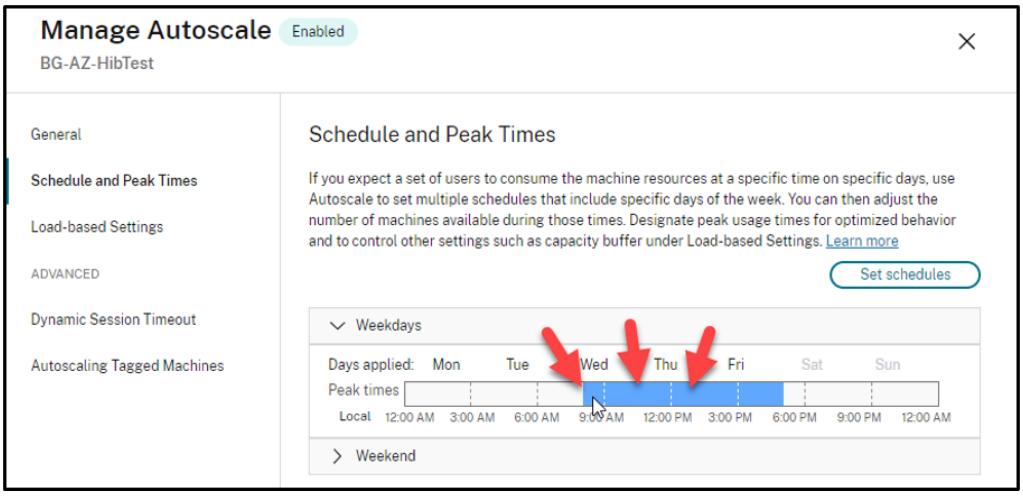
  - End users can start the VM using the Citrix Workspace™ menu once they click the desktop icon.



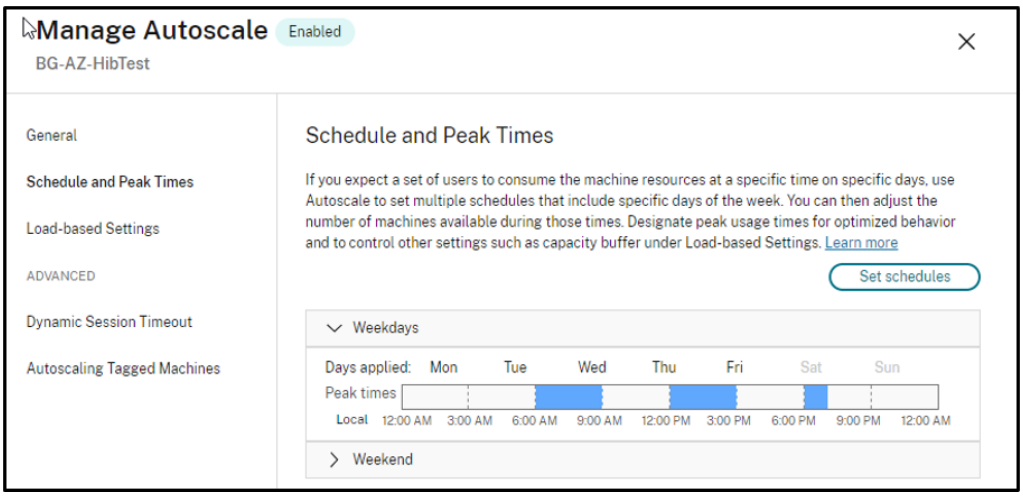
- **Automatically**:
  - Autoscale™ can automatically power on the hibernated machines if you configure the peak times correctly. You can set the peak times in 30-minutes intervals by clicking the time-schedule. Each blue frame represents a timeslot marked as peak time. The peak times can have consecutive and non-consecutive time slots.

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

- Consecutive time slots

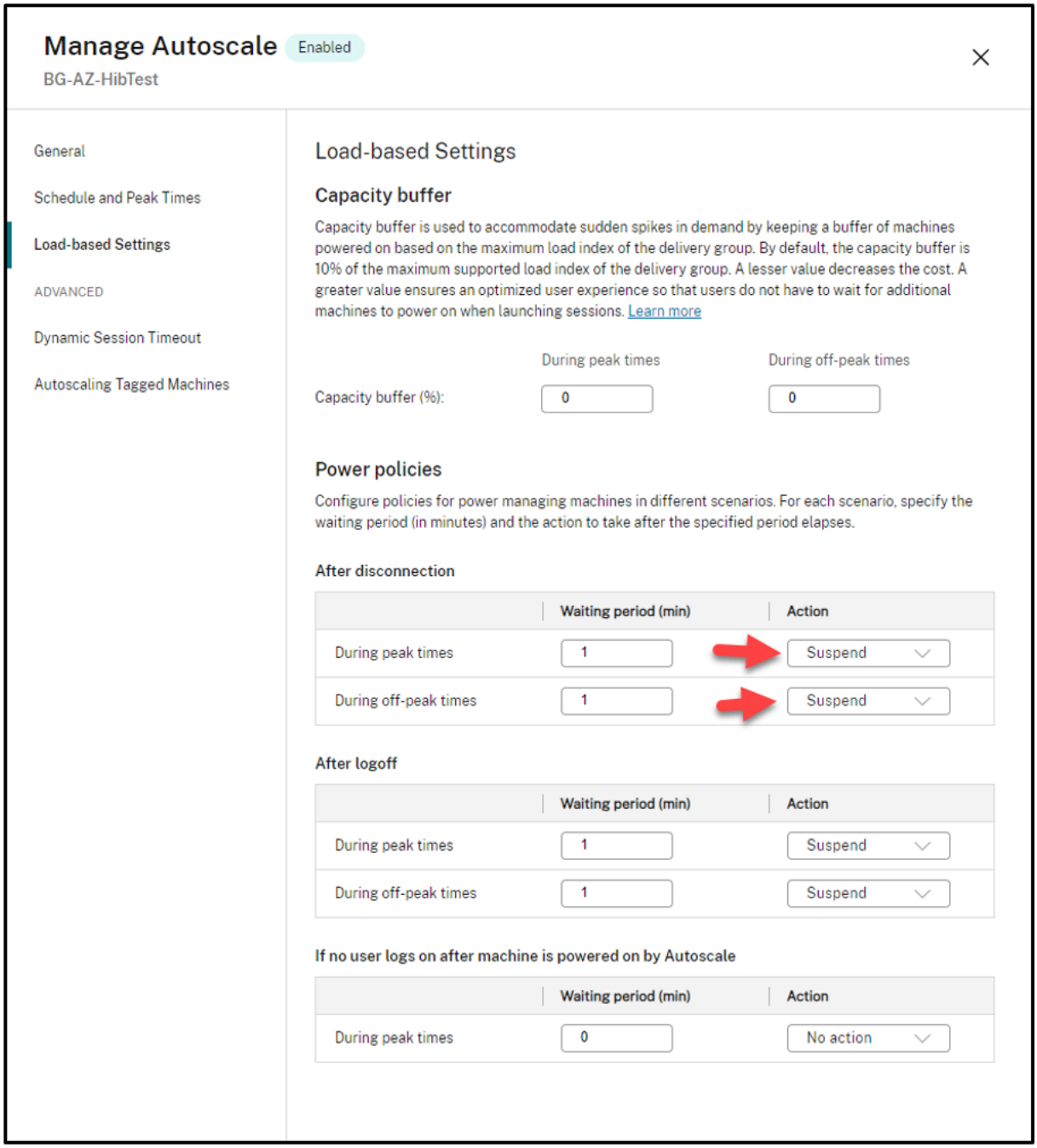


- Non-consecutive time slots



> **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:

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

1. Open a PowerShell window.
2. Run `asnp citrix*` to load Citrix-specific PowerShell modules.
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": {

                      "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\
```

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

```
                        tHypervisor"
21                      }
22
23                    }
24
25  EventCategory       : Warning
26  EventDateTime       : 1/11/2024 4:18:31 AM
27  EventId             : 0
28  EventMessage        : Failed to suspend machine my-resource-group/
        my-vm.
29  EventSeverity       : Important
30  EventSource         : AzureRmPlugin
31  EventState          : New
32  LinkedObjectType    : ProvisioningScheme
33  LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366
34  OperationName       : Suspend
35  OperationTargetName : my-resource-group/my-vm
36  OperationTargetType : VirtualMachine
37  OperationType       : PowerManagement
38  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. As per Microsoft Windows limitation, hibernation is only supported with nested virtualization when trusted launch is enabled on the VM.

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

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.

Power manage Red Hat OpenShift VMs

September 6, 2025

Citrix Virtual Apps and Desktops™ lets you do power management of Red Hat OpenShift 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
- Restart

> **Note:**
>
> Reset, Suspend, and Resume power actions are not supported.

Power manage Nutanix AHV VMs

August 6, 2026

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

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

- 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

May 5, 2025

This article describes security features on various supported cloud services. The security features include:

- Security groups
- Secure boot
- Encryption capabilities

Security groups

May 5, 2025

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
- 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

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

- 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 groups in AWS
- Security groups in Microsoft Azure
- Security groups in Google Cloud Platform

Security groups 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 groups in Microsoft Azure

Citrix Virtual Apps and Desktops 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 groups 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 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.

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

Secure Boot and vTPM

November 12, 2025

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 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
- 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.

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

> **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 Virtual Apps and Desktops.

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

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

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

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.

Encryption capabilities

May 5, 2025

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 cloud services:

- 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.

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

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 Virtual Apps and Desktops 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.

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

© 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. 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.

Load balance machines

May 5, 2025

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.

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

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

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. 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.

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

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

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.

  > **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

December 1, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

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.

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

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.

To create a delivery group:

1. If you have created a site and a machine catalog without a delivery group, Web Studio guides you to the correct starting place to create one.

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.
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 Load Balancing Users	Machines Delivery Type Users	Machines Users Applications	Machines Users Applications

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

	Multi-session OS	Single-session OS static (assigned)	Single-session OS shared (pooled)	Remote PC Access
	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	

> **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 setting 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.

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

- 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:
  - 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.

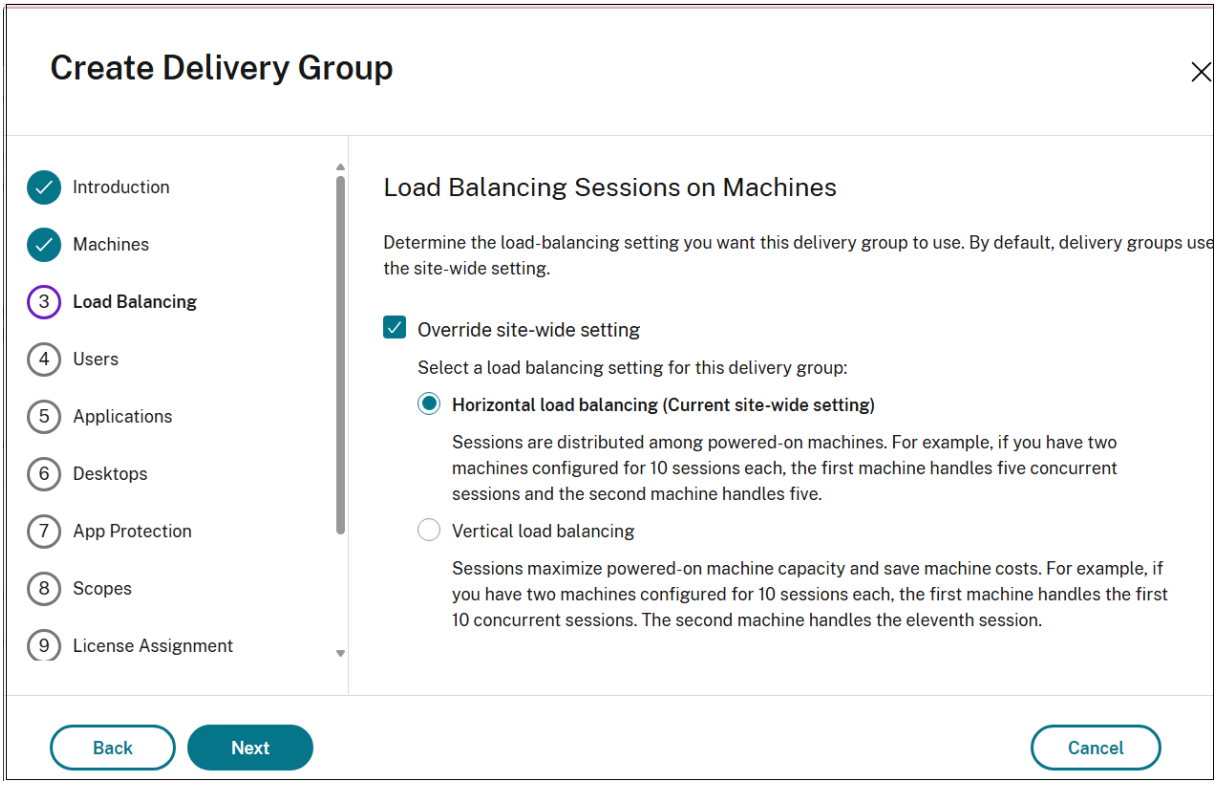
Load Balancing page

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.

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` cmdlets for details.
  - 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).

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.

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

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.

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.

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

- 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.

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 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 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.

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

- **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 you chose earlier in the wizard:

- 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. 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

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

can assign machines manually or use RemotePC to have the machines assigned automatically.

e) 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.

f) When you are finished with the dialog box, select **OK**.

Maximum instances of a desktop in a site (PowerShell only)

To configure the maximum instances of a desktop in the site (PowerShell only):

- In PowerShell, use the appropriate BrokerEntitlementPolicyRule cmdlet with the MaxPerEntitlementInstances parameter. For example, the following cmdlet modifies the `tsvda-desktop` rule to set the maximum concurrent instances of a desktop allowed in the site to two. When there are two desktop instances running, an error occurs if a third subscriber attempts to start a desktop.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInst
   2
  ```

- For guidance, use the Get-Help cmdlet. For example, `Get-Help Set-BrokerEntitlementPolicyRu -Parameter MaxPerEntitlementInstances`.

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.

- 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 > 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.

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

- **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.

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 Multi-type licensing.

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 setting page

This page is available only for delivery groups containing power-managed single-session pooled machines.

By default, pooled machines that are power managed are unavailable when in Local Host Cache (LHC) mode due to data exposure risks. To change the default behavior and make them available for new user connections when in LHC mode, select **Keep resources available**.

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.

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

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.

Prerequisites

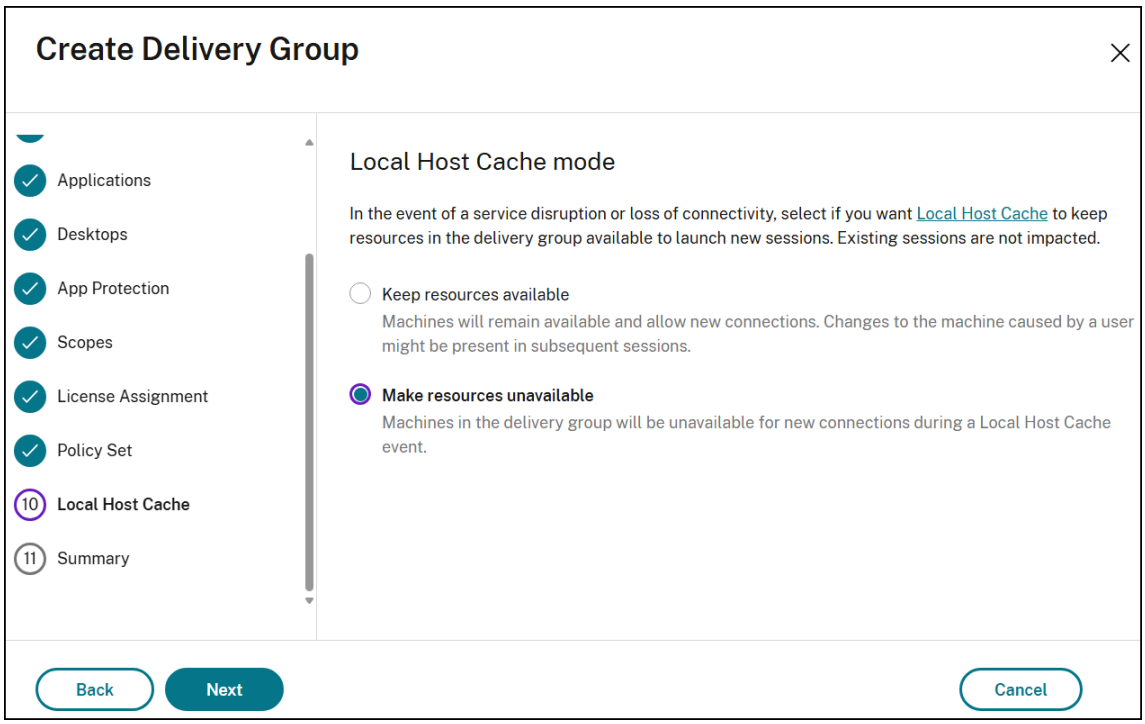
- VDA version 2407 or later for full hygiene enforcement. Legacy VDAs (prior to VDA version 2407) can be used only when reuse is enabled. These VDAs do not receive the hygiene blob or enforced reboots.
- Machine catalogs with single session machines.

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 Web Studio on the **Local Host Cache mode** page when creating a delivery group.

```
1 Set-BrokerDesktopGroup -Name "name" -
      ReuseMachinesWithoutShutdownInOutage $false
```

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



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.

> **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 very limited set of client types and configurations. Performing access filtering based on the client IP address uses the public IP address for cloud clients.

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

More information

- Manage delivery groups
- Applications

Manage delivery groups

September 13, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Introduction

This article describes procedures for managing delivery groups from the management console. In addition to changing settings specified when creating the group, you can configure other settings that are not available when you create a delivery group.

Procedure categories include: 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. 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.
- Managing delivery groups requires the Delivery Group Administrator built-in role permissions. For details, see Delegated administration.

General

- View group details
- Change the delivery type
- Change StoreFront™ addresses
- Change the functional level
- Manage Remote PC Access delivery groups
- Organize delivery groups using folders

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

- Manage App Protection
- Change the 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.
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 the delivery type of a delivery group

The delivery type indicates what the group can deliver: applications, desktops, or both.

Before changing an **application only** or **desktops and applications** type to the **desktops only** type, delete all applications from the group.

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.

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

3. On the **Delivery Type** page, select the delivery type you want.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

Change StoreFront addresses

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **StoreFront** page, select or add StoreFront URLs. These URLs are used by the Citrix Workspace™ app, which is installed on each machine in the delivery group.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

You can also specify StoreFront server addresses by selecting **StoreFront** in the left pane.

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 a Delivery Controller. This process tells the console about what needs upgrading in the delivery group.
- If you must continue to use earlier VDA versions, newer product features are not available. For more information, see the upgrade documentation.

To change the functional level for a delivery group:

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Change Functional Level** in the action bar. The **Change Functional Level** action appears only if upgraded VDAs are detected.
3. Click **Change**.

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, 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 the machine's assigned delivery group 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. 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. Select **Delivery Groups** in the left pane.
2. Select a Remote PC Access group.
3. In the **Details** section, click the **Machine Catalogs** tab and then select a Remote PC Access catalog.
4. To add or restore an association, click **Add Desktops**. To remove an association, click **Remove Association**.

Organize delivery groups using folders

You can create folders to organize delivery groups for easy access.

> **Tip:**
>
> You can set your preferred default view (folder or list view) for the Delivery Groups node by clicking the **Folder** icon in the upper 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 root folder).

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

- A folder can contain delivery groups and subfolders.
- All nodes in Web 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. 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**.

> **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. 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.

Be aware that you can delete a folder only if it and its subfolders don't contain delivery groups.

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

To manage a folder, follow these steps:

1. 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 onscreen instructions to complete the remaining steps.

Required permissions The following table lists the permissions required to perform actions on delivery group folders.

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 App protection. Mind the following details:

- 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 > 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.

To choose an App Protection method for a delivery group, follow these steps:

1. 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 **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. a) Click **Access Policy** in the left pane and click **Add**. b) On the **Add Policy** page, do the following • i. Enter a **Policy name** and configure the settings as required. • 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.

Change the 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 Web Studio, go to **Delivery Groups** in the left pane.
2. Select a group, and then click **Change Suspend Capability** in the action bar.
3. Click **Yes** to confirm your action.

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

Users

This section covers the following topics:

- Change user settings
- Add or remove users
- Manage user assignments

Change user settings in a delivery group

The name of this page appears as either **User Settings** or **Basic Settings**.

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **User Settings** (or **Basic Settings**) page, change any of the settings in the following table.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

Setting	Description
Description	The text that Citrix Workspace (or StoreFront) uses and that users see.
Enable delivery group	Whether the delivery group is enabled.
Time zone	The time zone in which the machines of this delivery group must reside. The option 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.

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

Add or remove users in a delivery group

For detailed information about users, see Users.

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Users** page:
   - To add users, click **Add**, and then specify the users you want to add.
   - To remove users, select one or more users and then click **Remove**.
   - Select or clear the checkbox to allow access by unauthenticated users.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

Import or export user lists For delivery groups containing physical single-session OS machines, you can import user information from a .csv file after you create the delivery group. You can also export user information to a .csv file. The .csv file can contain data from a previous product version.

The first line in the CSV file must contain two column headers, separated by a comma. Make sure that the first header is `Machine Account` and the second header is `User Names`. (You can include additional headers but they are not supported.) Subsequent lines in the file contain comma-separated data. The `Machine Account` entries can be computer SID, FQDN, or domain and computer name pairs.

To import or export user information:

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Machine Allocation** page, select **Import** list or **Export** list, and then browse to the file location.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

Manage user assignments

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 topic to make changes. Using these steps, you can also modify names displayed in the Citrix Workspace App for machines assigned to users.

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

Detailed steps are as follows:

1. In the console, 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.

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.

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. Note that 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.

Machines

- Change assignments of machines to users
- Enable Local Host Cache for power-managed single-session pooled VDAs
- Change the maximum number of machines per user
- Update a machine
- Add, change, or remove a tag restriction for a desktop
- Remove a machine

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

- Restrict access to machines
- Prevent users from connecting to a machine (maintenance mode)
- Shut down and restart machines
- Create and manage restart schedules for machines
- Enable one-time restart schedule
- Power managed machines

Change assignments of machines to users in a delivery group

You can change the assignments of single-session OS machines provisioned with MCS. You cannot change assignments for multi-session OS machines or machines provisioned with Citrix Provisioning.

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Desktops** or **Desktop Assignment Rules** page (the page title depends on the type of machine catalog that the delivery group uses), specify the new users.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

Enable Local Host Cache for power-managed single-session pooled VDAs

By default, power-managed single-session pooled machines are unavailable 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.

   In the group list, groups containing single-session pooled machines provisioned by MCS or Citrix Provisioning display a warning icon.

2. Select a group as needed, then select **Edit** in the action bar.
3. On the **Local Host Cache** page, select **Keep resources available**.
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 Application and desktop support.

> **Important:**
>
> Enabling access to power-managed single-session pooled machines can cause data and changes

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

> from previous user sessions being present in subsequent sessions.

Change the maximum number of machines per user in a delivery group

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Desktop Assignment Rules** page, set the maximum desktops per user value.
4. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

Update a machine in a delivery group

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **View Machines** in the action bar.
3. Select a machine and then click **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 master 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 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. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Desktops** page, select the desktop and click **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**.

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

6. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

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. Select **Delivery Groups** in the left pane.
2. Select a group and then click **View Machines** in the action bar.
3. Ensure that the machine is shut down.
4. Select the machine and then click **Remove from Delivery Group** in the action bar.

You can also remove a machine from a delivery group through the connection the machine uses.

Restrict access to machines 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 Workspace (instead of StoreFront).
  - Restrict access to users connected through a specific Workspace URL.

This section guides you through how to restrict user access to delivery groups through access policy rules:

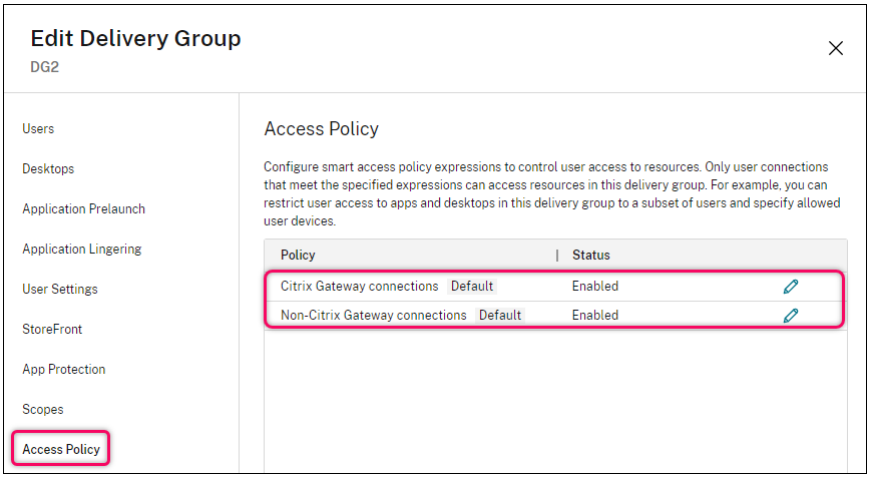
- About access policy rules
- Add access policy rules

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

- Manage access policy rules using Web 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 Web 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.
- **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 Web Studio.

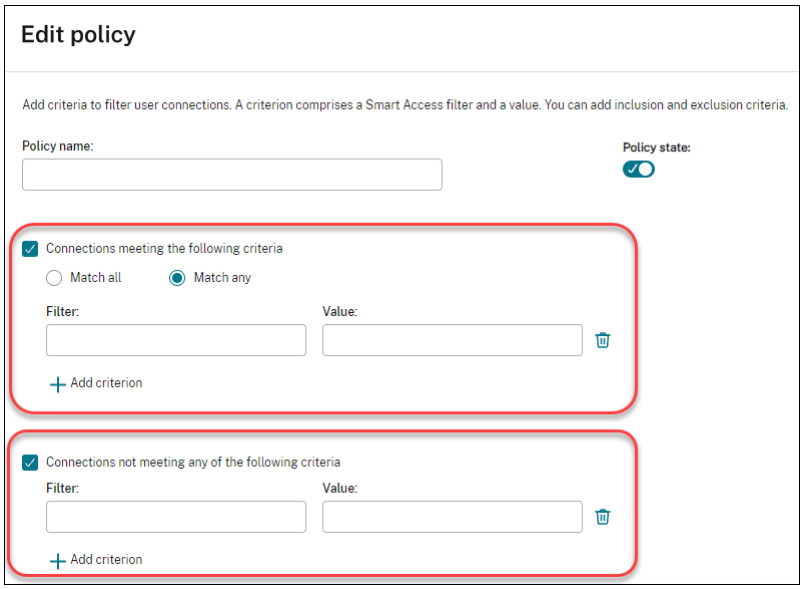
Add access policy rules using Web Studio An access policy rule comprises a set of filters. For more information about filters, see this article. When adding an access policy rule, you add multiple condi-

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

tion filters to the rule as needed.

To add a policy for a delivery group using Web Studio, follow these steps:

1. In the console, 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.



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` Workspace 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 Web 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 Web 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**.
3. Add, edit, or remove the SmartAccess policy expressions for the allowed user access scenarios.

For more information, see the Citrix Gateway documentation.

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

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.

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. Select **Delivery Groups** in the left pane.
2. Select a group.
3. To turn on maintenance mode for all machines in the delivery group, click **Turn On Maintenance Mode** in the action bar.

   To turn on maintenance mode for one machine, click **View Machines** in the action bar. Select a machine, and then click **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 click **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**. 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**.

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

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. Select **Delivery Groups** in the left pane.
2. Select a group and then click **View Machines** in the action bar.
3. Select the machine and then click one of the following entries in the action bar:

    - **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.
    - **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 is powered off before the updates finish.

Citrix recommends that you prevent single-session OS machine users from selecting **Shut down** within a session. See the Microsoft policy documentation for details.

You can also shut down and restart machines on a connection.

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.

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

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 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.

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.

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 are restarted only once.
- The more the schedules differ in start and duration times, it's more likely that multiple restarts 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. Select **Delivery Groups** in the left pane.
2. Select a group and then click **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

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

- Tag restriction used if any
- How often the machine restarts occur
- Whether machine users receive a notification
- Whether the schedule is enabled

Add (apply) tags When you configure a restart schedule that uses a tag restriction, ensure that the tag has been added 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.

Although you can apply more than one tag to a machine, a restart schedule can specify only one tag.

1. Select **Delivery Groups** in the left pane.
2. Select the group containing the machines controlled by the schedule.
3. Click **View Machines** and then select the machines you want to add a tag to.
4. Click **Manage Tags** in the action bar.
5. If the tag exists, enable the checkbox next to the tag name. If the tag does not exist, click **Create** and then specify the name for the tag. After the tag is created, enable the checkbox next to the newly created tag name.
6. Click **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. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Restart Schedule** page, click **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.

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

- 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.
- For **Restart duration**:
  - If you do not want to use natural restart, select **Restart all machines at the same time** or **Restart all machines within a time period**.
  - If you want to use natural restart, select **Restart all machines after draining all sessions**.

    Upon starting a restart schedule that is configured to use natural restart:

    - All idle machines belonging to the delivery group are restarted immediately
    - Each machine belonging to a delivery group with one or more active sessions is restarted when all sessions are logged off.

    > **Note:**
    >
    > Natural restart schedules can only restart power managed machines.

- In **Send notification to users**, choose 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 (in **Notification frequency**) 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 window open. Or, click **Save** to apply changes and close the window.

Restart after drain Another restart duration value is available when using PowerShell to create or update a machine restart schedule (`New-BrokerRebootSchedulev2` or `Set-BrokerRebootSchedulev2`).

When you enable the restart after drain feature with the `-UseNaturalReboot <Boolean>` parameter, all machines are restarted after draining all sessions. When the restart time is reached, machines are put into the drain state and then restarted when all sessions are logged off.

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

This feature is supported for delivery groups containing single-session or multi-session machines. You can use this option for machines that are power managed and also for machines that are not power managed.

In an on-premises environment, this feature is supported only when using PowerShell. The feature is not available in Web Studio.

Edit, remove, enable, or disable a restart schedule

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit** in the action bar.
3. On the **Restart Schedule** page, select the checkbox for a schedule.
    - To edit a schedule, click **Edit**. Update the schedule configuration, using the guidance in Create a restart schedule.
    - To enable or disable a schedule, click **Edit**. Select or clear the **Enable restart schedule** checkbox.
    - To remove a schedule, click **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 can have unintended results.

For example, let's say you've scheduled a delivery group's restarts to occur during off-production hours (beginning at 03:00). A site database outage occurs one hour before a scheduled restart begins (02:00). The outage lasts six hours (until 08:00). 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, resulting 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.

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

- 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. You cannot set this value when configuring a restart schedule in Web Studio.

Scheduled restarts for machines in maintenance mode

> **Note:**
>
> This feature is available only in PowerShell. The option `IgnoreMaintenanceMode` is supported with Citrix Virtual Apps and Desktops 7 2006 and later.

To indicate whether a restart schedule affects machines that are in maintenance mode, use the `IgnoreMaintenanceMode` option with `BrokerRebootScheduleV2` cmdlets.

For example, the following cmdlet creates a schedule that restarts machines that are in maintenance mode (in addition to machines that aren't 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. This feature is available only in PowerShell.

Enable one-time restart schedule

If you want to enable one-time restart schedule using PowerShell, use the following `BrokerCatalogRebootSch` PowerShell commands to create, modify, and delete a restart schedule:

- 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.

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

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.

```
C:\PS> 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.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot' -
    CatalogUid 17 -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**.

```
C:\PS> 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**.

```
C:\PS> 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.

  “‘

  C:\PS> 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.

```
C:\PS> 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** fifteen, ten, and five minutes before the restart of each VM.

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "
    Rebooting in %m% minutes." -WarningDuration 15 -
    WarningRepeatInterval 5
```

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

- To configure the time zone for the catalog named **MyCatalog**.

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
```

Power managed machines in a delivery group

You can power manage only virtual single-session OS machines, not physical machines (including Remote PC Access machines). Single-session OS machines with GPU capabilities cannot be suspended, so power-off operations fail. For multi-session OS machines, you can create a restart schedule.

In delivery groups containing pooled machines, virtual single-session OS machines can be in one of the following states:

- Randomly allocated and in use
- Unallocated and unconnected

In delivery groups containing static machines, virtual single-session OS machines can be:

- Permanently allocated and in use
- Permanently allocated and unconnected (but ready)
- Unallocated and unconnected

During normal use, static delivery groups typically contain both permanently allocated and unallocated machines. Initially, all machines are unallocated, except for manually allocated ones when the delivery group was created. As users connect, machines become permanently allocated. You can fully power manage the unallocated machines in those delivery groups, but only partially manage the permanently allocated machines.

- **Pools and buffers:** For pooled delivery groups and static delivery groups with unallocated machines, a pool (in this instance) is a set of unallocated or temporarily allocated machines that are kept in a powered-on state, ready for users to connect. A user gets a machine immediately after logon. The pool size (the number of machines kept powered-on) is configurable by time of day. For static delivery groups, use the SDK to configure the pool.

  A buffer is an extra standby set of unallocated machines that are turned on when the number of machines in the pool falls below a threshold. The threshold is a percentage of the delivery group size. For large delivery groups, a significant number of machines might be turned on when the threshold is exceeded. So, plan delivery group sizes carefully or use the SDK to adjust the default buffer size.

- **Power state timers:** You can use power state timers to suspend machines after users have disconnected for a specified amount of time. For example, machines suspend automatically outside of office hours if users are disconnected for at least 10 minutes.

  You can configure timers for weekdays and weekends, and for peak and nonpeak intervals.

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

- **Partial power management of permanently allocated machines:** For permanently allocated machines, you can set power state timers, but not pools or buffers. The machines are turned on at the start of each peak period, and turned off at the start of each off-peak period. You do not have the fine control that you have with unallocated machines over the number of machines that become available to compensate for machines that are consumed.

Power manage virtual single-session OS machines

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit Delivery Group** in the action bar.
3. On the **Power Management** page, select **Weekdays** in **Power manage machines**. By default, weekdays are Monday to Friday.
4. For random Delivery groups, in **Machines to be powered on**, click **Edit** and then specify the pool size during weekdays. Then, select the number of machines to power on.
5. In **Peak hours**, set the peak and off-peak hours for each day.
6. Set the power state timers for peak and non-peak hours during weekdays: In **During peak hours > When disconnected**, specify the delay (in minutes) before suspending any disconnected machine in the delivery group, and then select **Suspend**. In **During off-peak hours > When disconnected**, specify the delay before turning off any logged-off machine in the delivery group, and then select **Shutdown**. This timer is not available for delivery groups with random machines.
7. Select **Weekend** in **Power manage machines**, and then configure the peak hours and power state timers for weekends.
8. Click **Apply** to apply any changes you made and keep the window open. Or, click **Save** to apply changes and close the window.

Use the SDK to:

- Shut down, rather than suspend, machines in response to power state timers, or if you want the timers to be based on logoffs, rather than disconnections.
- Change the default weekday and weekend definitions.
- Disable power management. See CTX217289.

Power manage VDI machines transitioning to a different time period with disconnected sessions

> **Important:**
>
> This enhancement applies only to VDI machines with disconnected sessions. It does not apply to VDI machines with logged off sessions.

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

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

disconnected during a time period (peak or off-peak times) where no action (disconnect action=" **Nothing**") was required.

Starting with Citrix Virtual Apps and Desktops 7 1909, the machine is suspended or powered off 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 VDI delivery group:

- Set `PeakDisconnectAction` to "Nothing"
- Set `OffPeakDisconnectAction` to "Shutdown"
- Set `OffPeakDisconnectTimeout` to "10"

For more information about the disconnect action in the 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 VDI machine with a session disconnected during peak times remained powered on when it transitioned from peak to off-peak. Starting with Citrix Virtual Apps and Desktops 7 1909, the `OffPeakDisconnectAction` and the `OffPeakDisconnectTimeout` policy actions are applied to the VDI machine on period transition. As a result, the machine is powered off 10 minutes after it transitions to off-peak.

If 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`, the equivalent of *true* which enables the previous behavior. By default, the value is `0`, or *false*, which triggers disconnect power policy actions on period transition.
  - Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - Name: `LegacyPeakTransitionDisconnectedBehaviour`
  - 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:

- Have a disconnected session.

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

- Have no pending power actions.
- Belong to a VDI (single session) delivery group that transitions to a different time period.
- Have 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.

Change the percentage of VDAs in a powered state for catalogs

1. Adjust the peak hours for the delivery group from the **Power management** section for the delivery group.
2. Make a note of the Desktop Group name.
3. With administrator privileges, start PowerShell and run the following commands. Replace "Desktop Group Name"with the name of your desktop group that has a changed percentage of the VDAs running.

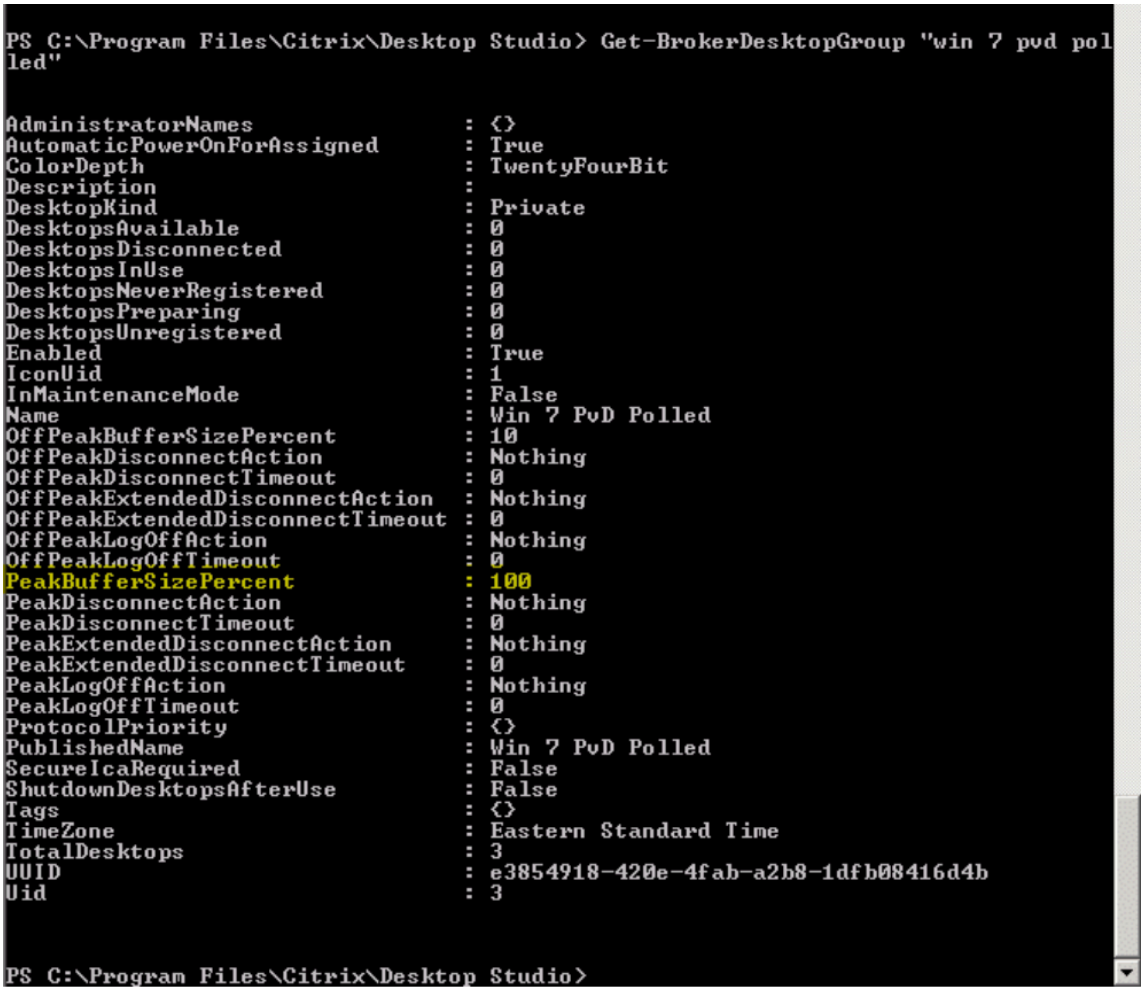
   ```
   asnp Citrix*

   # Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
    100
   ```

   A value of 100 means that 100% of the VDAs are in the ready state.
4. Verify the solution by running:

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```

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



It can take up to an hour for changes to take effect.

To shut down the VDAs after the user logs off, enter:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
 $True
```

To restart VDAs during peak hours, so that they're ready for users after they log off, enter:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
 $True
```

Sessions

- Log off or disconnect a session, or send a message to users
- Configure session prelaunch and session linger
- Control session reconnection when disconnected from machine in maintenance mode
- Configure session roaming

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

Log off or disconnect a session

1. Select **Delivery Groups** in the left pane.
2. Select a delivery group and then select **View Machines** in the action bar.
3. In the middle pane, select the machine, select **View Sessions** in the action bar, and then select a session.
    - Alternatively, in the middle pane, select the **Session** tab and then select a session.
4. To log off from a session, select **Log off** in the action bar. The session closes and the user is logged out. The machine becomes available to other users unless it is allocated to a specific user.
5. To disconnect a session, select **Disconnect** in the action bar. Applications continue to run in the session and the machine remains allocated to that user. The user can reconnect to the same machine.

You can configure power state timers for single-session OS machines to automatically handle unused sessions. For details, see Power managed machines.

Send a message to a delivery group

1. Select **Delivery Groups** in the left pane.
2. Select a delivery group and then select **View Machines** in the action bar.
3. In the middle pane, select a machine to which you want to send a message.
4. In the action bar, select **View Sessions**.
5. In the middle pane, select all sessions and then select **Send Message** in the action bar.
6. Type your message and click **OK**. You can specify the level of severity if needed. Options include **Critical**, **Question**, **Warning**, and **Information**.

Alternatively, you can send a message using Citrix Director. For more information, see Send messages to users.

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) and 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:

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

- 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 extra 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 must not log off.
- Prelaunched and lingering sessions consume a concurrent license, but only when connected. If using a user/device license, the license lasts 90 days. Unused prelaunched and lingering sessions disconnect after 15 minutes by default. This value can be configured 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.
- 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.

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

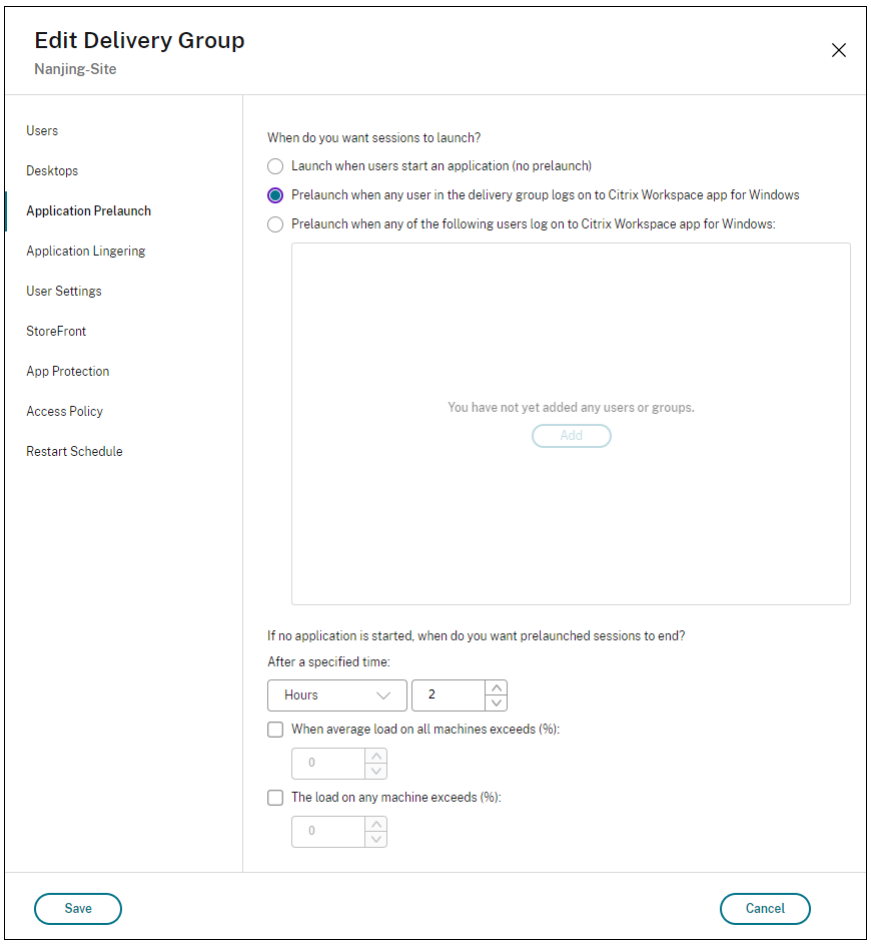
You can configure two thresholds: the average percentage load of all servers in the delivery group, and the maximum percentage load of a single server in the group. When a threshold is exceeded, the sessions that have been in the prelaunch or lingering state for the longest time are ended. Sessions are 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. Select a group and then click **Edit Delivery Group** in the action bar.
2. 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.
    - 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.

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



3. 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%)

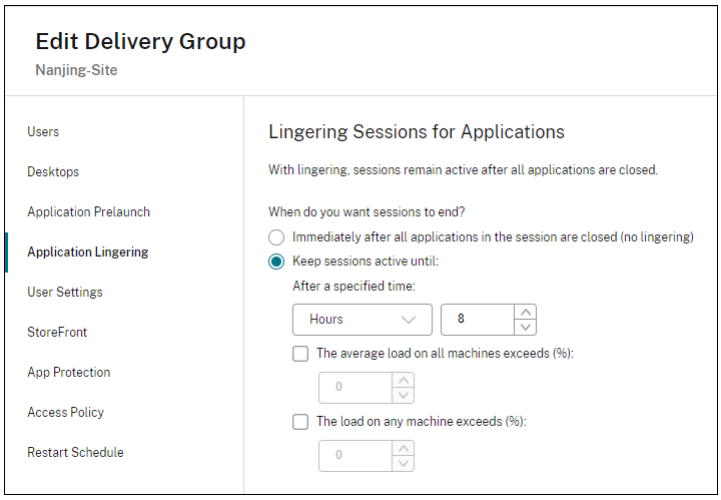
   Recap: A prelaunched session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

To enable session linger

1. Select **Delivery Groups** in the left pane.
2. Select a group and then click **Edit Delivery Group** in the action bar.

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

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.

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 version 2106, reconnection was not allowed for single-session pooled desktop sessions that had disconnected from machines in maintenance mode. As of version 2106, 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

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

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

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 use PowerShell. For more information, see Session roaming.

Configure session roaming for applications To configure session roaming for applications, follow these steps:

1. In the console, 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** checkbox.
    - 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. In the console, select **Delivery Groups** in the left pane.
2. Select a group and then select **Edit** in the action bar.
3. On the **Desktops** page, select the desktop and select **Edit**.
4. Enable session roaming by selecting the **Session roaming** checkbox.

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

- 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.

Select **OK** to apply changes and close the window.

Applications

View and add applications to a delivery group.

1. In the console, 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.

Seamless log in from Citrix Secure Access Client on VDA

You can seamlessly log in to Citrix Workspace using Single Sign-On (SSO) from the Citrix Secure Access (CSA) client present on the VDA to Citrix Secure Private Access. This feature is applicable to both single and multi-session VDAs.

The steps to achieve this are as follows:

1. Edit an existing delivery group to enable SPA SSO. For example,

```
Set-BrokerDesktopGroup -Name <String> -SpaSsoEnabled 1
```

2. Check the status of SPA SSO of a delivery group using the Get -BrokerDesktopGroup PowerShell command. For example:

```
Get-BrokerDesktopGroup -Name <String> -property 'SpaSsoEnabled'
```

3. In SPA, create Application and Policy. See Configure TCP/UDP apps and Configure access policies for the applications.
4. RDP into the single-session or multi-session VDA and install the latest CSA agent.
5. Open Citrix Workspace and log into the single-session or multi-session VDA.

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

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

various reasons that 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 can 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

September 13, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Introduction

Application groups let you manage collections of applications. Create application groups for applications shared across different delivery groups. Or, applications 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. Associate delivery groups with more than one application group, and associate an application group with more than one delivery group.

Using application groups can provide application management and resource control advantages over using more delivery groups:

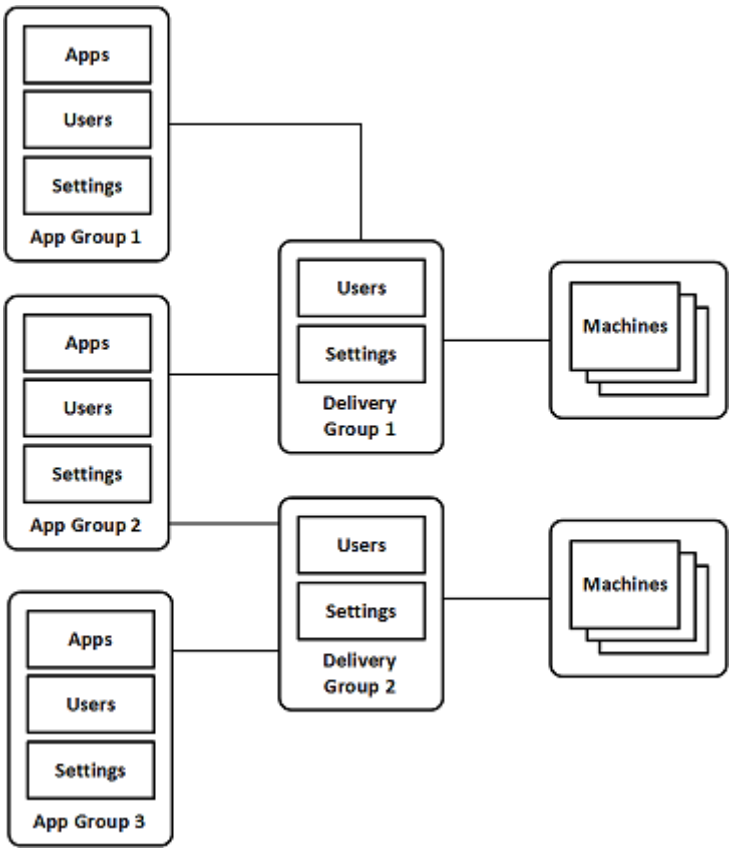
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 can be beneficial.
- 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 extra 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 Citrix Virtual Apps and Desktops deployment that includes application groups:



In this configuration, applications are added to the application groups, not the delivery groups. The

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

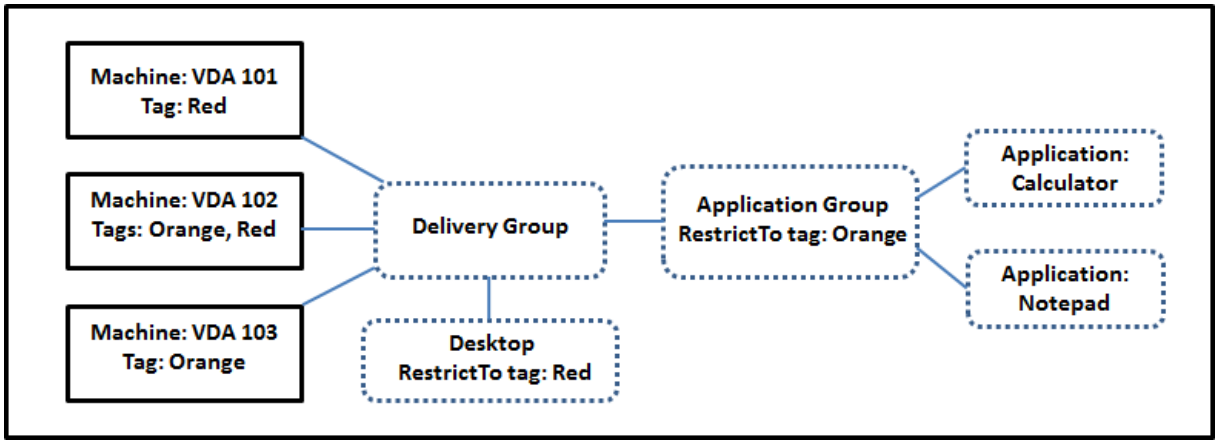
delivery groups specify which machines are used. (Although not shown, the machines are in machine catalogs.)

Application group 1 is associated with delivery group 1. Access the applications in application group 1 by the users specified in application group 1. These groups only appear as long as they are also in the user list for delivery group 1. This configuration follows the guidance that the user list for an application group is 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 groups) apply to applications and users in that group. The settings in delivery group 1 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 is assigned a priority in application group 2, indicating the order in which the delivery groups are checked when an application is launched. Delivery groups with equal priority are load balanced. Access the applications in application group 2 by the users specified in application group 2. However, they must also appear in the user lists for delivery group 1 and delivery group 2.

Example 2:

This simple layout uses tag restrictions to limit which machines are 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. Each of its applications is 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.

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

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.

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 process requires:

1. Upgrading VDAs on the machines used in the delivery group.
2. Upgrading the machine catalogs containing those machines.
3. Upgrading 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. It differentiates that action from adding instances of that application from an available source. Similarly, delivery groups are associated with application groups, 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 more application sessions, and allows the use of application features that involve the clipboard, such as copy-paste operations. However, in some situations you can clear 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 controller finds that 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:**

  A configuration with 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.

  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. The user can still run other applications at the same time, but not in the same session. When launching one of the different-versioned applications, or any application that is not contained in an application group, 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.

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.

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

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.

By default, application session sharing is enabled when you create an application group. You cannot change this setting 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

To create an application group:

1. Sign in to Web Studio.
2. Select **Applications** in the left pane, and then select the **Application Groups** tab.
3. To organize application groups using folders, create folders under the **Application Groups** root folder. For more information, see Organize application groups using folders.
4. 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.
5. 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 that you can select. Compatible delivery groups contain random (not permanently or statically assigned) multi-session or single-session OS machines.
- The **Incompatible Delivery Groups** list contains delivery groups that you cannot select. Each entry explains why it is not compatible, such as containing statically assigned machines.

An application group can be associated with delivery groups containing shared (not private) machines that can deliver applications.

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

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 application 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. Also, you cannot add applications to the application group from the **From Start** menu source if there are no delivery groups specified.

The delivery groups that you select specify the machines that are used to deliver applications. Select the check boxes next to the delivery groups that you want to associate with the application group.

To add a tag restriction, select **Restrict launches to machines with the tag** and then select the tag from the drop-down list.

Step 2. Users

Specify application users in the application group. Either allow all users and user groups in the delivery groups that you selected on the previous page, or select specific users and user groups from those delivery groups. If you restrict use to specified users, then only the users specified in the delivery group, the application group can access the applications in this 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 exists in that folder, you are prompted to rename the application you are adding. If you agree with the

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

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 Web Studio. Otherwise, users see duplicate names in 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.

Click the **Add** from the drop-down menu 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 click **OK**.

  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 defined:** 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, click **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 click **OK**. This source cannot be selected If the site has no applications.

- **App-V**: Applications in App-V packages. When you select this source, a new page launches where you select **App-V server** or **Application Library**. From the resulting display, select the check boxes of applications to add, and then click **OK**. For more information, see Deploy and deliver App-V applications. This source cannot be selected (or might not appear) if App-V is not configured for the site.

As noted, certain entries in the **Add** drop-down menu are not 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).

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

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.

Step 5. Summary

Enter a name for the application group. You can also (optionally) enter a description.

Review the summary information and then click **Finish**.

Manage application groups

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

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. See Delegated administration for details.

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

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

groups. If the application was explicitly added to delivery groups associated with 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 configuration when you create the group.

1. 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. Click **Apply** to keep the window open, or click **Save** to apply changes and close the window.

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 configuration when you create the group. For more information, see Session sharing with application groups.

1. 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. Click **Apply** to keep the window open, or click **Save** 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 option is 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, when launching Notepad with a disconnected session with Notepad running, that session is reconnected instead of creating a one. When multiple suitable disconnected sessions are available, one of the sessions is chosen to reconnect to, in a random but deterministic manner. When the situation reoccurs in the same circumstances, the same session is chosen, but the session is not necessarily predictable otherwise.

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

Use the PowerShell SDK either to disable application session sharing for all applications in an existing application group, or to create a group with application session sharing disabled.

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 associated directly with a delivery group share session 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. 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 click **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. 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, click **Add**. Select the check boxes of available delivery groups. (Incompatible delivery groups cannot be selected.) When you finish your selections, click **OK**.
5. To remove delivery groups, select the check boxes of the groups you want to remove and then click **Remove**. Confirm the deletion when prompted.
6. To change the priority of delivery groups, select the check box of the delivery group and then click **Edit Priority**. Enter the priority (0 = highest) and then click **OK**.
7. Click **Apply** to apply any changes you made and keep the window open, or click **Save** 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. 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 a tag restriction, select **Restrict launches to machines with the tag** and then select the tag from the drop-down list.
5. To change or remove a tag restriction, select a different tag or remove the tag restriction entirely by clearing **Restrict launches to machines with this tag**.
6. Click **Apply** to apply any changes you made and keep the window open, or click **Save** to apply changes and close the window.

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

Add or remove users in an application group

For detailed information about users, see Create application groups.

1. 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, click **Add**, and then specify the users you want to add. To remove users, select one or more users and then click **Remove**.
4. Click **Apply** to apply any changes you made and keep the window open, or click **Save** 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. Select **Applications** in the left pane.
2. On the **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.

   > **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 **Save** to apply changes and close the window.

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.

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

1. 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 **Scopes** page. Select or clear the check box next to a scope.
4. Click **Apply** to apply any changes you made and keep the window open, or click **Save** to apply changes and close the window.

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. 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 **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 **Save** 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 results in one or more applications no longer belonging to a group, you are warned that deleting that group also removes 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. 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 can create and manage folders for application groups if you have one of the following built-in roles:

- Cloud Administrator

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

- 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.

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 root 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 Web 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
```

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

Remote PC Access

September 13, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

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 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 this functionality:

- Ability to add machines by specifying OUs. This ability facilitates the addition of PCs in bulk.
- Automatic user assignment based on the user that logs into the office Windows PC. We support single user and multiple users assignments. By default, we automatically assign multiple users to the next unassigned machine. To restrict automatic assignment to a single user, sign in to Web Studio, go to **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.

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

> For on-premises deployments, Remote PC Access is valid only for Citrix Virtual Apps and Desktops 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 (formerly Citrix Virtual Apps and Desktops service) and Workspace Premium Plus.

Considerations

While all the technical requirements and considerations that apply to Citrix Virtual Apps and Desktops 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 previously mentioned 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 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 the available options:

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

  - Electronic Software Distribution (ESD) tools such as SCCM: Install VDAs using SCCM.
  - Deployment scripts: Install VDAs using scripts.
- Review the Remote PC Access security considerations.

> **Note:**
>
> When designing Remote PC Access, you must consider the number of physical monitors connected to the GPU on the remote PC and currently configured/operating. Even if the monitor is not used in the Citrix session, but is detected by the GPU, the monitor's presence is counted towards the maximum supported monitor limit by the GPU.

Machine catalog considerations

The type of machine catalog required depends on the use case:

- Remote PC Access machine catalog
  - Windows dedicated PCs
  - Windows dedicated multi-user PCs. This use case applies to physical office PCs that multiple users can access remotely in different shifts.
  - Pooled Windows PCs. This use case applies to physical PCs that multiple random users can access, such as computer labs.
- Single-session OS machine catalog
  - Static - Dedicated Linux PCs
  - Random - Pooled Linux PCs

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.

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

- If it is not easy to choose OUs to add machines to the machine catalog because of the OU structure, you don't have to select any OUs. You can use PowerShell to add machines to the catalog afterward. User auto-assignments continue to work if the desktop assignment is configured correctly in the Delivery Group. A sample script to add machines to the machine catalog along with user assignments is available in GitHub.
- 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:

- Use the Linux VDA on physical machines only in non-3D mode. 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.
- Use machine catalogs of type single-session OS for physical Linux machines.
- Automatic user assignment is not available for Linux machines.
- If users are already logged on to their PCs locally, attempts to launch the PCs from StoreFront™ fail.
- Power saving options are not available for 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 and Windows 11 only.
- The PC must have an active network connection. A wired connection is preferred for greater reliability and bandwidth.

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

- If using Wi-Fi, do the following:

  1. Set the power settings to leave the wireless adapter turned on.
  2. 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.
  3. 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:

  1. Disable the hibernate feature.
  2. Disable the sleep feature.
  3. Set the close lid action to **Do Nothing**.
  4. Set the "press the power button"action to **Shut Down**.
  5. 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:

  1. In the **Start** menu, select **Settings > System > Power & Sleep**, and set **Sleep** to **Never**.
  2. 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. When a user logs on to Citrix Workspace, 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.

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

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:

   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.

     > **Note:**
     >
     > For RemotePC installation, use `/physicalmachine` argument with `/remotepc` for VDA to behave as expected in certain user scenarios.

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

- 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.

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 `https://www.citrix.com/downloads/` 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.

Disable multiple user auto-assignments

On each Delivery Controller™, add the following registry setting:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Name: AllowMultipleRemotePCAssignments
- Type: DWORD
- Data: 0

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.

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

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

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.

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

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.

Session management logging

Remote PC Access now has logging capabilities that log when someone tries to access a PC with an active ICA® session. This allows you to monitor your environment for unwanted or unexpected activity and be able to audit such events if you need to investigate any incidents.

Events are logged using Windows Event Viewer and are in **Applications and Services > Citrix > Host-Core > ICA Service > Admin**.

There are three distinct events that are logged when using Remote PC Access.

Ctrl+Alt+Del event

This event appears when the local user presses Ctrl+Alt+Del on the console keyboard with an active remote session.

Event details

- Log name: Application and Services
- Event ID: 43, 44, 45
- Source: ICA Service

Event ID 43 This event ID appears when the SasNotification registry value does not exist or when the SasNotification registry value is 0.

- Message:

```
Ctrl+Alt+Del has been pressed on the endpoint.
The session management behavior is set to automatically
   disconnect the remote session.
```

Event ID 44 This event ID appears when the SasNotification registry value is 1 and the RpcaMode registry value is 1 or the RpcaMode registry value does not exist.

- Message:

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

```
Ctrl+Alt+Del has been pressed on the endpoint.
The session management behavior is set to notify the
    remote user. The user preference is set to remote user
    .
```

Event ID 45 This event ID appears when the SasNotification registry value is 1 and the RpcaMode registry value is 2.

- Message:

```
Ctrl+Alt+Del has been pressed on the endpoint.
The session management behavior is set to notify the
    remote user.
The user preference is set to local user.
```

Remote session disconnect event

This event appears when the remote session has been disconnected for various reasons.

Event details

- Log name: Application and Services
- Event ID: 46, 47, 48
- Source: ICA Service

Event ID 46 This event ID appears when the remote session has been disconnected and when the SasNotification registry value does not exist or the SasNotification registry value is 0.

- Message:

```
The remote session for <remoteUserName> has been
    disconnected.
```

Event ID 47 This event ID appears when the remote user agrees to disconnect the session and when the SasNotification registry value is 1 and the RpcaMode registry value is 1 or the RpcaMode registry value is 2 or the RpcaMode registry value does not exist.

- Message:

```
The remote session for <remoteUserName> has been
    disconnected because the user accepted the request to
    disconnect the session.
```

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

Event ID 48 This event ID appears when the remote user does not decline the disconnect request within the specific timeout period and when the SasNotification registry value is 1 and the RpcaMode registry value is 2.

- Message:

```
The remote session for <remoteUserName> has been
    disconnected because the user did not decline the
    disconnection request within the configured timeout
    period (<timeout period>).
```

Ctrl+Alt+Del pressed twice event This event appears when Ctrl+Alt+Del is pressed twice within 10 seconds.

Event details

- Log name: Application and Services
- Event ID: 49
- Source: ICA Service

Event ID 49 This event ID appears when Ctrl+Alt+Del is pressed twice within 10 seconds.

- Message:

```
The remote session for <remoteUserName> has been forcibly
    disconnected.
```

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 feature to work without dependencies on extra 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. For information on the SCCM-based Wake on LAN, see Wake on LAN –SCCM-integrated.

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

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

Configure Wake on LAN using Studio To create the Wake on LAN connection:

1. In the left pane, select the **Hosting** node.
2. Select **Add Connection and Resources**.
3. On 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
   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.

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

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*"

# 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
        $hypHc.HypervisorConnectionUid
 }
```

When the host connection is ready, run the following commands to retrieve the host connection's unique identifier:

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

```
$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.
- Wake on LAN can only be used to wake up PCs. It does not support other power actions, such as restart or shut down.
- After the Wake on LAN connection is created, it is visible in Web Studio. However, editing its properties within Web Studio is not supported if using Citrix Virtual Apps and Desktops on-premises.
- Magic packets are sent in one of the two ways:
    1. When a user tries to launch a session to their PC and the VDA is unregistered
    2. When an administrator manually sends a power on command from Web Studio or PowerShell

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

- Because the delivery controller is unaware of a PC's power state, Web Studio displays **Not Supported** under power state. The delivery controller uses the VDA registration state to determine whether a PC is on or off.
- Physical PCs:
  - VDA version 1912 or later
  - Windows 10. 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
- System Center Configuration Manager (SCCM) 2012 R2 or later

Configure SCCM-integrated Wake on LAN

Complete the following prerequisites:

1. Configure SCCM 2012 R2, 2016, or 2019 within the organization. Then deploy the SCCM client to all Remote PC Access machines, allowing time for the scheduled SCCM inventory cycle to run, or force one manually, if necessary.
2. For Wake Proxy support, enable the option in SCCM. For each subnet in the organization that contains PCs that use the Remote PC Access Wake on LAN feature, ensure that three or more machines can serve as sentinel machines.
3. For magic packet support, configure network routers and firewalls to allow magic packets to be sent, using either a subnet-directed broadcast or unicast.
4. Configure Wake on LAN in each PC's BIOS/UEFI settings.
5. Deploy the VDA to the physical PCs if you haven't done it already.

After you address the prerequisites, complete the following steps to allow the Delivery Controller to communicate with SCCM:

1. Create a host connection for SCCM. For more information, see Connections and resources.
   - Select **Microsoft Configuration Manager Wake on LAN** as the connection type.
   - The credentials entered must have access to the collections in the scope and must have the **Remote Tools Operator** role.
2. Select the connection in Web Studio, then select **Edit Connection**, and click **Advanced**.
3. Select the appropriate option for handling Wake on LAN:
   - If you are using Wake-up proxy, select the first option: **Microsoft System Center Configuration Manager Wake-up proxy**.
   - If you are using magic packets, select the second option: **Wake on LAN packets transmitted by the Delivery Controller**.

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

- Select the appropriate transmission method: **subnet-directed boradcasts** or **unicast**.

After you create the host connection, associate the connection with a Remote PC Access catalog:

- If you are creating a new Remote PC Access catalog, in the **Operating System** page of the catalog creation wizard, select **Remote PC Access** as the catalog type and choose the appropriate connection from the drop-down list.
- To add Wake on LAN to an existing Remote PC Access catalog:
  1. Go to the **Machine Catalogs** node in Web Studio, select the machine catalog, and then select **Edit Machine Catalog**.
  2. Select the **Power Management** tab and choose **Yes** to enable power management for the machine catalog.
  3. Select the appropriate connection from the drop-down list and click **OK**.

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`

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

- Name: ForceEnableRemotePC
- 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 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.

Cloud Connector Standalone Citrix Secure Ticketing Authority (STA) service

September 6, 2025

If using on-premises Site aggregation with Citrix Workspace™ or using Citrix Gateway Service with StoreFront, Cloud Connectors handle Secure Ticket Authority (STA) traffic for your Citrix Virtual Apps and Desktops™ site. The standalone 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. The standalone STA 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.

System requirements

- If using on-premises StoreFront™: Version 2311 or later
- Delivery Controller™: 2503 or later

Enable Standalone STA service

To enable the Standalone STA service, which enables the Citrix Gateway Service with on-prem Delivery Controllers and improves resiliency for on-prem site aggregation to the Citrix Workspace service, configure the following Registry Key:

1. On your Cloud Connectors, set the registry key `HKEY_LOCAL_MACHINE\Software\Citrix\XaXdCloudProxyPersist\StandaloneStaServiceForced` to 1.

Name: `StandaloneStaServiceForced`
Type: DWORD
Value: 1

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

Once the registry key is configured, restart the Citrix Remote Broker Provider Service for the change to take effect.

Important considerations

- For using Citrix Workspace and on-premises Citrix Gateway in an on-premises environment, see Aggregate Virtual Apps and Desktops in workspaces.
- For using on-premises StoreFront with Citrix Gateway Service, see Citrix Gateway Service for StoreFront.
- Configure on-premises StoreFront to use the FQDN of Cloud Connectors as STA servers. The on-premises NetScaler® Gateway vServer must include the complete list of Cloud Connectors configured as STAs, matching those specified in StoreFront.
- When you are using Citrix Workspace with an on-premises NetScaler Gateway vServer for ICA® proxy: Configure NetScaler Gateways to use all Cloud Connectors as the STA servers.

Limitations

- Dual STA ticket redemption is not supported for Citrix Workspace.
- If DaaS is not configured in your cloud tenant, Configuration Syncs will not happen, and 517 errors will be logged in the event log.

Publish content

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

You can publish an application that is simply a URL or UNC path to a resource, such as a Microsoft Word document or a web link. This feature is known as published content. The ability to publish content adds flexibility to how you deliver content to users. You benefit from the existing access control and management of applications. You can also specify whether to use local or published applications to open the content.

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

The published content appears just like other applications in StoreFront™ and Citrix Workspace™ app. Users access it in the same way they access applications. On the client, the resource opens as usual.

- If a locally installed application is appropriate, it is launched to open the resource.
- If a File Type Association has been defined, a published application launches to open the resource.

You publish content using the PowerShell SDK. You cannot use Web Studio to publish content. However, you can use Web Studio to edit application properties later, after they are published.

Configuration overview and preparation

Publishing content uses the `New-BrokerApplication` cmdlet with the following key properties. (See the cmdlet help for descriptions of all cmdlet properties.)

```
New-BrokerApplication –ApplicationType PublishedContent -
    CommandLineExecutable location -Name app-name -DesktopGroup delivery
    -group-name
```

The `ApplicationType` property must be `PublishedContent`.

The `CommandLineExecutable` property specifies the location of the published content. The following formats are supported, with a limit of 255 characters.

- HTML website address (for example, http://www.citrix.com)
- Document file on a web server (for example, `https://www.citrix.com/press/pressrelease.doc`)
- Directory on an FTP server (for example, `ftp://ftp.citrix.com/code`)
- Document file on an FTP server (for example, `ftp://ftp.citrix.com/code/Readme.txt`>)
- UNC directory path (for example, `file://myServer/myShare or \\\\\myServer\\myShare`)
- UNC file path (for example, `file://myServer/myShare/myFile.asf` or `\\myServer\myShare\myFile.asf`)

Ensure that you have the correct SDK.

- For Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments, download and install the Citrix Virtual Apps and Desktops Remote PowerShell SDK.
- For on-premises Citrix Virtual Apps and Desktops deployments, use the PowerShell SDK that is installed with the Delivery Controller. Adding a published content application requires a minimum version 7.11 Delivery Controller.

The following procedures use examples. In the examples:

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

- A machine catalog has been created.
- A delivery group named `PublishedContentApps` has been created. The group uses a multi-session OS machine from the catalog. The WordPad application has been added to the group.
- Assignments are made for the delivery group name, the `CommandLineExecutable` location, and the application name.

Get started

On the machine containing the PowerShell SDK, open PowerShell.

The following cmdlet adds the appropriate PowerShell SDK snap-in, and assigns the returned delivery group record.

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

If you are using Citrix DaaS, authenticate by entering your Citrix Cloud™ credentials. If there is more than one customer, choose one.

Publish a URL

After assigning the location and application name, the following cmdlet publishes the Citrix home page as an application.

```
1 $citrixUrl = "https://www.citrix.com/"
2 $appName = "Citrix Home Page"
3
4 New-BrokerApplication –ApplicationType PublishedContent –
     CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
     Uid
```

Verify success:

- Open StoreFront and log on as a user who can access applications in the PublishedContentApps delivery group. The display includes the newly created application with the default icon. To learn about customizing the icon, see https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.
- Click the **Citrix Home Page** application. The URL launches in a new tab in a locally running instance of your default browser.

Publish resources located at UNC paths

In this example, the administrator has already created a share named `PublishedResources`. After assigning the locations and application names, the following cmdlets publish an RTF and a DOCX file

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

in that share as a resource.

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf
    "
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
 –CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.
    docx"
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
 –CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
```

Verify success:

- Refresh your StoreFront window to see the newly published documents.
- Click the **PublishedRTF** and **PublishedDOCX** applications. Each document opens in a locally running WordPad.

View and edit PublishedContent applications

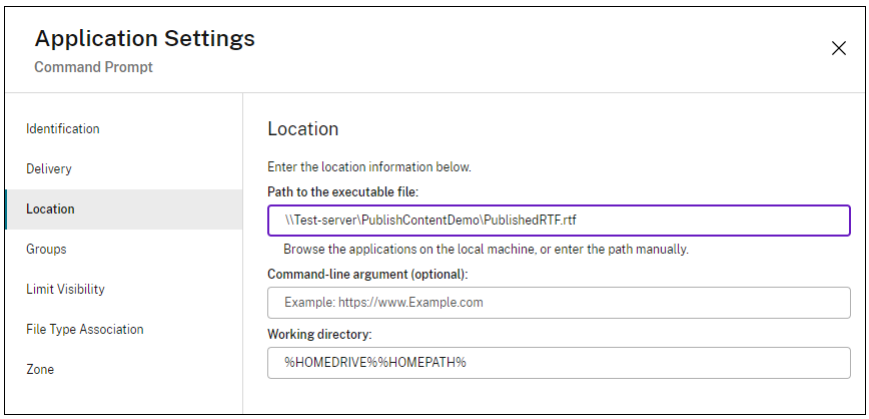
You manage published content using the same methods that you use for other application types.

To view and edit `PublishedContent` applications, follow these steps:

1. Sign in to Web Studio and select **Applications** in the left pane.
2. On the **Applications** tab, select a PublishedContent application, and then select **Properties**.

   Application properties (such as user visibility, group association, and shortcut) apply to the published content. However, you cannot change the command-line argument or working directory properties on the **Location** page.
3. To change the resource, modify the **Path to the executable file** field on that page.

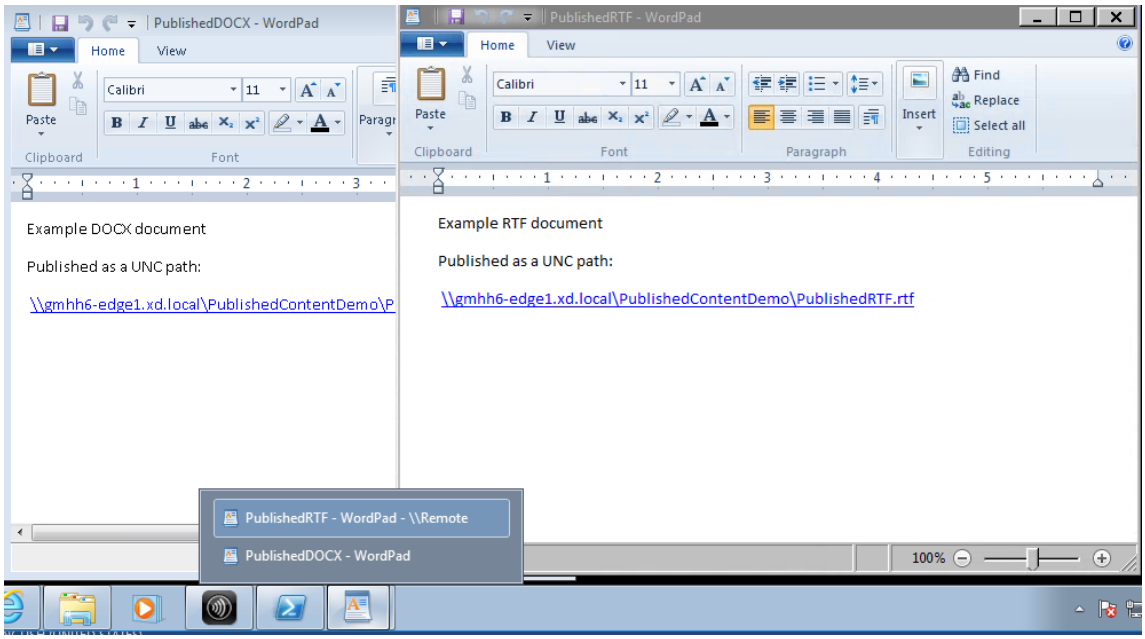
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. To use a published application to open a `PublishedContent` application (rather than a local application), follow these steps:

   In this example, the published WordPad application is edited to create a File Type Association for .rtf files.

   a) Turn on maintenance mode for the delivery group.
   b) Edit the **File Type Association** property.
   c) Turn off maintenance mode when you're done.
   d) Refresh StoreFront to load the File Type Association changes, and then click the **PublishedRTF** and **PublishedDOCX** applications. Notice the difference. **PublishedDOCX** still opens in the local WordPad. However, **PublishedRTF** now opens in the published WordPad due to the file type association.



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

For more information

- Create machine catalogs
- Create delivery groups
- Change application properties

Server VDI

September 13, 2025

Use the Server VDI (Virtual Desktop Infrastructure) feature to deliver a desktop from a server operating system for a single user.

- Enterprise administrators can deliver server operating systems as VDI desktops, which can be valuable for users such as engineers and designers.
- Service Providers can offer desktops from the cloud. Those desktops comply with the Microsoft Services Provider License Agreement (SPLA).

Support:

- In Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments, Server VDI is supported on Windows Server 2022, and Windows Server 2019.
- All Server VDI deployments support the user personalization layer technology.
- For Server VDI to work with TWAIN devices such as scanners, the Windows Server Desktop Experience feature must be installed.
- The following features cannot be used with Server VDI:
  - Hosted applications
  - Local App Access
  - Direct (non-brokered) desktop connections
  - Remote PC Access

Install and configure Server VDI

1. Prepare the Windows server for installation.
   - Use Windows Server Manager to ensure that the Remote Desktop Services role services are not installed. If they were previously installed, remove them. The VDA installation fails if these role services are installed.

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

- Ensure that the **Restrict each user to a single session** property is enabled. On the Windows server, edit the registry for the Terminal Server setting:

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

  `DWORD fSingleSessionPerUser = 1`

2. Use the Citrix Virtual Apps and Desktops installer's command line interface to install a VDA on a supported server or server master image, specifying the `/servervdi` option. (By default, the installer's graphical interface blocks the Windows single-session OS VDA on a server operating system. Using the command line overrides this behavior.) Use one of the following commands:

   - Citrix Virtual Apps and Desktops deployments:
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Citrix DaaS™ deployments:
     - `VDAWorkstationSetup.exe /servervdi`

   Other options:

   - Use `/controllers` to specify Delivery Controllers or Cloud Connectors.
   - Use `/enable_hdx_ports` to open ports in the firewall, unless the firewall is to be configured manually.
   - Use `/mastermcsimage` (or `/masterimage`) if you are installing the VDA on an image, and will use MCS to create server VMs from that image.
   - For all option details, see Install using the command line.

3. Create a machine catalog for Server VDI. In the catalog creation wizard:

   - On the **Operating System** page, select **Single-session OS**.
   - On the **Summary** page, specify a machine catalog name and description for administrators that clearly identifies it as Server VDI. This is the only indicator in Studio that the catalog supports Server VDI.

   When using search in Studio, the Server VDI catalog is displayed on the **Single-session OS Machines** tab, even though the VDA is installed on a multi-session machine.

4. Create a Delivery Group and select the Server VDI catalog you created.

If you did not specify Delivery Controllers or Cloud Connectors during VDA installation, remember to specify them afterward. For details, see VDA registration.

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

User personalization layer

September 13, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

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.

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. Don't 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.

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:

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

- 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.

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 a 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 Server 2019 (Azure Files supported)
- Windows Server 2022 (Azure Files supported)

For Citrix Virtual Apps and Desktops 7, the use of Azure Files with User personalization layers is supported on Windows Server 2022, Windows Server 2019, and Windows 10 clients.

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

> **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 the user personalization layer with multi-session server operating systems, only with single-session server systems. User personalization layer is supported for non-persistent desktops only.

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** policy. See **Step 5: Create delivery group custom policies**, under **Optional: Click Select next to User Layer Size in GB.**

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

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**:

- 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 Web 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 exhibits unexpected behaviors and instability.

To deploy the user personalization layer feature, complete the following steps in this order:

- Step 1: Verify the 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 in 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

Ensure 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.

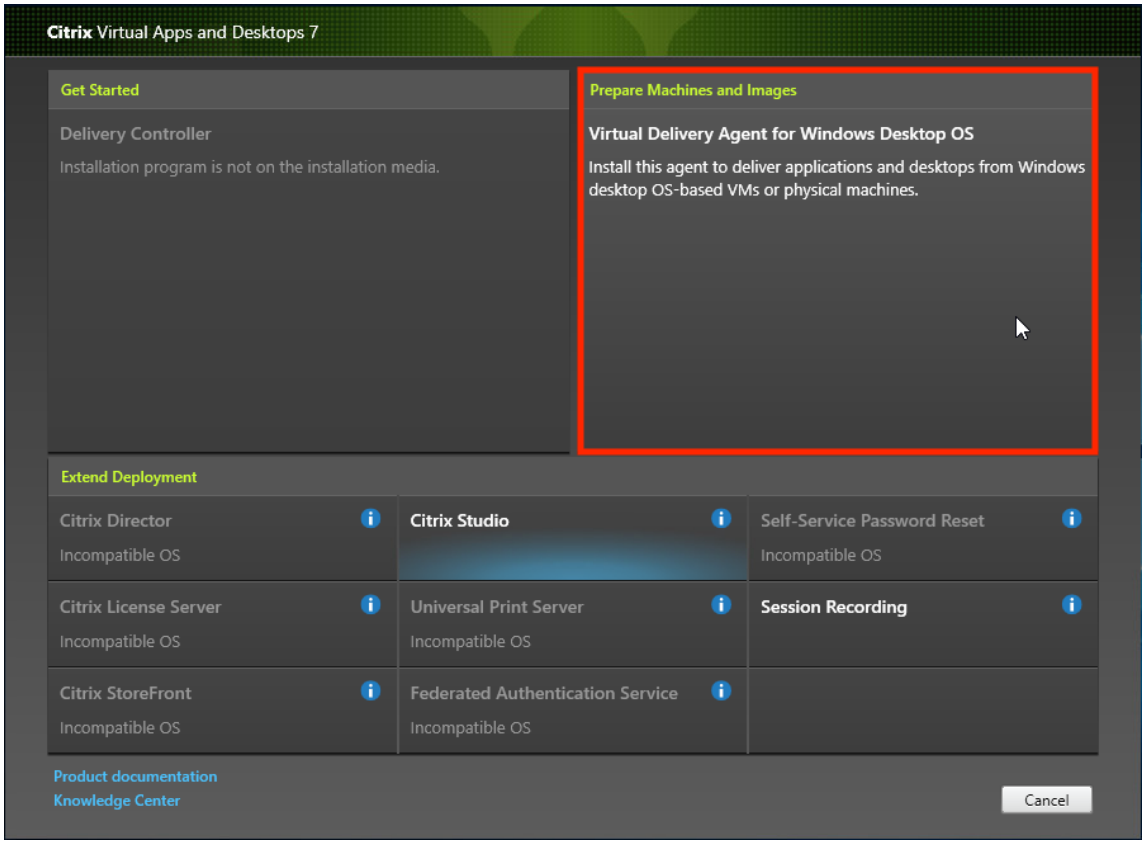
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Prepare your master image

To prepare your master image:

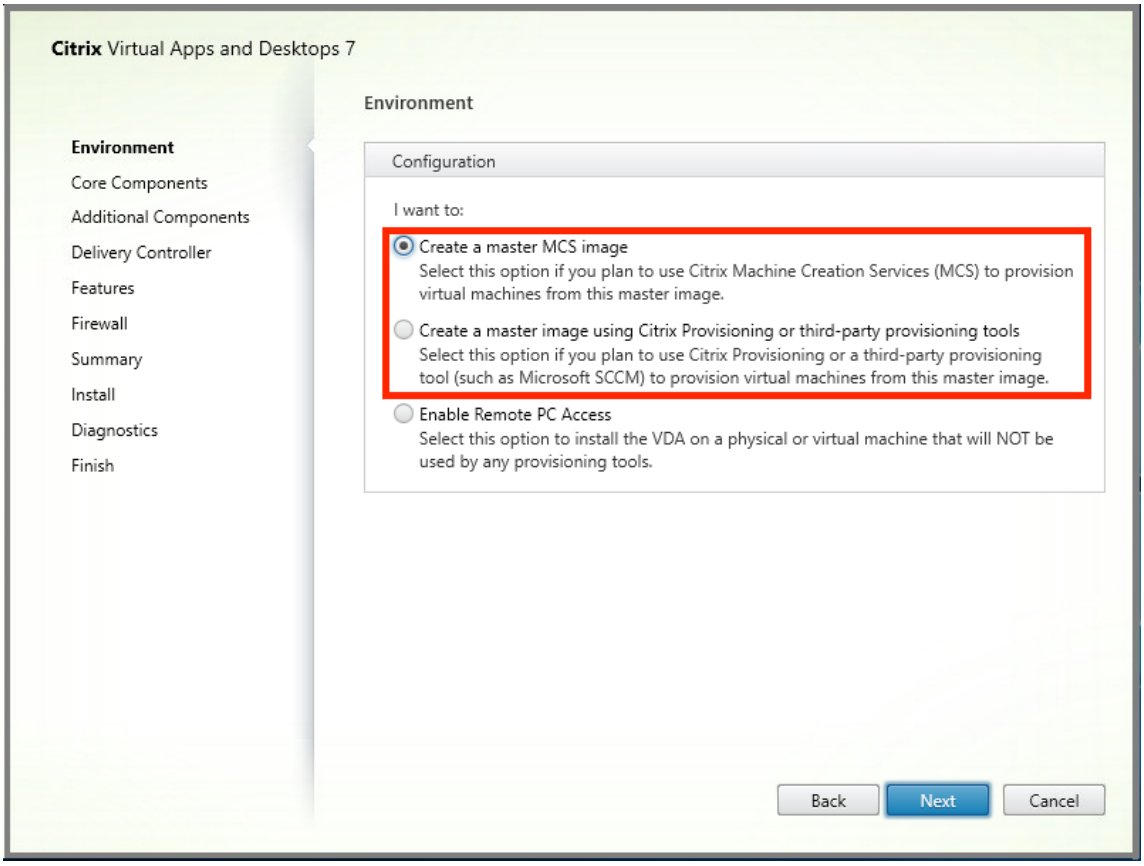
1. Locate the master image. Install your organization's enterprise applications and any other apps your users generally find useful.
2. If you are deploying Server VDI, follow the steps in the Server VDI article. Be sure to include the optional component, the **User personalization layer**. For details, 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 **Virtual Delivery Agent for Windows Desktop OS** tile:



    a) **Environment:** Select either **Create a master MCS image** or **Create a master image using Citrix Provisioning or third-party provisioning tools**.

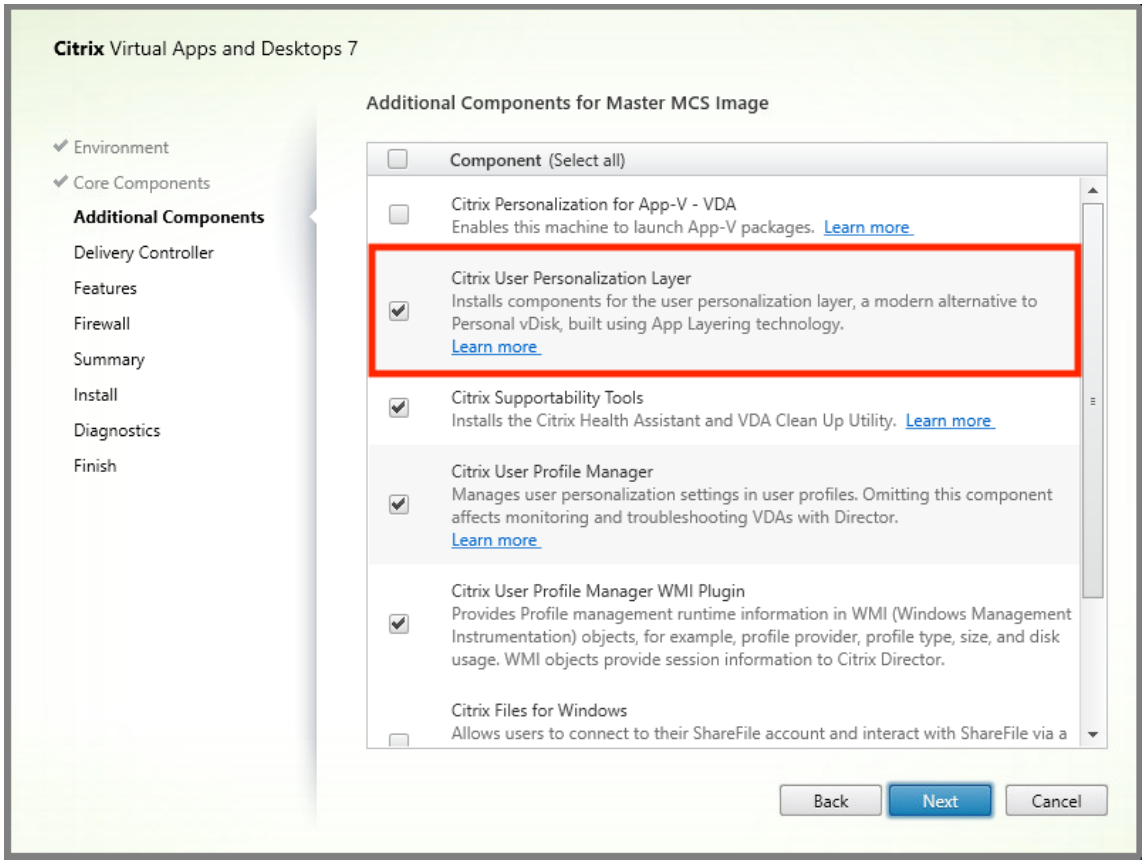
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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, configure 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 Web Studio.

> **Note:**
>
> If you simply want 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

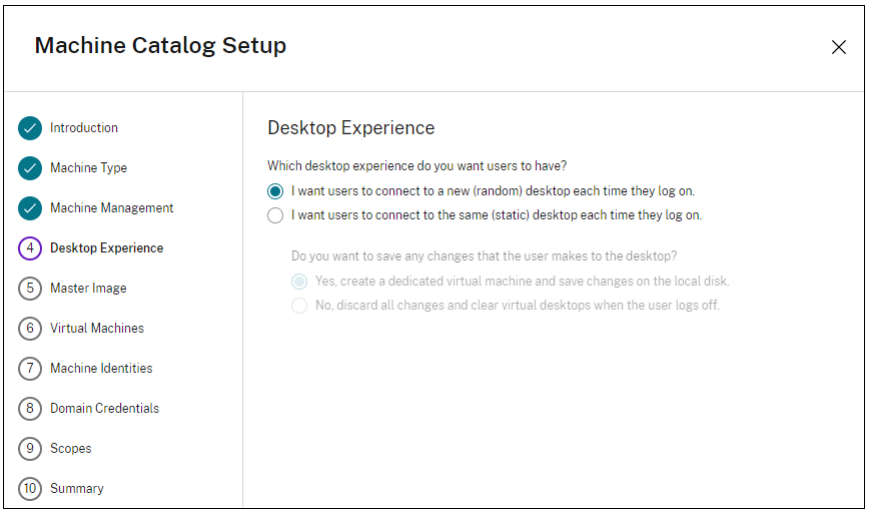
In Web Studio, follow the steps to create a machine catalog. Use the following options during catalog creation:

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.

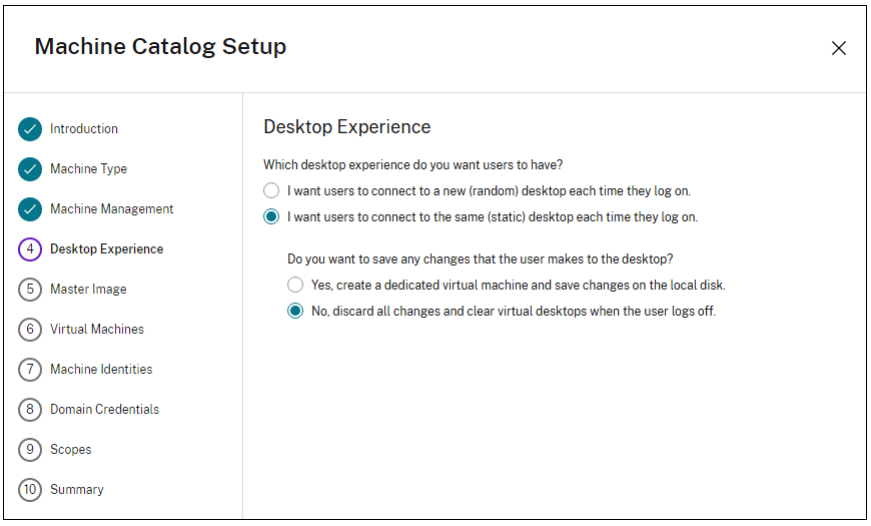
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:



> **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.

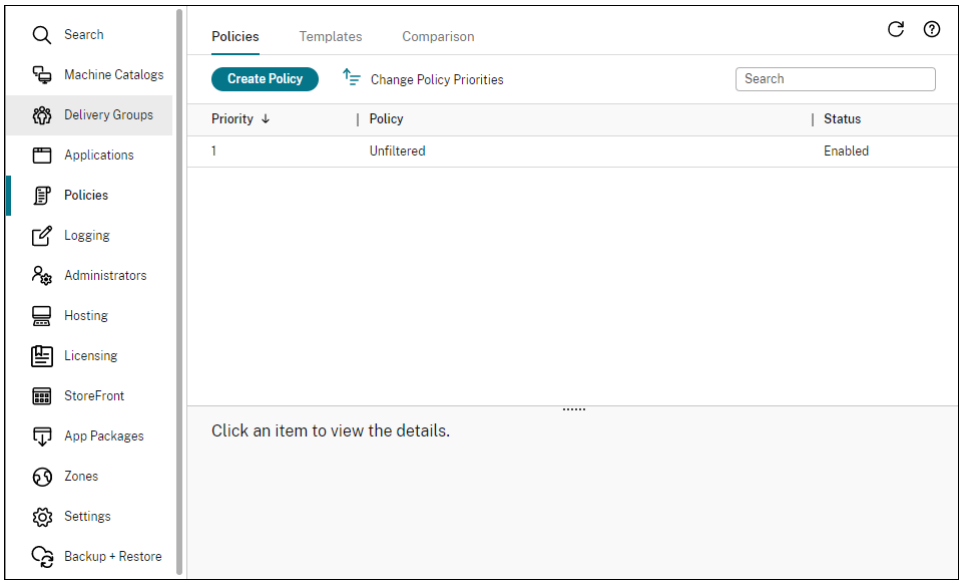
Step 5: Create delivery group custom policies

To enable the 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 Web Studio and assign them to your delivery group.

1. Sign in to Web Studio and select **Policies** in the left pane:

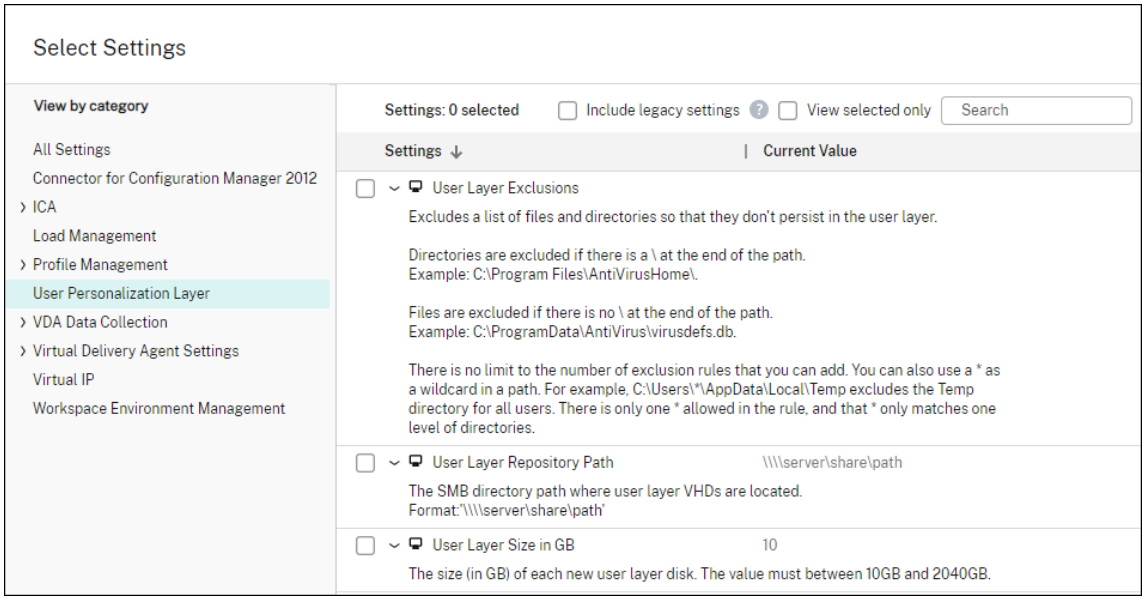


2. Select **Create Policy** in the action bar. The Create Policy window appears.
3. Type `user layer` into the search field. The following three policies appear in the list of available policies:

    - User Layer Exclusions
    - User Layer Repository Path
    - User Layer Size GB

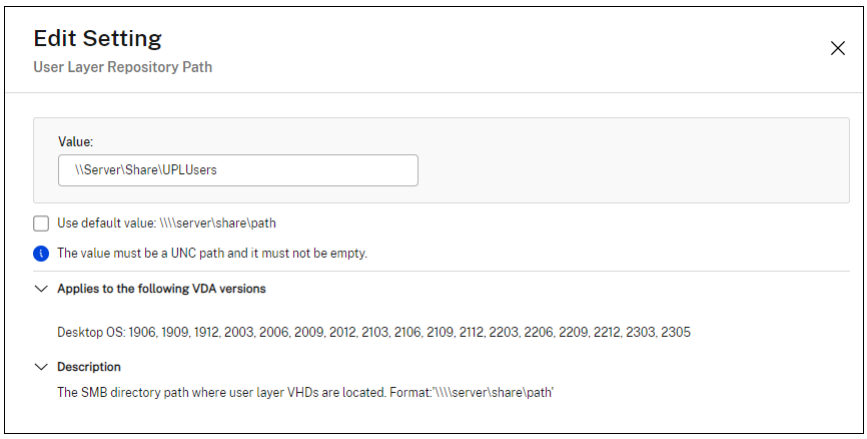
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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 is: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



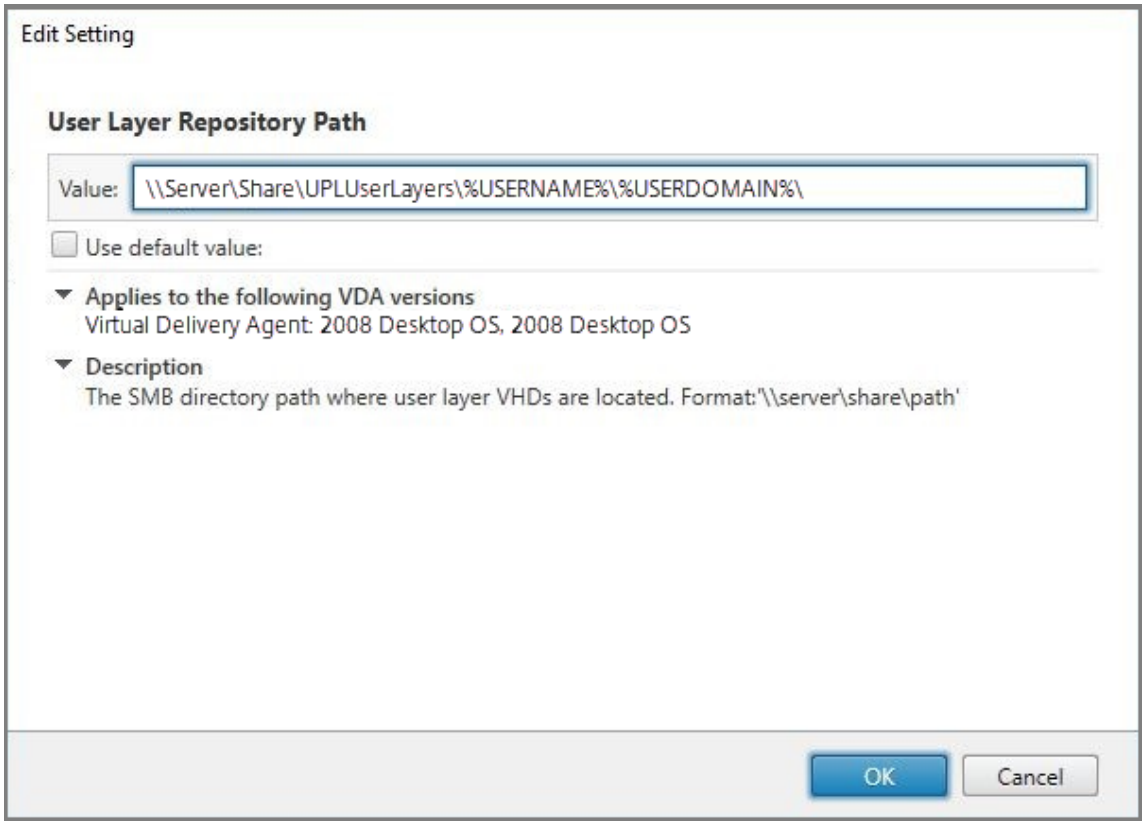
You can customize the path using the %USERNAME% and %USERDOMAIN% variables, machine environment variables, and Active Directory (AD) attributes. When expanded, these variables

© 1997–2026 Citrix Systems, Inc. All rights reserved.

result in explicit paths.

Example of environment variables:

- **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`

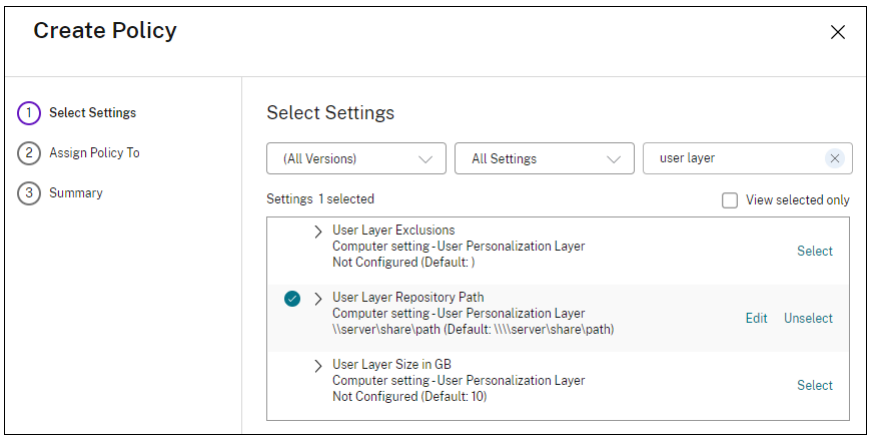


Example of custom AD attributes:

- 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)

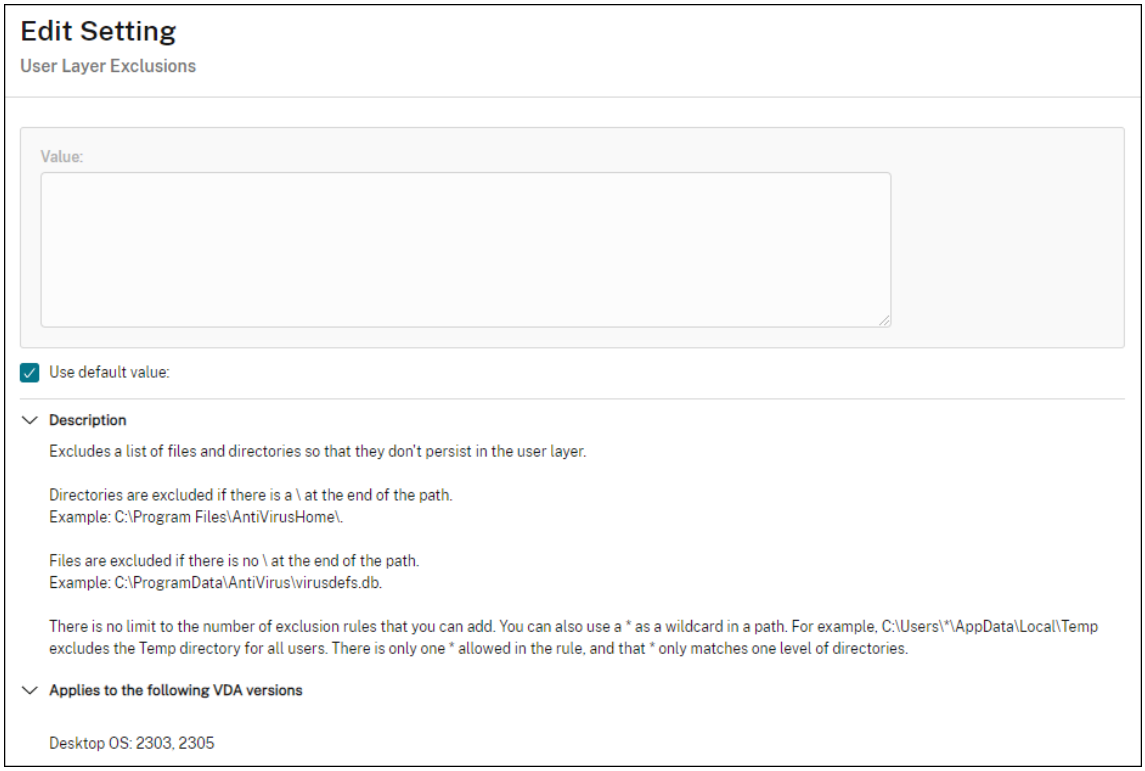
6. Optional: Mark the check box next to **User Layer Size in GB** and click **Edit**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



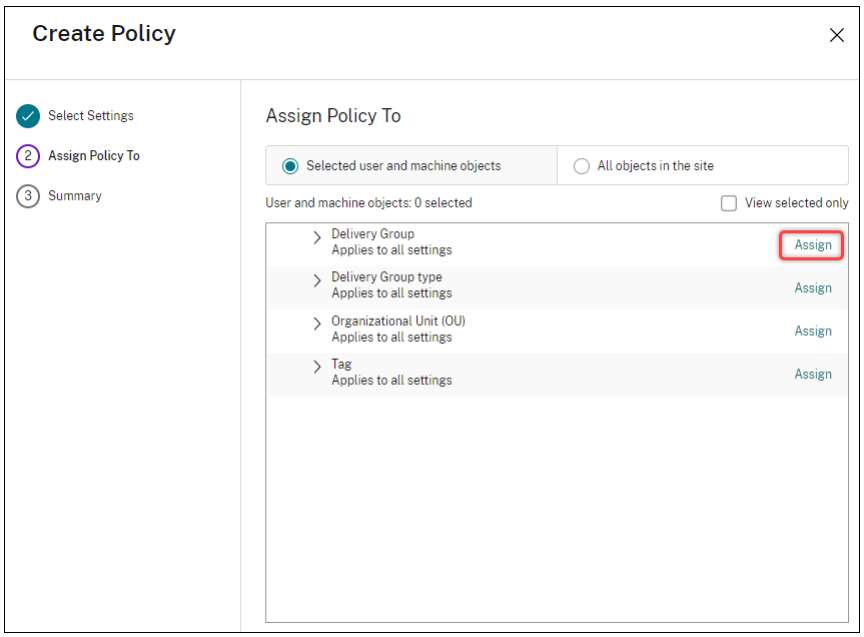
The Edit Settings window appears.

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**.

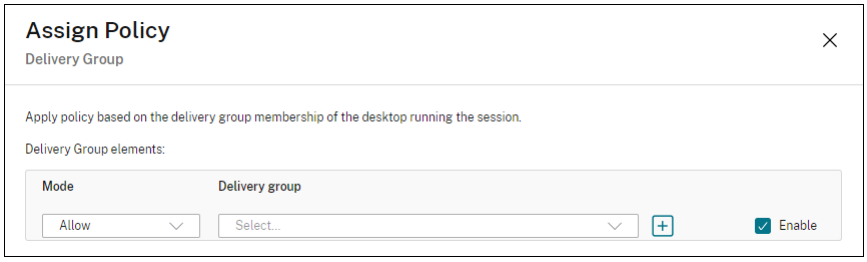


9. Optional: Specify the files and folders to exclude, then click **Save**. For more information, see the Citrix App Layering documentation.
10. Click **Next** to configure the users and machines to which you want to assign. Click the **Delivery Group Assign** link highlighted in this image:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

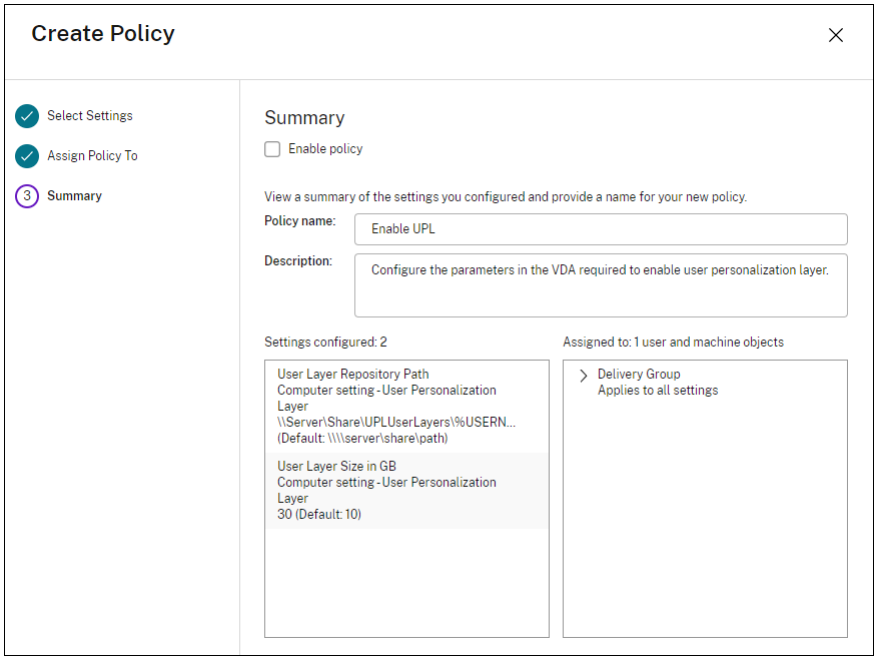


11. In the **Delivery Group** menu, select the delivery group created in the previous section. Click **OK**.



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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

User Layer/UPL space reclamation

You can use **User Layer/UPL space reclamation** to automatically compress the VHDX files every time the user logs off.
For more information, see User Layer/UPL space reclamation

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 that you need.
- Do *not* configure the user personalization layer feature with persistent machine catalogs.
- Do *not* use Session hosts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Do *not* update the machine catalog with an image running a new OS install (even the same version of Windows 10). The 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 or 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 Policies (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.

  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 might have issues.
- Custom certificates do not persist when UPL is enabled in a pure Azure AD 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.

Remove components

September 6, 2025

To remove components, Citrix® recommends using the Windows feature for removing or changing programs. Alternatively, you can remove components using the command line, or a script on the installation media.

When you remove components, prerequisites are not removed, and firewall settings are not changed. For example, when you remove a Delivery Controller™, the SQL Server software and the databases are not removed.

If you upgraded a Controller from an earlier deployment that included Web Interface, you must remove the Web Interface component separately. You cannot use the installer to remove Web Interface.

For information about removing features not mentioned below, see the feature's documentation.

Preparation

Before removing a Controller, remove it from the site. For details, see Remove a Controller.

Close Studio and Director before removing them.

Remove components using the Windows feature for removing or changing programs

From the Windows feature for removing or changing programs:

- To remove a Controller, Studio, Director, License Server, or StoreFront, right-click **Citrix Virtual Apps *version*** or **Citrix Virtual Apps and Desktops™ *version*** and select **Uninstall**. The installer launches. Select the components to be removed.

  Alternatively, you can remove StoreFront™ by right-clicking **Citrix StoreFront** and selecting **Uninstall**.

- To remove a VDA, right-click **Citrix Virtual Delivery Agent *version*** and select **Uninstall**. The installer launches and you can select the components to be removed. The machine restarts automatically after the removal, by default.

- To remove the Universal Print Server, right-click **Citrix Universal™ Print Server** and select **Uninstall**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remove core components using the command line

From the \x64\XenDesktop Setup directory, run the XenDesktopServerSetup.exe command.

- To remove one or more components, specify the /remove and /components options.
- To remove all components, specify the /removeall option.

For command and parameter details, see Install using the command line.

For example, the following command removes Web Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
webstudio
```

While upgrading if you have installed License Server first using the commands \x64\Licensing\CitrixLicensing.exe /quiet or \x64\Licensing\CitrixLicensing.exe /quiet /l install.log and then installed the core components, then follow the same order to uninstall:

1. Uninstall License Server using the command line:

```
1 CitrixLicensing.exe /quiet /uninstall /l uninstall.log
```

2. Uninstall components using the GUI or command line. For information, see Remove components.

If you uninstall the License Server and components using the command line XenDesktopServerSetup.exe or removeall, then clean up the registry entry and the remaining files.

To clean registry entries :

1. Search for the registry key Citrix Licensing and delete that entry. Mostly, you can find the entry in the following location:

```
1 "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\
     Windows\CurrentVersion\Uninstall\
```

2. Delete the folder pointed by the **Uninstall String** in the registry key.

Remove VDAs using the command line

From the \x64\XenDesktop Setup directory, run the XenDesktopVdaSetup.exe command.

- To remove one or more components, use the /remove and /components options. For example, to remove the VDA and Citrix Workspace app, use /remove /components vda,plugin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The `/removeall` option removes only the VDA. It does not remove the Citrix Workspace app.

For command and parameter details, see Install using the command line.

The machine restarts automatically after the removal, by default.

To remove VDAs using a script in Active Directory, see Install or remove VDAs using scripts.

Upgrade and migrate

July 31, 2026

> **Note:**
>
> File based licensing system, traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license Citrix on-premises components after April 15, 2026. To remain supported, your Citrix Virtual Apps and Desktops deployment must be on a LAS compatible version. The minimum required CVAD versions that are LAS compatible are:
>
> - CVAD 2203 LTSR CU7
> - CVAD 2402 LTSR CU3
> - CVAD 2507 LTSR
> - CVAD 2411
>
> If you have questions or concerns, contact Customer Care. Citrix might limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix might have at law or equity. These requirements don't apply where prohibited by law or regulation.

> **Note:**
>
> - **The "Version Intersect"Warning**
>
> Please be advised that different LTSR versions often overlap in their maintenance cycles. Before initiating an upgrade, you must verify the **Release Date** of both your current Cumulative Update (CU) and your target LTSR (or its subsequent CU).
> If your current environment's release date is **later** than the target LTSR or LTSR CU release date, Citrix strongly recommends waiting for the next CU of the newer LTSR. Proceeding otherwise may cause older code to overwrite existing security updates, stability patches and feature enhancements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - **The "Unsupported State"Clause**
>
>   Attempting to upgrade to a version with an earlier release date is technically considered a **downgrade of core components**. This specific configuration may result in a '**Partial Success**' status.

Introduction

Upgrading changes your deployment to the Citrix Virtual Apps and Desktops™ 7 **Current Release (CR)** without having to set up new machines or sites. This is known as an in-place upgrade.

Upgrading gives you access to the latest features and technologies that you're eligible for. Upgrades can also contain fixes, clarifications, and enhancements from earlier versions.

Upgrade overview

1. Review the Upgrade a deployment article before beginning the upgrade. This is the primary information source for learning how to prepare for and implement an upgrade.
2. Ensure that your current Customer Success Services dates are valid and have not expired. For more information, see the Customer Success Services renewal licenses article.
3. Complete the preparation guidance.
4. Run installers to upgrade core components.
5. Upgrade the system databases and the site.
6. Upgrade VDAs on images (or directly on machines).
7. Upgrade other components.

Each preparation and upgrade step is detailed in Upgrade a deployment.

Versions you can upgrade

You can upgrade to Citrix Virtual Apps and Desktops 2507 LTSR from:

- Virtual Apps and Desktops 2402 LTSR with or without CUs, up to and including CU2
- Virtual Apps and Desktops 2203 LTSR with or without CUs, up to and including CU7
- Currently supported CR versions of Citrix Virtual Apps and Desktops

> Note:
>
> Before initiating the upgrade process, we recommend that you test the upgrade in a controlled environment and verify that it meets your specific requirements. Additionally, we advise reviewing all relevant product documentation, including the deprecation list and known issues, to ensure a seamless transition. This approach helps mitigate potential disruptions to production

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> systems and enhances the overall upgrade experience.
>
> For more information on the list of supported versions, see Product Matrix.

Frequently asked questions

This section answers some commonly asked questions about upgrading Citrix Virtual Apps and Desktops.

- **What is the correct order to upgrade my Virtual Apps and Desktops environment?**

  For an illustration and description of the recommended upgrade sequence, see Upgrade sequence and Upgrade procedure.

- **My site has several Delivery Controllers (in different zones). What happens if I upgrade only some of them? Am I required to upgrade every Controller in the site during the same maintenance window?**

  The best practice is to upgrade all Delivery Controllers during the same maintenance window, as various services on each Controller communicate with each other. Keeping different versions might cause issues. During a maintenance window, we recommend you upgrade half of the Controllers, upgrade the site, and then upgrade the remaining Controllers. For details, see the Upgrade procedure.

- **Can I go directly to the latest version, or do I have to do incremental upgrades?**

  You can almost always upgrade to the latest version and skip intermediate releases, unless explicitly stated in the **What's new** article for the version you're upgrading to.
  See the [Upgrade Guide](/en-us/upgrade).

- **Can a customer upgrade from a Long Term Service Release (LTSR) environment to a Current Release?**

  Yes. Customers are not required to remain on a Long Term Service Release for an extended period. Customers can move an LTSR environment to a Current Release, based on business requirements and features.

- **Are mixed versions of components allowed?**

  Within each site, Citrix recommends upgrading all components to the same version. Although you can use earlier versions of some components, all features in the latest version might not be available. For more information, see Mixed environment considerations.

- **How often must a Current Release be upgraded?**

  Current Releases reach End of Maintenance (EOM) 6 months after the release date. Citrix recommends that customers adopt the latest Current Release. Current Releases reach End of Life (EOL) 18 months after the release date.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Current Release Lifecycle.

- **What is recommended: upgrade to LTSR or CR?**

  Current Releases (CRs) deliver the latest and most innovative app, desktop, and server virtualization features and functionality. This allows you to stay on leading-edge technology and ahead of your competition.

  Long Term Service Releases (LTSRs) are ideal for large enterprise production environments that prefer to retain the same base version for an extended period.

  For more information, see Servicing Options.

- **Do I need to upgrade my licenses?**

  Ensure that the current license date has not expired, and is valid for the release you are upgrading to. See CTX111618. For information about renewal, see Customer Success Services renewal licenses.

- **How long does an upgrade take?**

  The time required to upgrade a deployment varies, depending on the infrastructure and network. So, we can't provide an exact time.

- **What are the best practices?**

  Ensure that you understand and follow the preparation guidance.

- **Which operating systems are supported?**

  The System requirements article for the version you're upgrading to lists the supported OSs.

  If your current deployment uses operating systems that are no longer supported, see Earlier operating systems.

- **Which versions of VMware vSphere (vCenter + ESXi) are supported?**

  CTX131239 lists the supported hosts and versions, plus links to known issues.

- **When does my version go EOL?**

  Check the Product Matrix.

- **What are the known issues with the latest release?**

  - Citrix Virtual Apps and Desktops
  - StoreFront
  - Citrix Provisioning
  - Citrix License Server
  - Citrix Workspace app for Windows

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information

Long Term Service Release (LTSR)

Long Term Service Release (LTSR) deployment updates use Cumulative Updates (CUs). A CU updates baseline components of the LTSR, and each CU includes its own metainstaller.

Each CU has dedicated documentation. For example, for the 2203 LTSR, check the link on that LTSR's **What's new** page for the latest CU. Each CU page includes supported version information, instructions, and a link to the CU download package.

Migrate

Migrate to the cloud

You can use the Automated Configuration tool for Citrix Virtual Apps and Desktops to migrate your on-premises deployment onto the cloud. For more information, see Migrate to Cloud.

Legacy migration

Migrating moves data from an earlier deployment to a newer version. The process includes installing newer components and creating a new site, exporting data from the older farm, and then importing the data to the new site.

There are no supported tools or scripts for migrating XenApp and XenDesktop versions, or migrating earlier Citrix Virtual Apps and Desktops versions. *Upgrading* is supported for the Citrix Virtual Apps and Desktops versions described in this product documentation.

For earlier XenApp 6.x migration content, see the following. Neither the scripts nor the articles are supported or maintained.

- Open source migration scripts for XenApp 6.x versions are available at https://github.com/citrix/xa65migrationtool. Citrix does not support or maintain these migration scripts
- Changes in 7.x
- Upgrade a XenApp 6.5 worker to a new VDA
- Migrate XenApp 6.x

Upgrade a deployment

January 30, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> File based licensing system, traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license Citrix on-premises components after April 15, 2026. To remain supported, your Citrix Virtual Apps and Desktops deployment must be on a LAS compatible version. The minimum required CVAD versions that are LAS compatible are:
>
> - CVAD 2203 LTSR CU7
> - CVAD 2402 LTSR CU3
> - CVAD 2507 LTSR
> - CVAD 2411
>
> If you have questions or concerns, contact Customer Care. Citrix might limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix might have at law or equity. These requirements don't apply where prohibited by law or regulation.

Introduction

> **Note:**
>
> This article covers upgrades for deployments involving Web Studio. For information about upgrades involving Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops™ 7 2212 or earlier.

You can upgrade certain deployments to newer versions without having to first set up new machines or sites. This is called an in-place upgrade.

To learn which Citrix Virtual Apps and Desktops versions you can upgrade, see the Versions you can upgrade.

Before you upgrade to any of the Citrix Virtual Apps and Desktops releases, ensure that your current Customer Success Services dates are valid and have not expired. For more information, see the Customer Success Services renewal licenses article.

To start an upgrade, you run the installer from the new version to upgrade previously installed core components, VDAs, and certain other components. Then you upgrade the database and the site.

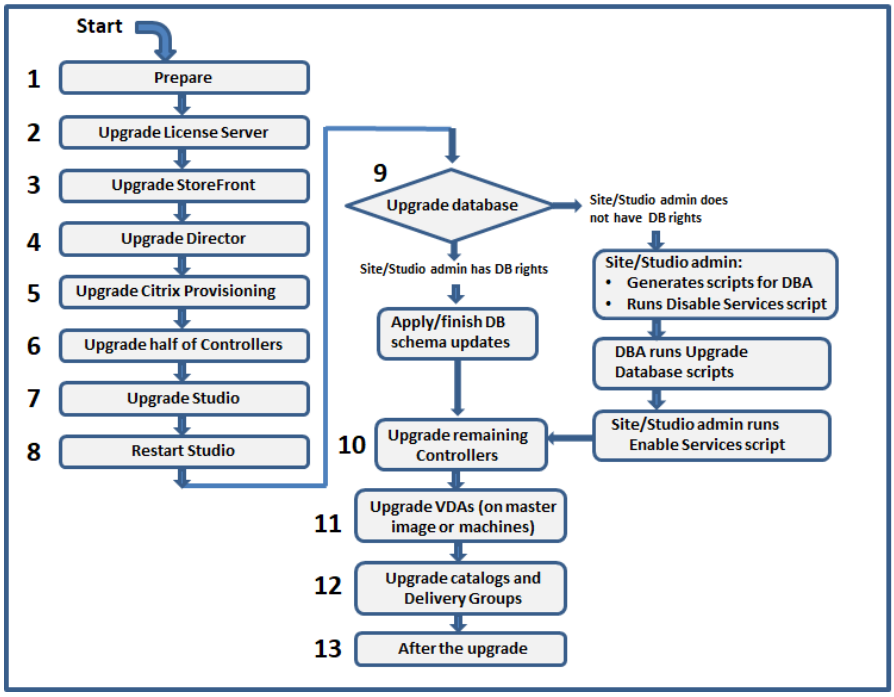
You can upgrade any component that can be installed with the full-product installer (and the standalone VDA installers), if there is a newer version provided. For other components that are not installed with the full-product installer (such as Citrix Provisioning™ and Profile Management), see that component's documentation for guidance. For host upgrades, see the appropriate documentation.

Review all the information in this article before beginning an upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade sequence

The following diagram shows the steps the upgrade sequence. Upgrade procedure contains details of each step in the diagram.



> **Note:**
>
> To avoid failures, you must upgrade all Delivery Controllers and database before performing any of the provisioning and delivery group related tasks such as creating a new machine catalog, deleting a machine catalog, updating a machine in a delivery group, and so on.

Hybrid Rights Licenses

Hybrid Rights licenses are term-based subscription licenses that are provided, in addition to the cloud service subscription, when a customer transitions or trades up from a perpetual license to a cloud service subscription. You can also purchase a Hybrid Rights add-on with your DaaS subscriptions.

If you have a Hybrid Rights license with a SaaS attribute, when you upgrade to Citrix Virtual Apps and Desktops LTSR 2203 and later, you become eligible to access capabilities not available with Citrix Virtual Apps and Desktops LTSR 1912. These capabilities include provisioning and hosting workloads in public clouds, such as Microsoft Azure, AWS EC2, and Google Cloud. Before deploying the new license file, update your License Server to the most recent version. Failure to meet this prerequisite will block the Citrix Virtual Apps and Desktops site upgrades and site creation.

If you have access to a Hybrid Rights license with no SaaS attribute, follow these steps to get access to the new Hybrid Rights license with SaaS attribute:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - You get an email with a new license code. For more information see, Use license access code.
> - Your existing licenses are rescinded. Rescinded licenses must be deleted from License Servers followed by new license installation. For more information, see Deleting license files.

1. Go to citrix.com Manage Licenses portal and download the new Hybrid Rights license file with cloud provisioning rights enabled (SaaS attribute). For more information, see Download licenses. The following image shows the Hybrid Rights license file with the SaaS attribute in the Increments section.

2. Install the Hybrid Rights license file on the License Server. For more information, see Install licenses.
3. If there is a change in license editions or model, make sure you run the broker command to set the edition and the model and then start the in-place upgrade. For more information about Broker commands, see Broker PowerShell SDK section.

For more information about public cloud support with Citrix Virtual Apps and Desktops Current Releases and Long Term Service Releases, see CTX270373.

Upgrade procedure

Most of the main product components can be upgraded by running the product installer on the machine containing the component.

If one machine contains more than one component (for example, Studio and License Server), all components on that machine are upgraded, if the product media contains newer versions of their software.

To use the installers:

- To run the full product installer's graphical interface, log on to the machine and then insert the media or mount the ISO drive for the new release. Double-click **AutoSelect**.
- To use the command-line interface, issue the appropriate command. See Install using the command line.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Prepare

Before you begin an upgrade, make sure you're ready. Read and complete any necessary tasks:

- Remove PVD, AppDisks™, and unsupported hosts
- VDAs that have PvD or AppDisk components
- Limitations
- Mixed environment considerations
- Earlier operating systems
- Preparation
- Preliminary site tests
- SQL Server version check

Step 2: Upgrade License Server

If the installation has a new version of the Citrix License Server software, upgrade this component first before any other components.

If you have not yet determined whether your License Server is compatible with the new version, it is essential that you run the installer on the License Server before upgrading any other core components.

Step 3: Upgrade StoreFront™

If the installation media contains a new version of the StoreFront software, run the installer on the machine containing the StoreFront server.

- In the graphical interface, choose **Citrix StoreFront** from the **Extend deployment** section.
- From the command line, run `CitrixStoreFront-x64.exe`, which is available in the Citrix Virtual Apps and Desktops installation media's `x64` folder.

Step 4: Upgrade Director

If the installation media contains a new version of the Director software, run the installer on the machine containing Director.

Step 5: Upgrade Citrix Provisioning

The Citrix Provisioning installation media is available separately from the Citrix Virtual Apps and Desktops installation media. To learn how to install and upgrade Citrix Provisioning server and target device software, see the Citrix Provisioning product documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 6: Upgrade half of Delivery Controllers

For example, if your site has four Controllers, run the installer on two of them.

Leaving half of the Controllers active allows users to access the site. VDAs can register with the remaining Controllers. There might be times when the site has reduced capacity because fewer Controllers are available. The upgrade causes only a brief interruption in establishing new client connections during the final database upgrade steps. The upgraded Controllers cannot process requests until the entire site is upgraded.

If your site has only one Controller, it is inoperable during the upgrade.

Preliminary site tests run on the first Controller, before the actual upgrade starts. For details, see Preliminary site tests.

Step 7: Upgrade Studio

If you haven't already upgraded Web Studio (because it was on the same machine as another component), run the installer on the machine containing Studio.

> **Note:**
>
> After you upgrade Web Studio, the version information might not update immediately. You might be prompted to upgrade Web Studio even though it's already up to date. To address the issue, go to the Web Studio server, open Internet Information Services (IIS) Manager, navigate to Start Page > Sites > Default Web Site, and select **Restart** in the **Manage Website** pane.

Step 8: Restart Studio

Restart the upgraded Web Studio. The upgrade process automatically resumes.

Step 9: Upgrade database and site

> **Note:**
>
> To avoid failures, you must upgrade all Delivery Controllers and database before performing any of the provisioning and delivery group related tasks such as creating a new machine catalog, deleting a machine catalog, updating a machine in a delivery group, and so on.

Check Preparation for the permissions required to update the schema of the SQL Server databases.

- If you have sufficient permission to update the SQL Server database schema, you can initiate an automatic database upgrade. Continue with Upgrade the database and site automatically.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you do not have sufficient database permissions, you can initiate a manual upgrade that uses scripts, and proceed with the help of your database administrator (someone who has the required permissions). For a manual upgrade, the Studio user generates the scripts and then runs the scripts that enable and disable services. The database administrator runs other scripts that update the database schema, using either the SQLCMD utility or the SQL Server Management Studio in SQLCMD mode. Continue with Upgrade the database and site manually.
- If you have a multi-zone deployment and want to upgrade the database and site automatically, Citrix recommends that the dbschema upgrade must be performed in the same zone that hosts the SQL server databases of the site. Otherwise, upgrading the database and site automatically might fail.

Citrix strongly recommends that you back up the database before upgrading. See CTX135207. During a database upgrade, product services are disabled. During that time, Controllers cannot broker new connections for the site, so plan carefully.

Upgrade the database and site automatically

1. Start the newly upgraded Studio.
2. Indicate that you want to start the site upgrade automatically and confirm that you are ready.

The database and site upgrade proceeds.

Upgrade the database and site manually

1. Start the newly upgraded Studio.
2. Indicate that you want to upgrade the site manually. The wizard checks for License Server compatibility and requests confirmation.
3. Confirm that you have backed up the database.

   The wizard generates and displays the scripts and a checklist of upgrade steps. If a database's schema has not changed since the product version being upgraded, that script is not generated. For example, if the logging database schema does not change, the `UpgradeLoggingDatabase.sql` script is not generated.
4. Run the following scripts in the order shown.

   - `DisableServices.ps1`: The Studio user runs this PowerShell script on a Controller to disable product services.
   - `UpgradeSiteDatabase.sql`: The database administrator runs this SQL script on the server containing the Site database
   - `UpgradeMonitorDatabase.sql`: The database administrator runs this SQL script on the server containing the Monitor database.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `UpgradeLoggingDatabase.sql`: The database administrator runs this SQL script on the server containing the Configuration Logging database. Run this script only if this database changes (for example, after applying a hotfix).
- `EnableServices.ps1`: The Studio user runs this PowerShell script on a Controller to enable product services.

After the database upgrade completes and product services are enabled, Studio automatically tests the environment and configuration, and then generates an HTML report. If problems are identified, you can restore the database backup. After resolving issues, you can upgrade the database again.

5. After completing the checklist tasks, click **Finish upgrade**.

Step 10: Upgrade remaining Delivery Controllers

From the newly upgraded Studio, select the **Citrix Studio** *site-name* in the navigation pane. On the **Common Tasks** tab, select **Upgrade remaining Delivery Controllers**.

> **Note:**
>
> To make **Upgrade remaining Delivery Controllers** available, create at least one machine catalog and one delivery group for the site.

After completing the upgrade and confirming completion, close and then reopen Studio. Studio might prompt for an extra site upgrade to register the Controller's services to the site, or to create a zone ID if it does not exist.

Step 11: Upgrade VDAs

> **Important:**
>
> If you're upgrading a VDA to version 1912 or later, see Upgrading VDAs to 1912 or later.

Run the product installer on machines containing VDAs.

If you used Machine Creation Services™ and a master image to create machines, go to your host and upgrade the VDA on the master image. You can use any of the available VDA installers.

- For graphic interface guidance, see Install VDAs.
- For command line guidance, see Install using the command line.

If you used Citrix Provisioning to create machines, see the Citrix Provisioning product documentation for guidance about upgrading.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 12: Update machine catalogs and Delivery Groups

- Update catalogs that use machines with upgraded VDAs.
- Upgrade catalogs that use machines with upgraded VDAs.
- Upgrade Delivery Groups that use machines with upgraded VDAs.

Step 13: After the upgrade

Upgrade other components in your deployment. For guidance, see the following product documentation:

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Session Recording
- Workspace Environment Management

If you need to replace the Microsoft SQL Server Express LocalDB software with a later version, see Replace SQL Server Express LocalDB.

Dbschema upgrade

When you update your deployment, several database schemas can be upgraded. The following table lists which database schemas are upgraded in the process:

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

Definition of terms:

- Site: Site Datastore. Dbschema update is made to the Site Datastore.
- Monitor: Monitor Datastore. Dbschema update is made to the Monitor Datastore.
- Config: Configuration table. Desktop Studio version, Licensing information, or both are updated in the Configuration table.
- Logging: Logging Datastore. Dbschema update is made to the Logging Datastore.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade VDAs to 2203 or later

If the Personal vDisk (PvD) component was ever installed on a VDA, that VDA cannot be upgraded to version 2203 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 never used PvD.

Here's how the PvD component might have been installed in earlier versions:

- In the VDA installer's graphical interface, PvD was an option on the **Additional Components** page.
- On the command line, the `/baseimage` option installed PvD. If you specified this option, or used a script that contained this option, PvD was installed.

If you don't know whether your VDA has PvD installed, run the installer for the new VDA (2203 or later) on the machine or image.

- If PvD is installed, a message appears, indicating there is an incompatible component.
  - From the graphical interface, click **Cancel** on the page containing the message, and then confirm that you want to close the installer.
  - From the CLI, the command simply fails with the displayed message.
- If PvD is not installed, the upgrade proceeds.

What to do

If the VDA does not have PvD installed, follow the usual upgrade procedure.

If the VDA has PvD installed:

1. Uninstall the current VDA.
2. Install the new VDA.

If you want to continue using PvD on your Windows 10 (1607 and earlier, without updates) machines, VDA 7.15 LTSR is the latest supported version.

> **Note:**
>
> *Can I use Personal vDisk with Windows 7 desktops in XenApp and XenDesktop 7.15 LTSR?*
>
> Citrix excluded Personal vDisk (PvD) from XenApp and XenDesktop 7.6 LTSR which was announced in January 2016. Additionally, Citrix has announced the deprecation of the PvD technology and recommends that customers start using Citrix App Layering going forward. Citrix App Layering (version 4.4 and later) is a compatible component of XenApp and XenDesktop 7.15 LTSR. However, to help customers with existing PvD deployments on Windows 7 migrate

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> to Citrix App Layering technology, Citrix has decided to provide limited time support for PvD deployments for Windows 7 desktops through XenApp and XenDesktop 7.15 LTSR Cumulative Updates (CUs) until Jan 14, 2020. The PvD component will be removed from LTSR CUs and not supported after Jan 14, 2020. Also, use of PvD for Windows 7 beyond Jan 14, 2020 will render LTSR sites non-compliant. Also, PvD for Windows 10 remains excluded from 7.15 LTSR. Therefore, customers must not use it with their 7.15 LTSR sites.

Remove PvD, AppDisks, and unsupported hosts

The following technologies and host types are not supported in Citrix Virtual Apps and Desktops 7 Current Release deployments:

- **Personal vDisks (PvD)** for storing data next to users'VMs in catalogs. The user personalization layer feature now handles user persistence.
- **AppDisks** for managing applications used in Delivery Groups.
- **Host types:** Azure Classic, CloudPlatform (the original Citrix product).
    - For host types supported in this release, see System requirements.

If your current deployment uses PvDs or AppDisks, or has connections to unsupported host types (for example, Microsoft Azure Classic), you can upgrade to version 2006 (or later supported versions) only after removing items that use those technologies. If your current deployment uses public cloud host connections (for example, AWS), ensure that you have Hybrid Rights License before upgrading. When the installer detects one or more of the unsupported technologies or host connections without Hybrid Rights License, the upgrade pauses or stops, and an explanatory message appears. The installer logs contain details.

To help ensure a successful upgrade, review and follow the applicable guidance for removing the unsupported items.

- Remove PvD
- Remove AppDisks
- Remove unsupported host items

Even if you did not use PvD or AppDisks in your deployment, related MSIs might have been included in an earlier VDA installation or upgrade. Before you can upgrade your VDAs to version 2006 (or a later supported version), you must remove that software, even if you never used it. When using the graphical interface, that removal can be done for you, or you can include removal options when using the CLI. For details, see Upgrading VDAs that have PvD or AppDisks components.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remove PvD

A deployment upgrade cannot succeed until you remove all machines that are configured to use PvD. This affects catalogs and Delivery Groups.

To remove PvD from groups and catalogs:

1. From Studio, if a Delivery Group contains machines from a catalog that uses PvD, remove those machines from the group.
2. From Studio, delete all catalogs containing machines that use PvD.

VDA upgrades: The deployment upgrade does not detect whether VDAs have the AppDisk or PvD components installed. However, the VDA installers do. For details, see VDAs that have PvD or AppDisks components.

If you plan to use App Layering instead of PvD, see Migrating PvD to App Layering for information about moving data.

Remove AppDisks

A deployment upgrade cannot proceed until you remove AppDisks from all Delivery Groups that use them, and then remove the AppDisks themselves.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then click **Manage AppDisks** in the Action pane.
3. Click the action that removes the AppDisk from the group.
4. Repeat steps 2 and 3 for each Delivery Group that uses AppDisks.
5. Select **AppDisks** in the Studio navigation pane.
6. Select an AppDisk and click the action that deletes the AppDisk.
7. Repeat steps 5 and 6 for each AppDisk.

VDA upgrades: The deployment upgrade does not detect whether VDAs have the AppDisk or PvD components installed. However, the VDA installers do. For details, see VDAs that have PvD or AppDisks components.

Remove unsupported host items

A deployment upgrade to version 2006 (or later supported version) cannot proceed if the site has connections to unsupported host types, such as Citrix CloudPlatform or Microsoft Azure Classic. Complete the following tasks before attempting an upgrade.

From Studio:

- Delete all connections to unsupported hosts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If a Delivery Group contains machines from a catalog created with a master image from an unsupported host, remove those machines from the group.
- Delete all catalogs that were created using a master image from an unsupported host.

VDAs that have PvD or AppDisks components

If the components that enable PvD and AppDisks technologies are installed on a VDA, that VDA cannot be upgraded until those components are removed.

> **Note:**
>
> When upgrading to version 1912, you had to uninstall the current VDA and then install the new VDA. In this version, you're asked if you want Citrix to remove the component and then continue the upgrade.

The AppDisk and PvD components might have been installed in earlier VDA versions, even if you never used those technologies:

- Graphical interface: In the VDA installers, the **Additional Components** page contained the **Citrix AppDisk / Personal vDisk** option. The 7.15 LTSR and earlier 7.x releases enabled this option by default. So, if you accepted the defaults (or explicitly enabled the option in any release that offered it), that component was installed.
- CLI: Specifying the `/baseimage` option installed the component.

What to do If the VDA installer does not detect the AppDisks or PvD components in the currently installed VDA, the upgrade proceeds as usual.

If the installer detects AppDisks or PvD components in the currently installed VDA:

- Graphical interface: The upgrade pauses. A message asks if you want the unsupported components removed automatically. If you click **OK**, the components are removed automatically and the upgrade proceeds.
- CLI: To avoid command failure, include the following options in the command:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

Limitations

The following limitations apply to upgrades:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Selective component install:** If you install or upgrade any components to the new version but choose not to upgrade other components (on different machines) that require upgrade, Studio reminds you. For example, let's say an upgrade includes new versions of the Controller and Studio. You upgrade the Controller but you do not run the installer on the machine where Studio is installed. Studio will not let you continue to manage the site until you upgrade Studio.

  You do not have to upgrade VDAs, but Citrix recommends upgrading all VDAs to enable you to use all available features.

- **Early Release or Technology Preview versions:** You cannot upgrade from an Early Release, Technology Preview, or preview version.

- **Components on earlier operating systems:** You cannot install current VDAs on operating systems that are no longer supported by Microsoft or Citrix. For more information, see Earlier operating systems.

- **Mixed environments/sites:** If you must continue to run earlier version sites and current version sites, see Mixed environment considerations.

- **Product selection:** When you upgrade from an earlier version, you do not choose or specify the product (Citrix Virtual Apps or Citrix Virtual Apps and Desktops) that was set during the installation.

Mixed environment considerations

When you upgrade, Citrix recommends that you upgrade all components and VDAs so that you can access all the new and enhanced features in your edition and version.

For example, although you can use current VDAs in deployments containing earlier Controller versions, new features in the current release might not be available. VDA registration issues can also occur when using non-current versions.

In some environments, you might not be able to upgrade all VDAs to the most current version. In that case, when you create a machine catalog, you can specify the VDA version installed on the machines. (This is called the functional level.) By default, this setting specifies the minimum recommended VDA version. The default value is sufficient for most deployments. Consider changing the setting to an earlier version only if the catalog contains VDAs earlier than the default. Mixing VDA versions in a machine catalog is not recommended.

If a catalog is created with the default minimum VDA version setting, and one or more machines has a VDA earlier than the default version, those machines cannot register with the Controller, and will not work.

For more information, see VDA versions and functional levels.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multiple sites with different versions

When your environment contains sites with different product versions (for example, a XenDesktop 7.18 site and a Citrix Virtual Apps and Desktops 1909 site), Citrix recommends using StoreFront to aggregate applications and desktops from different product versions. For details, see the StoreFront documentation.

In a mixed environment, continue using the Studio and Director versions for each release, but ensure that different versions are installed on separate machines.

Earlier operating systems

Let's say you installed an earlier version of a component on a machine that was running a supported operating system (OS) version. Now, you want to use a newer component version, but that OS is no longer supported for the current version of the component.

For example, assume that you installed a server VDA on a Windows Server 2016 machine. Now you want to upgrade that VDA to the current release, but Windows Server 2016 is not supported in the current release you're upgrading to.

If you try to install or upgrade a component on an operating system that is no longer allowed, an error message displays, such as "Cannot be installed on this operating system".

These considerations apply to upgrading Current Release and Long Term Service Release versions. (It does not affect applying CUs to an LTSR version.)

Follow the links to learn which OSs are supported:

- Citrix Virtual Apps and Desktops (Current Release):
  - Delivery Controller, Studio, Director, VDAs, Universal Print Server
  - Federated Authentication Service
  - For StoreFront, Self-Service Password Reset, and Session Recording, see the system requirements article for the current release.
- For LTSRs, see the components lists for your LTSR version and CU. (Select your LTSR version from the main Citrix Virtual Apps and Desktops product documentation page.)

Invalid operating systems

The following table lists the earlier operating systems that are not valid for installing/upgrading components in the current release. It indicates the latest valid component version supported for each listed OS, and the component version when installation and upgrade became invalid.

The operating systems in the table include service packs and updates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Operating system	Component/feature	Latest valid version	Install/upgrade not possible as of version
Windows 7 and Windows 8	VDA	7.15 LTSR	7.16
Windows 7 and Windows 8	Other installer components	7.17	7.18
Windows 10 versions earlier than 1607	VDA	7.15 LTSR	7.16
Windows 10 x86 version	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	Other installer components	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16
Windows Server 2012	Other installer components	7.17	7.18
Windows Server 2012 R2	Other installer components *	1912 LTSR	2003
Windows Server 2012 R2	Server VDI	7.15 LTSR	7.16
Windows Server 2016	Server VDI	7.15 LTSR	7.16

Windows XP and Windows Vista are not valid for any 7.x components or technologies.

* Applies to Delivery Controller, Studio, Director, and VDAs.

What you can do

You have choices. You can:

- Continue with the current OS
- Reimage or upgrade the machine
- Add new machines and then remove old machines

Continue with the current OS These methods are feasible for VDAs. If you want to continue using machines with the earlier OS, you can choose one of the following:

- Continue using the installed component version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Download the latest valid component version and then upgrade the component to that version. (This assumes that the latest valid component version isn't already installed.)

For example, you have a 7.14 VDA on a Windows 7 SP1 machine. The latest valid VDA version on Windows 7 OS machines is XenApp and XenDesktop 7.15 LTSR. You can either continue using 7.14, or download a 7.15 LTSR VDA and then upgrade your VDA to that version. Those earlier VDA versions work in deployments containing Delivery Controllers with newer versions. For example, a 7.15 LTSR VDA can connect to a Citrix Virtual Apps and Desktops 7 1808 Controller.

Reimage or upgrade the machine These methods are feasible for VDAs and other machines that do not have core components (such as Delivery Controllers) installed. Choose one of the following:

- After taking the machine out of service (turning on maintenance mode and allowing all sessions to close), you can reimage it to a supported Windows OS version, and then install the latest version of the component.
- To upgrade the OS in a VDA machine without reimaging, you must first install the VDA version that is supported on the OS that you are upgrading to or upgrade the VDA after upgrading the OS. Otherwise, the Citrix software will be unsupported. You can upgrade to the following minimum OS versions when performing an in-place upgrade without uninstalling the VDA:
  - Windows 11 with 2023-07 Cumulative Update for Windows 11 (KB5028185) or later installed (build 22621.1992 or later).
  - Windows 10 with 2023-07 Dynamic Update for Windows 10 (KB5028311) installed.
- If the Windows version you plan to upgrade to does not align with the aforementioned guideline, you must uninstall the VDA before upgrading the OS, and then install a supported VDA version after the OS upgrade is complete.

Add new machines and then remove old machines This method is feasible if you must upgrade the OS on machines containing a Delivery Controller™ or other core component.

Citrix recommends that all Controllers in a site have the same OS. The following upgrade sequence minimizes the interval when different Controllers have different OSs.

1. Take a snapshot of all Delivery Controllers in the site and then back up the site database.
2. Install new Delivery Controllers on clean servers with supported operating systems.
3. Add the new Controllers to the site.
4. Remove the Controllers that are running on operating systems that are not valid for the current release. Follow the recommendations for removing Controllers in Delivery Controllers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Preparation

Before beginning an upgrade, review the following information and complete necessary tasks.

> **Note:**
>
> Although upgrading VDAs occurs later in the upgrade sequence, it's a good idea to choose an installer and review the procedure before you start the upgrade, so you know what to expect.

Choose an installer and interface

Use the full-product installer from the product ISO to upgrade components. You can upgrade VDAs using the full-product installer or one of the standalone VDA installers. All installers offer graphical and command-line interfaces.

For more information, see Installers.

Installation specifics: After you complete any preparation work and are ready to start the installer, the installation article shows you what you will see (if you're using the graphical interface) or what to type (if you're using the command-line interface).

- Install/upgrade core components using the graphical interface
- Install/upgrade core components using the command line
- Install/upgrade VDAs using the graphical interface
- Install/upgrade VDAs using the command line

For single-session operating systems, four different installers are available. Citrix advises using a consistent installer type throughout the entire life cycle of a Citrix VDA—including installation, upgrade, and uninstallation. For more information, see Best practices for using single-session VDA installers

When upgrading a VDA to the current release, a machine restart occurs during the upgrade process. (This requirement started with the 7.17 release.) This cannot be avoided. The upgrade resumes automatically after the restart (unless you specify `/noresume` on the command line).

Database actions

Back up the site, monitoring, and configuration logging databases. Follow the instructions in CTX135207. If any issues are discovered after the upgrade, you can restore the backup.

For information about upgrading SQL Server versions that are no longer supported, see SQL Server version check. (This refers to the SQL Server that is used for the site, monitor, and configuration logging databases.)

Microsoft SQL Server Express LocalDB is installed automatically, for use with Local Host Cache. If you need to replace an earlier version, the new version must be SQL Server Express LocalDB 2019. For

© 1997–2026 Citrix Systems, Inc. All rights reserved.

details about replacing SQL Server Express LocalDB with the new version after you upgrade the components and the site, see Replace SQL Server Express LocalDB.

Ensure that your Citrix licensing is up-to-date

For a comprehensive look at managing Citrix Licensing, see Activate, upgrade, and manage Citrix licenses.

You can use the full-product installer to upgrade the License Server. Or, you can download and upgrade the license components separately. See Upgrade.

Before upgrading, be sure your Customer Success Services / Software Maintenance / Subscription Advantage date is valid for the new product version. The date must be at least 2021.11.15.

Ensure that your Citrix License Server is compatible

Ensure that your Citrix License Server is compatible with the new version. There are two ways to do this:

- Before upgrading any other Citrix components, run the `XenDesktopServerSetup.exe` installer from the ISO layout on the machine containing a Delivery Controller. If there are any incompatibility issues, the installer reports it with recommended steps to resolve the issues.
- From the `XenDesktop Setup` directory on the installation media, run the command: `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. The display indicates whether the License Server is compatible. If the License Server is incompatible, upgrade the license server.

Back up any StoreFront modifications

Before starting an upgrade, if you have modified files in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, such as *default.ica* and *usernamepassword.tfrm*, back them up for each store. After the upgrade you can restore them to reinstate your modifications.

Close applications and consoles

Before starting an upgrade, close all programs that might potentially cause file locks, including administration consoles and PowerShell sessions.

Restarting the machine ensures that any file locks are cleared, and that there are no Windows updates pending.

Before starting an upgrade, stop and disable any third-party monitoring agent services.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ensure that you have proper permissions

In addition to being a domain user, you must be a local administrator on the machines where you are upgrading product components.

The site database and the site can be upgraded automatically or manually. For an automatic database upgrade, the Studio user's permissions must include the ability to update the SQL Server database schema (for example, the `db_securityadmin` or `db_owner` database role). For details, see Databases.

If the Studio user does not have those permissions, initiating a manual database upgrade generates scripts. The Studio user runs some of the scripts from Studio. The database administrator runs other scripts, using a tool such as SQL Server Management Studio.

Other preparation tasks

- Back up templates and upgrade hypervisors, if needed
- Complete any other preparation tasks dictated by your business continuity plan.

Preliminary site tests

When you upgrade Delivery Controllers and a site, preliminary site tests run before the actual upgrade begins. These tests verify:

- The site database can be reached and has been backed up
- Connections to essential Citrix services are working correctly
- The Citrix License Server address is available
- The configuration logging database can be reached
- Ensure you have Hybrid Rights License if you want to add public cloud host connections (for example, AWS). Otherwise, the preliminary site test pauses or stops, and an explanatory message appears.

After the tests run, you can view a report of the results. You can then fix any issues that were detected, and run the tests again. Failure to run the preliminary site tests and then resolve any issues can impact how your site works.

The report containing the test results is an HTML file (`PreliminarySiteTestResult.html`) in the same directory as the installation logs. That file is created if it does not exist. If the file exists, its content is overwritten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run the tests

- When you're using the installer's graphical interface to upgrade, the wizard includes a page where you can start the tests and then display the report. After the tests run and you have viewed the report and resolved any issues that were found, you can rerun the tests. When the tests complete successfully, click Next to continue with the wizard.
- When you're using the command-line interface to upgrade, the tests run automatically. By default, if a test fails, the upgrade is not performed. After you view the report and resolve issues, rerun the command.

Citrix recommends always running the preliminary site tests and then resolving any issues before you continue the Controller and site upgrade. The potential benefit is well worth the few moments to run the tests. However, you can override this recommended action.

- When upgrading with the graphical interface, you can choose to skip the tests and continue with the upgrade.
- When upgrading from the command line, you cannot skip the tests. By default, a failed site test causes the installer to fail, without performing the upgrade. Usually, if you include the `/ignore_site_test_failure` option, any test failures are ignored and the upgrade proceeds. (See SQL Server version check for exceptions.)

When upgrading multiple Controllers

When you start an upgrade on one Controller, and then start an upgrade of another Controller in the same site (before the first upgrade completes):

- If the preliminary site tests are completed on the first Controller, the preliminary site tests page does not appear in the wizard on the other Controller.
- If the tests on the first Controller are ongoing when you start the upgrade on the other Controller, the site tests page appears in the wizard on the other Controller. However, if the tests on the first Controller finish, only the test results from the first Controller are retained.

Test failures not related to the site's health

- If the preliminary site tests fail due to insufficient memory, make more memory available and then rerun the tests.
- If you have permission to upgrade, but not run site tests, the preliminary site tests fail. To resolve this, rerun the installer with a user account that has permission to run the tests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SQL Server version check

A successful Citrix Virtual Apps and Desktops deployment requires a supported version of Microsoft SQL Server for the site, monitor, and configuration logging databases. Upgrading a Citrix deployment with a SQL Server version that's no longer supported can result in functionality issues, and the site will be unsupported.

To learn which SQL Server versions are supported for the Citrix release you're upgrading to, see the System requirements article for that release.

When upgrading a Controller, the Citrix installer checks the currently installed SQL Server version used for the site, monitor, and configuration logging databases.

- If the check determines that the currently installed SQL Server version is not a supported version in the Citrix release you're upgrading to:
  - Graphical interface: The upgrade halts with a message. Click **I understand** and then click **Cancel** to close the Citrix installer. (You cannot continue with the upgrade.)
  - Command-line interface: the command fails (even if you included the `/ignore_db_check_failur` option with the command).

  Upgrade the SQL Server version, and then start the Citrix upgrade again.
- If the check cannot determine which SQL Server version is currently installed, see if your currently installed version is supported in the version you're upgrading to (System requirements).
  - Graphical interface: The upgrade halts with a message.
    - If the currently installed SQL Server version is supported, click **I understand** to close the message, and then click **Next** to continue with the Citrix upgrade.
    - If the currently installed SQL Server version is not supported, click **I understand** to close the message, and then click **Cancel** to end the Citrix upgrade. Upgrade your SQL Server to a supported version and then start the Citrix upgrade again.
  - Command-line interface: The command fails with a message. After closing the message:
    - If the currently installed SQL Server version is supported, run the command again with the `/ignore_db_check_failure` option.
    - If the currently installed SQL Server version is not supported, upgrade your SQL Server to a supported version. Run the command again to start the Citrix upgrade.

Upgrading SQL Server

If you bring up new SQL Server servers and migrate the site database, then connection strings must be updated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the site currently uses SQL Server Express for the site database (that Citrix installed automatically during site creation):

1. Install the latest SQL Server Express version.
2. Detach the database.
3. Attach the database to the new SQL Server Express.
4. Migrate connection strings.

For more information, see Configuring connection strings and the Microsoft SQL Server product documentation.

Replace SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB is a feature of SQL Server Express that Local Host Cache uses on a standalone basis. Local Host Cache does not require any components of SQL Server Express other than SQL Server Express LocalDB.

When upgrading Delivery Controllers to Citrix Virtual Apps and Desktops version 2203 LTSR or later versions, the supported version is SQL Server Express LocalDB 2019 or SQL Server Express LocalDB 2022.

There are two ways of updating SQL Server Express LocalDB:

- Automatic update
- Manual update

Automatic update

When you upgrade Delivery Controllers, the metainstaller automatically installs the latest compatible version of the SQL Server Express LocalDB. The metainstaller does not uninstall the old LocalDB version. You must manually uninstall the old version after you confirm the new version works correctly.

Verify new SQL Server Express LocalDB installation Before uninstalling the old version, verify that the new SQL Server Express LocalDB installation is working correctly:

1. Use Command Prompt to navigate to the SqlLocalDB instance:
    - For SQL LocalDB 2014: cd `C:\Program Files\Microsoft SQL Server\120\Tools\Binn`
    - For SQL LocalDB 2017: cd `C:\Program Files\Microsoft SQL Server\140\Tools\Binn`
    - For SQL LocalDB 2019: cd `C:\Program Files\Microsoft SQL Server\150\Tools\Binn`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For SQL LocalDB 2022: cd `C:\Program Files\Microsoft SQL Server\160\Tools\Binn`

2. Run `SqlLocalDB i`.

   You must see two files: `CitrixHA` and `MSSQLLocalDB`.

Manual update

Prerequisites

- The Citrix Virtual Apps and Desktops installation media.
- The PsExec tool from the Windows Sysinternals toolbox.

Procedure

1. Complete the upgrade of your Citrix Virtual Apps and Desktops components, databases, and site. (Those database upgrades affect the site, monitoring, and configuration logging databases. They do not affect the Local Host Cache database that uses SQL Server Express LocalDB.)
2. Log on to the Delivery Controller, where you would like to update SQL Server Express LocalDB.
3. Download PsExec from Microsoft and place it in an easily accessible location on that Delivery Controller, such as C:\Temp.
4. Stop the Citrix High Availability Service on the Delivery Controller from the Windows System Services.
5. Open the Command Prompt on the Delivery Controller, navigate to the location with PsExec (example, `C:\Temp`), and then run the following command to elevate the command prompt with the Network Service account:

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. Run `whoami` to confirm that the command prompt is running as the Network Service account. You must get the following output: `nt authority\networkservice`.
7. Use the command prompt to navigate to the SQL LocalDB instance:

   - If upgrading from SQL LocalDB 2014:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - If upgrading from SQL LocalDB 2017:

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - If upgrading from SQL LocalDB 2019:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
```

8. Stop and delete the SQL LocalDB instance: `CitrixHA`.

```
SqlLocalDB stop CitrixHA

SqlLocalDB delete CitrixHA
```

9. Remove the following files from the Delivery Controller:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*
C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if exists)
C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.* (if exists)
```

10. Uninstall your existing SQL LocalDB SQL Server Express from the Delivery Controller using the native Windows feature for removing programs.
11. Reboot the Delivery Controller after the uninstallation is complete.
12. Stop the Citrix High Availability Service on the Delivery Controller from the Windows System Services.
13. Mount the Citrix Virtual Apps and Desktops installation media to your Delivery Controller.
14. Install SQL Server Express LocalDB 2022 as an administrator on the Delivery Controller.
    a) Use the `sqllocaldb.msi` file in the `Support > SQLLocalDB` folder of the Citrix Virtual Apps and Desktops installation media. For example, if the installation media is mounted to the `E drive` letter, the file can be found at `E:\Support\SQLLocalDB\sqllocaldb.msi`. A restart is required to complete the installation.
    b) The new SQL LocalDB must be in `C:\Program Files\Microsoft SQL Server\160\Tools\Binn`.
15. Start the Citrix High Availability Service on the Delivery Controller from the Windows System Services.
16. In the Command Prompt of the Delivery Controller, navigate to `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` and run `SqlLocalDB i` to confirm that the CitrixHA instance was created. The `CitrixHA` must be included in the list of instances returned.

> **Note:**
>
> It can take up to 15 minutes for the CitrixHA database to be created after starting the Citrix High Availability Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

17. Ensure that the Local Host Cache database files are created to confirm that the High Availability Service (secondary broker) can take over if needed.
    a) On the Delivery Controller, browse to `C:\Windows\ServiceProfiles\NetworkService`.
    b) Verify that `HaDatabaseName.mdf` and `HaDatabaseName_log.ldf` are created.
18. Repeat the steps on the remaining Delivery Controllers.

Proxy Support for VDA Upgrade Agent

May 5, 2025

Proxy Support for VDA Upgrade Agent has been added in 2311 VDA.

VDA Upgrade Agent from 2311 VDA i,e Version: 7.40 can recognize and send traffic through the Proxy.

VDA Upgrade Agent (VUA) Supports Proxy in the form of Hostname:Port (IP:Port) and PAC file.

Only HTTP proxies are supported.
Packet decryption and inspection are not supported.

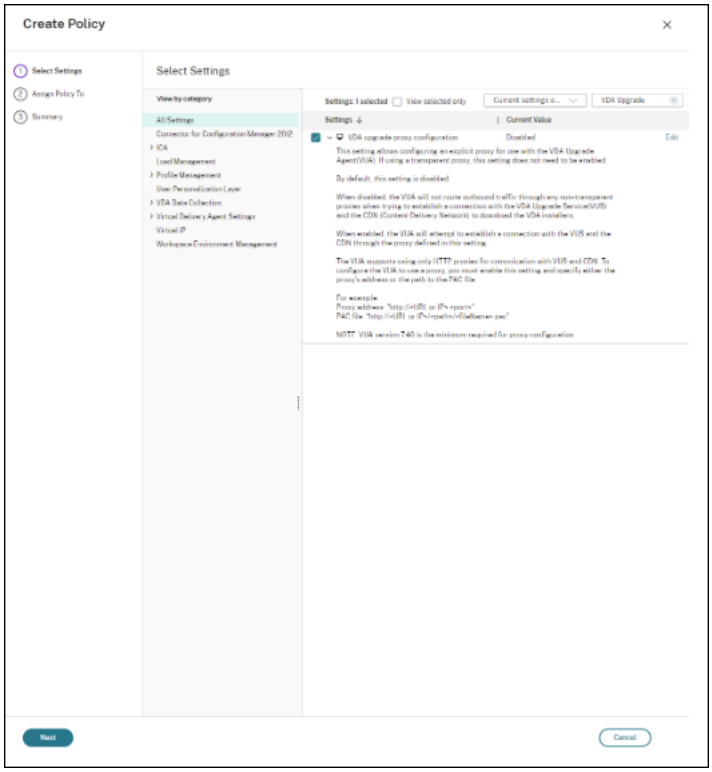
Proxy authentication is not supported.
SOCKS5 is not supported.

Configuring VDA Upgrade Agent Proxy

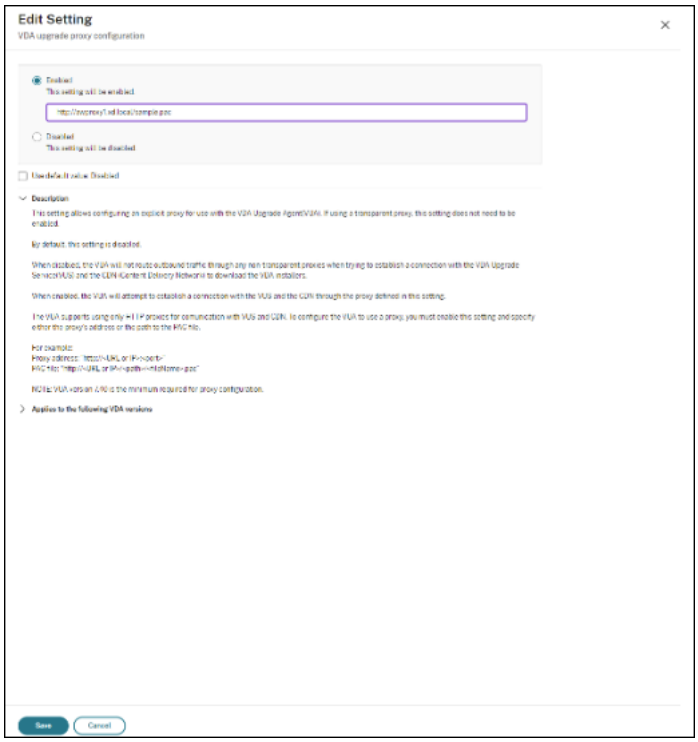
VDA Upgrade Agent Proxy can be configured in 2 ways:

1. **Configuring VDA Upgrade Agent Policy** using **Webstudio Policy**.
2. Select **VDA upgrade proxy configuration** from the **Settings** on the **Create Policy** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Enable the setting. By default, the setting is disabled.



4. Configuring VDA Upgrade Agent using Registry Key.

   The registry Key is set to Meta-Installer during VDA Installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

a) Proxy address: http://<URL or IP>:<port>
b) Pac file: http://<URL or IP>/<path/<filename>.pac

Secure

September 13, 2025

Citrix Virtual Apps and Desktops™ offers a secure-by-design solution that allows you to tailor your environment to your security needs.

One security concern IT faces with mobile workers is lost or stolen data. By hosting applications and desktops, Citrix Virtual Apps and Desktops securely separates sensitive data and intellectual property from end-point devices by keeping all data in a data center. When policies are enabled to allow data transfer, all data is encrypted.

The Citrix Virtual Apps and Desktops data centers also make incident response easier with a centralized monitoring and management service. Director allows IT to monitor and analyze data that is being accessed around the network, and Studio allows IT to patch and remedy most vulnerabilities in the data center instead of fixing the problems locally on each end-user device.

Citrix Virtual Apps and Desktops also simplify audits and regulatory compliance because investigators can use a centralized audit trail to determine who accessed what applications and data. Director gathers historical data regarding updates to the system and user data usage by accessing Configuration Logging and OData API.

Delegated administration allows you to set up administrator roles to control access to Citrix Virtual Apps and Desktops at a granular level. This allows flexibility in your organization to give certain administrators full access to tasks, operations, and scopes while other administrators have limited access.

Citrix Virtual Apps and Desktops give administrators granular control over users by applying policies at different levels of the network - from the local level to the Organizational Unit level. This control of policies determines if a user, device, or groups of users and devices can connect, print, copy/paste,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

or map local drives, which can minimize security concerns with third-party contingency workers. Administrators can also use the Desktop Lock feature so end users can only use the virtual desktop while preventing any access to the local operating system of the end-user device.

Administrators can increase security on Citrix Virtual Apps or Citrix Virtual Desktops by configuring the Site to use the Transport Layer Security (TLS) protocol of the Controller or between end users and Virtual Delivery Agents (VDA). The protocol can also be enabled on a Site to provide server authentication, data stream encryption, and message integrity checks for a TCP/IP connection.

Citrix Virtual Apps and Desktops also support multifactor authentication for Windows or a specific application. Multifactor authentication can also be used to manage all resources delivered by Citrix Virtual Apps and Desktops. These methods include:

- Tokens
- Smart cards
- RADIUS
- Kerberos
- Biometrics

Citrix Virtual Desktops can be integrated with many third-party security solutions, ranging from identity management to antivirus software. A list of supported products can be found at http://www.citrix.com/ready.

Select releases of Citrix Virtual Apps and Desktops are certified for Common Criteria standard. For a list of those standards, go to https://www.commoncriteriaportal.org/cc/.

FIDO2 and WebAuthn authentication

April 23, 2026

Local authorization and virtual authentication using FIDO2 and WebAuthn

Users can authenticate to applications that leverage FIDO2 or WebAuthn in their virtual session using FIDO2 security keys and integrated biometrics devices with TPM 2.0 and Windows Hello.

For more information about FIDO2, see FIDO2: WebAuthn & CTAP.

For information about using this feature, see FIDO2 redirection.

> **NOTE**
>
> Please note that this feature does not support logging into the virtual session using WebAuthn or FIDO2. This feature only allows using these authentication methods in applications within the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> virtual session.

Supportability matrix

Session host operating system	Web application authentication	UWP application authentication
Windows Server 2016	Supported via USB redirection	Not supported
Windows Server 2019	Supported	Not supported
Windows Server 2022	Supported	Supported
Windows Server 2025	Supported	Supported
Windows 10	Supported	Supported
Windows 11	Supported	Supported

For additional information, please review the requirements below.

Web application authentication

Requirements

The following are the requirements for using FIDO2 and WebAuthn authentication with web applications:

Citrix® control plane

- Citrix Virtual Apps and Desktops™ 2009 or later

Session host

- Operating system
  - Windows 10 1809 or later
  - Windows 11
  - Windows Server 2019 or later
- VDA
  - Windows: version 2009 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client device

- Operating system
  - Windows 10 1809 or later
  - Windows 11
  - Linux: Please refer to the Workspace app for Linux system requirements
- Workspace app
  - Windows: version 2009.1 or later
  - Linux: 2303 or later

Web browser requirements

- 32-bit and 64-bit browsers

Authentication methods supported

- FIDO2 Security Key
- Windows Hello
  - TPM 2.0
  - Integrated biometrics
    - Facial recognition
    - Fingerprint scanner
  - WebAuthn

UWP application authentication

With the release of Citrix Virtual Apps and Desktops 2112, Citrix supports WebAuthn and FIDO2 authentication in UWP applications.

Applications such as Microsoft Teams, Microsoft Outlook for Office 365 and OneDrive use a UWP application for authentication as a link to Azure Active Directory. Citrix now supports using FIDO2 to authenticate those applications.

Requirements

The following are the requirements for using FIDO2 and WebAuthn authentication with UWP applications:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix control plane

- Citrix Virtual Apps and Desktops 2112 or later

Session host

- Operating system
  - Windows 10 1809 or later
  - Windows 11
  - Windows Server 2022 or later
- VDA
  - Windows: version 2112 or later

Client device

- Operating system
  - Windows 10 1809 or later
  - Windows 11
  - Linux: Please refer to the Workspace app for Linux system requirements
- Workspace app
  - Windows: version 2009.1 or later
  - Linux: 2303 or later

UWP application requirements

- 32-bit and 64-bit applications

Authentication methods supported

- FIDO2 Security Key
- Windows Hello
  - TPM 2.0
  - Integrated biometrics
    - Facial recognition
    - Fingerprint scanner
  - WebAuthn

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Support for the authentication methods listed above depends on the capabilities of the underlying operating system.
>
> In scenarios where FIDO2 redirection is not available because the feature is not supported by the client or VDA or the operating system, USB based FIDO2 keys can be redirected using USB redirection.
> It is also possible to use USB redirection to redirect USB based FIDO2 keys in scenarios where FIDO2 redirection is available. In this case, you must disable FIDO2 redirection and configure the appropriate USB redirection rules.
> Please refer to the USB redirection device rules documentation for details on how to configure FIDO2 keys using USB redirection rules.

Advanced configuration for msedgewebview2.exe based applications

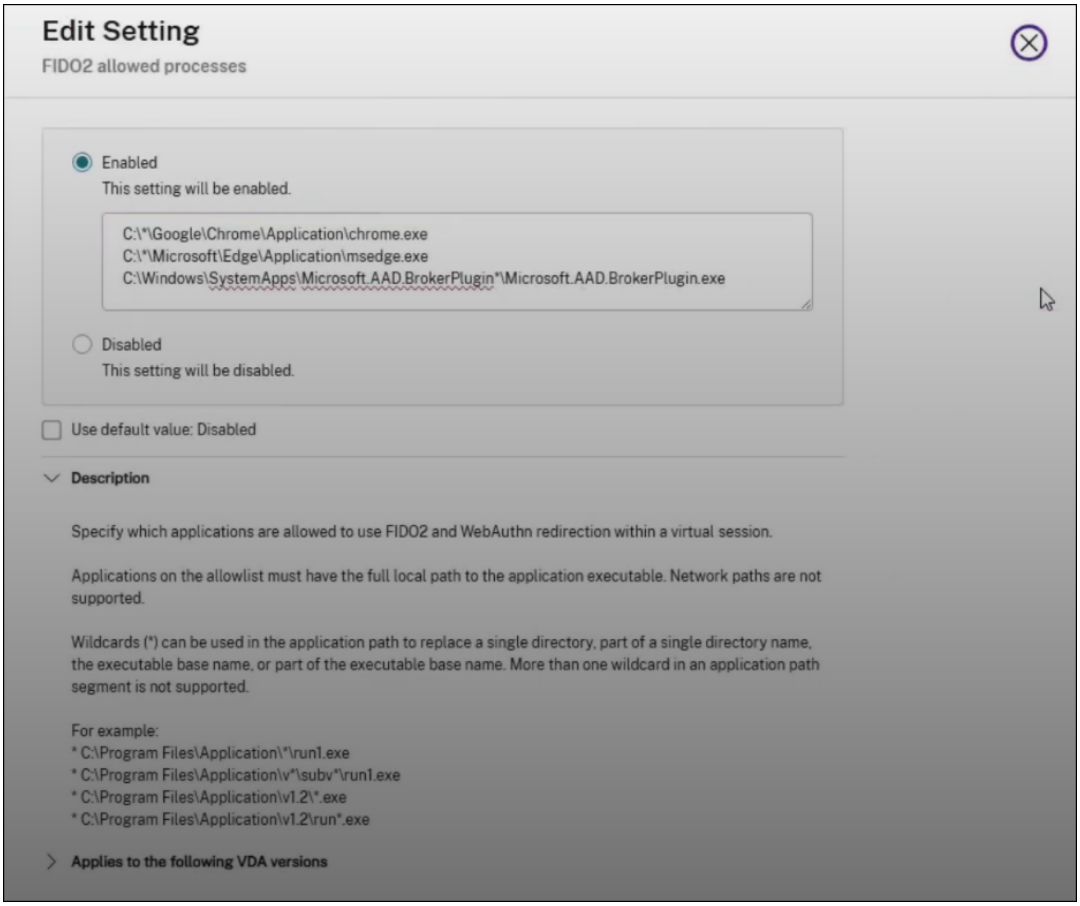
> **Note:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved.
> Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

For enterprises that have web applications based on msedgewebview2.exe, the following changes need to be made for FIDO2 redirection to work inside HDX sessions -

1. Set the **FIDO2 allowed processes** policy setting in Studio.
    - Add the full path of the application in the text field. Additional details on policy setting usage can be found in the policies.

      > **Note:**
      >
      > Wildcards(*) can be used in the application path to replace a single directory, a part of the directory name, the executable base name or a part of the executable base name. More than one wildcard in an application path segment is not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Set the following hook keys in the VDA

   a) For 64-bit applications, the following values need to be set:

   - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msed
   - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
   - Value name: FilePathName
   - Value type: REG_SZ
   - Value data: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
   - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
   - Value name: Flag
   - Value type: DWORD
   - Value data: 00000002

   b) For 32-bit applications, the following values need to be set:

   - Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebA
   - Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebA
   - Value name: FilePathName
   - Value type: REG_SZ
   - Value data: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAu
- Value name: Flag
- Value type: DWORD
- Value data: 00000002

Reboot the VDA after setting the registry values for FIDO2 redirection to be enabled for msedgeweb-view2.exe based applications.

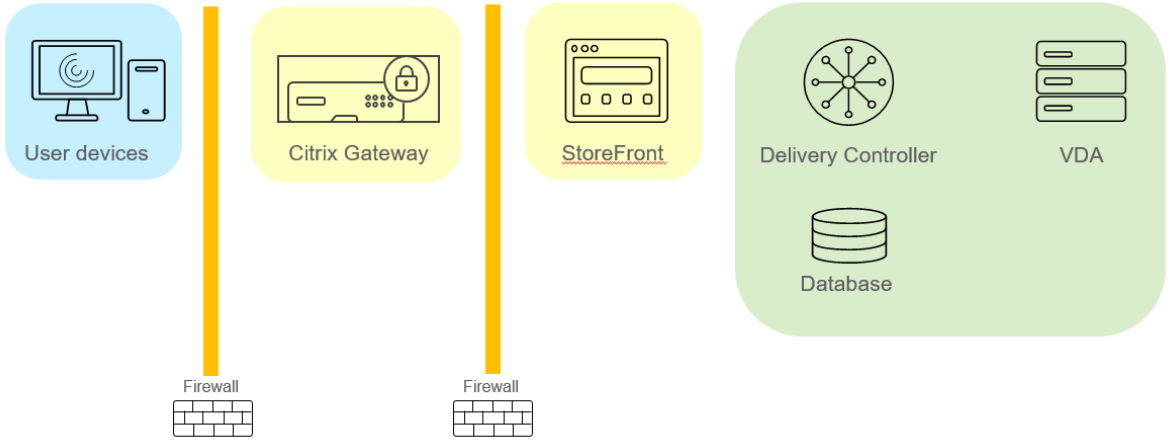
Integrate Citrix Virtual Apps and Desktops™ with Citrix Gateway

September 13, 2025

StoreFront™ servers are deployed and configured to manage access to published resources and data. For remote access, adding Citrix Gateway in front of StoreFront is recommended.

> **Note:**
>
> For detailed configuration steps on how to integrate Citrix Virtual Apps and Desktops with Citrix Gateway, see the StoreFront documentation.

The following diagram illustrates an example of a simplified Citrix deployment that includes Citrix Gateway. Citrix Gateway communicates with StoreFront to protect apps and data delivered by Citrix Virtual Apps and Desktops. The user devices run Citrix Workspace™ app to create a secure connection and access their apps, desktops, and files.



Users log on and authenticate using Citrix Gateway. Citrix Gateway is deployed and secured in the DMZ. Two-factor authentication is configured. Based on the user credentials, users are provided with the relevant resources and applications. Applications and data are on appropriate servers (not shown on the diagram). Separate servers used for security sensitive applications and data.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security considerations and best practices

September 13, 2025

> **Note:**
>
> Your organization might need to meet specific security standards to satisfy regulatory requirements. This document does not cover this subject, because such security standards change over time. For up-to-date information on security standards and Citrix products, consult the Citrix Trust Center.

Firewalls

Protect all machines in your environment with perimeter firewalls, including at enclave boundaries as appropriate.

All machines in your environment must be protected by a personal firewall. When you install core components and VDAs, you can choose to have the ports required for component and feature communication opened automatically if the Windows Firewall Service is detected (even if the firewall is not enabled). You can also choose to manually configure those firewall ports. If you use a different firewall, you must manually configure it. For more information on required ports, see Tech Paper: Communication Ports Used by Citrix Technologies.

If you are migrating a conventional environment to this release, you may need to reposition an existing perimeter firewall or add new perimeter firewalls. For example, suppose there is a perimeter firewall between a conventional client and database server in the data center. When this release is used, that perimeter firewall must be placed so that the virtual desktop and user device are on one side, and the database servers and Delivery Controllers in the data center are on the other side. Therefore, consider creating an enclave within your data center to contain the database servers and Controllers. Also consider having protection between the user device and the virtual desktop.

> **Note:**
>
> TCP ports 1494 and 2598 are used for ICA and CGP and are therefore likely to be open at firewalls so that users outside the data center can access them. Citrix recommends that you do not use these ports for anything else, to avoid the possibility of inadvertently leaving administrative interfaces open to attack. Ports 1494 and 2598 are officially registered with the Internet Assigned Number Authority (http://www.iana.org/).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure communications with Delivery Controller™

Encrypting communication using HTTPS

StoreFront and NetScaler gateway communicate with the XML service running on the delivery controller over HTTP or HTTPS. Depending on configuration, VDAs may communicate with the delivery controller using WebSocket. Director communicates with the monitor data using OData over HTTP or HTTPS. It is recommended that you enable HTTPS and disable HTTP. This requires that you Enable TLS on Delivery Controllers.

- To configure StoreFront to connect using HTTPS, see Add resource feeds for Citrix Virtual Apps and Desktops and Add Citrix Gateway appliance.
- To configure a NetScaler gateway to connect to the Delivery Controller using HTTPS, see Configuring the Secure Ticket Authority on NetScaler Gateway.

Security Keys

You can use Security Keys to ensure that only authorized StoreFront and NetScaler servers are able to connect to DaaS via the cloud connectors. This is especially important if you have enabled XML trust.

XML trust

By default, when StoreFront connects to the delivery controller 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, Citrix Virtual Apps and Desktops 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 Delivery Controllers.

Use the Citrix Virtual Apps and Desktops PowerShell SDK to check, enable, or disable the XML trust setting.

- To check the XML trust setting's current value, run `Get-BrokerSite` and inspect the value of `TrustRequestsSentToTheXMLServicePort`.
- To enable or disable XML trust, run `Set-BrokerSite` with parameter `TrustRequestsSentToTheXml`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Communication between VDA and Delivery Controller

There are two mechanisms for VDAs communicating with controllers.

- Windows Communication Foundation

  Windows Communication Foundation (WCF) message-level protection secures communication between the Delivery Controller and the VDA. This eliminates the need for extra transport-level protection using TLS. The default port used for communication between VDA and Delivery Controller is 80. However, you can customize the port. For information, see Customize a VDA.

  For information on message security in WCF, see the Microsoft documentation Message Security in WCF.

  The WCF configuration uses Kerberos for mutual authentication between the Controller and VDA. Encryption uses AES in CBC mode with a 256-bit key. Message integrity uses SHA-1.

  According to Microsoft, the Security protocols used by WCF conform to standards from OASIS (Organization for the Advancement of Structured Information Standards), including WS-SecurityPolicy 1.2. Also, Microsoft states that WCF supports all algorithm suites listed in Security Policy 1.2.

  Communication between the Controller and VDA uses the basic256 algorithm suite, whose algorithms are as stated before.

  The WCF configuration uses SOAP over HTTP protocol along with the message-level security encryption.

- WebSockets

  This is the modern replacement for WCF. It provides the benefit that only the TLS port 443 for communication from the VDA to the Delivery Controller. It is currently only available for MCS provisioned machines. For more information, see WebSocket communication between VDA and Delivery Controller.

Secure communications between Delivery Controller and License Server

The Delivery controller communicates with the License Server over HTTPS. By default it uses a self-signed certificate but it is recommended that you replace this with a certificate issued by an enterprise or public certificate authority. For more information, see Manually install a certificate used by the Citrix Licensing Manager and Web Services for Licensing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure communications between web browsers and Web Studio and Director

Web Studio and Director may be installed on the same machine as the Delivery Controller or a separate machines. Users connect to Web Studio and Director using a web browser. By default Web Studio enables HTTPS using a self-signed certificate, while Director installed stand-alone does not configure HTTPS. It is recommended that you Enable TLS on Web Studio and Director, using an appropriate certificate.

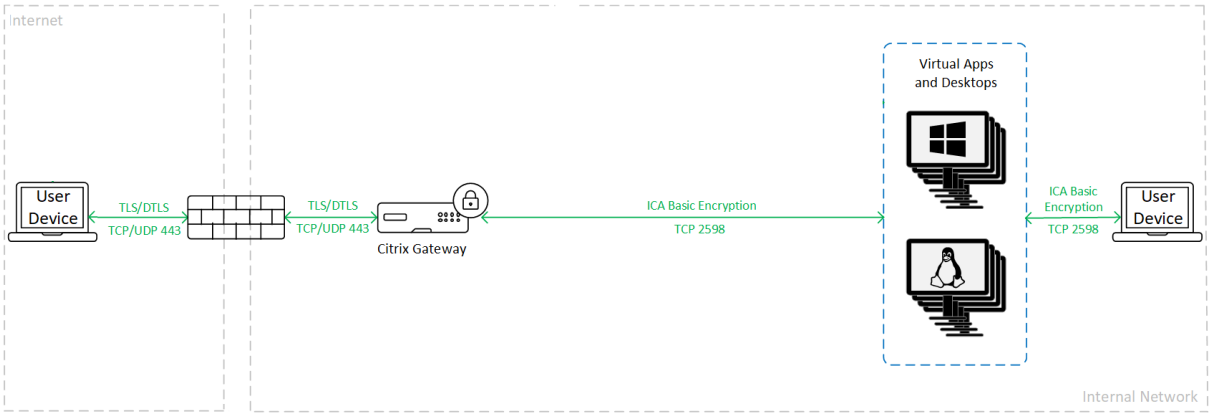
Securing ICA® communications

Citrix Virtual Apps and Desktops™ provides several options for securing ICA traffic between the client and the VDA. The following are the options available:

- **Basic encryption:** The default setting.
- **SecureICA:** Allows encrypting session data using RC5 (128-bit) encryption.
- **VDA TLS/DTLS:** Allows using network-level encryption using TLS/DTLS.

Basic encryption

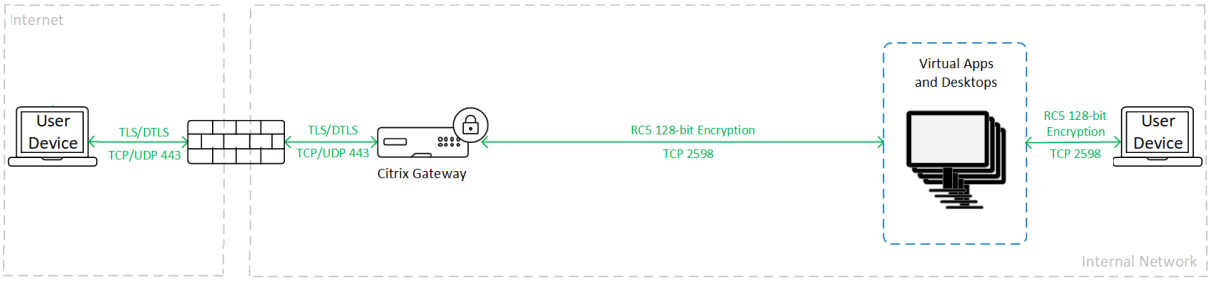
When using basic encryption, traffic is encrypted as shown in the following graphic.



SecureICA

When using SecureICA, traffic is encrypted as shown in the following graphic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

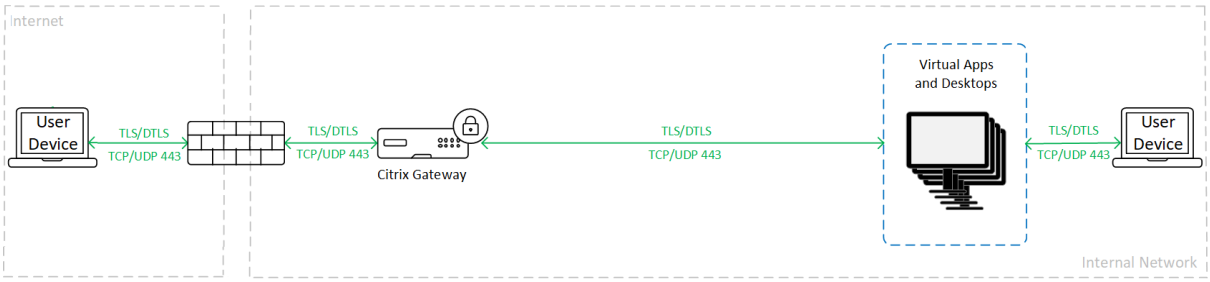


For more information see Security policy settings

> **Note 1:**
>
> SecureICA is not supported when the Workspace app for HTML5.
>
> **Note 2:**
>
> Citrix SecureICA forms part of the ICA/HDX protocol but it is not a standards-compliant network security protocol like Transport Layer Security (TLS).

VDA TLS/DTLS

When using VDA TLS/DTLS encryption, traffic is encrypted as shown in the following graphic.



To configure VDA TLS/DTLS, see TLS settings on VDAs.

Virtual channels

Use the virtual channel allow list to control which non-Citrix virtual channels are allowed in your environment.

Secure communications with print server

You can enable TLS for TCP-based connections between the Virtual Delivery Agent (VDA) and the Universal Print Server. For more information, see Transport Layer Security (TLS) on Universal Print Server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure communication with the site database

For information about enabling TLS to the Site database, see CTX137556.

VDA machine security

General recommendations

Ensure that your VDAs are kept up to date with the latest operating security updates and antivirus.

Application security

To prevent non-admin users from performing malicious actions, Citrix® recommends that you configure Windows AppLocker rules for installers, applications, executables, and scripts on the VDA host.

8.3 file names

You can disable 8.3 file names on VDAs. See Microsoft fsutil documentation.

Data storage considerations

Your desktop environment might consist of various types of desktops, such as pooled and dedicated desktops. Users must never store data on desktops that are shared among the users, such as pooled desktops. If users store data on dedicated desktops, that data must be removed if the desktop is later made available to other users.

User account management

Apply Windows best practice for account management. Do not create an account on a template or image before it is duplicated by Machine Creation Services or Provisioning Services. Do not schedule tasks using stored privileged domain accounts. Do not manually create shared Active Directory machine accounts. These practices will help prevent a machine attack from obtaining local persistent account passwords and then using them to log on to MCS/PVS shared images belonging to others.

Grant users only the capabilities they require. Microsoft Windows privileges continue to be applied to desktops in the usual way: configure privileges through User Rights Assignment and group memberships through Group Policy. One advantage of this release is that it is possible to grant a user administrative rights to a desktop without also granting physical control over the computer on which the desktop is stored.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note the following when planning for desktop privileges:

- By default, when non-privileged users connect to a desktop, they see the time zone of the system running the desktop instead of the time zone of their own user device. For information on how to allow users to see their local time when using desktops, see the Manage Delivery Groups article.
- A user who is an administrator on a desktop has full control over that desktop. If a desktop is a pooled desktop rather than a dedicated desktop, the user must be trusted in respect of all other users of that desktop, including future users. All users of the desktop need to be aware of the potential permanent risk to their data security posed by this situation. This consideration does not apply to dedicated desktops, which have only a single user; that user should not be an administrator on any other desktop.
- A user who is an administrator on a desktop can generally install software on that desktop, including potentially malicious software. The user can also potentially monitor or control traffic on any network connected to the desktop.

Manage logon rights

Logon rights are required for both user accounts and computer accounts. As with Microsoft Windows privileges, logon rights continue to be applied to desktops in the usual way: configure logon rights through User Rights Assignment and group memberships through Group Policy.

The Windows logon rights are: log on locally, log on through Remote Desktop Services, log on over the network (access this computer from the network), log on as a batch job, and log on as a service.

For computer accounts, grant computers only the logon rights they require. The logon right "Access this computer from the network"is required for the computer accounts of Delivery Controllers.

For user accounts, grant users only the logon rights they require.

According to Microsoft, by default the group Remote Desktop Users is granted the logon right "Allow log on through Remote Desktop Services"(except on domain controllers).

Your organization's security policy may state explicitly that this group should be removed from that logon right. Consider the following approach:

- The Virtual Delivery Agent (VDA) for Multi-session OS uses Microsoft Remote Desktop Services. You can configure the Remote Desktop Users group as a restricted group, and control membership of the group via Active Directory group policies. Refer to Microsoft documentation for more information.
- For other components of Citrix Virtual Apps and Desktops, including the VDA for Single-session OS, the group Remote Desktop Users is not required. So, for those components, the group Remote Desktop Users does not require the logon right "Allow log on through Remote Desktop Services"; you can remove it. Additionally:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you administer those computers via Remote Desktop Services, ensure that all such administrators are already members of the Administrators group.
- If you do not administer those computers via Remote Desktop Services, consider disabling Remote Desktop Services itself on those computers.

Although it is possible to add users and groups to the login right "Deny logon through Remote Desktop Services", the use of deny logon rights is not generally recommended. Refer to Microsoft documentation for more information.

Delivery Controller security

Windows services on Delivery Controller

Delivery Controller installation creates the following Windows services:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): Manages Microsoft Active Directory computer accounts for VMs.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): Collects site configuration usage information for use by Citrix, if this collection been approved by the site administrator. It then submits this information to Citrix, to help improve the product.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): Supports management and provisioning of AppDisks, AppDNA integration, and management of App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): Selects the virtual desktops or applications that are available to users.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): Records all configuration changes and other state changes made by administrators to the site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): Site-wide repository for shared configuration.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): Manages the permissions granted to administrators.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): Manages self-tests of the other Delivery Controller services.
- Citrix Host Service (NT SERVICE\CitrixHostService): Stores information about the hypervisor infrastructures used in a Citrix Virtual Apps or Citrix Virtual Desktops deployment, and also offers functionality used by the console to enumerate resources in a hypervisor pool.
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): Orchestrates the creation of desktop VMs.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Collects metrics for Citrix Virtual Apps or Citrix Virtual Desktops, stores historical information, and provides a query interface for troubleshooting and reporting tools.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix StoreFront Service (NT SERVICE\ CitrixStorefront): Supports management of StoreFront. (It is not part of the StoreFront component itself.)
- Citrix StoreFront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Supports privileged management operations of StoreFront. (It is not part of the StoreFront component itself.)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): Propagates configuration data from the main site database to the Local Host Cache.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): Selects the virtual desktops or applications that are available to users when the main site database is unavailable.

Delivery Controller installation also creates the following Windows services. These are also created when installed with other Citrix components:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Supports the collection of diagnostic information for use by Citrix Support.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Collects diagnostic information for analysis by Citrix, such that the analysis results and recommendations can be viewed by administrators to help diagnose issues with the site.

Delivery Controller installation also creates the following Windows service. This is not currently used. If it has been enabled, disable it.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

Delivery Controller installation also creates these following Windows services. These are not currently used, but must be enabled. Do not disable them.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

Except for the Citrix StoreFront™ Privileged Administration Service, these services are granted the logon right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. You do not need to change these user rights. These privileges are not used by the Delivery Controller and are automatically disabled.

Except for the Citrix StoreFront Privileged Administration service and the Citrix Telemetry Service, the Delivery Controller Windows services listed before are configured to log on as the NETWORK SERVICE identity. Do not alter these service settings.

The Citrix Config Synchronizer Service needs the NETWORK SERVICE account to belong to the Local Administrator group on the Delivery Controller. This allows Local Host Cache to work correctly.

The Citrix StoreFront Privileged Administration service is configured to log on Local System (NT AUTHORITY\SYSTEM). This is required for Delivery Controller StoreFront operations that are not normally available to services (including creating Microsoft IIS sites). Do not alter its service settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Citrix Telemetry Service is configured to log on as its own service-specific identity.

You can disable the Citrix Telemetry Service. Apart from this service, and services that are already disabled, do not disable any other of these Delivery Controller Windows services.

Manage logon rights

The computer accounts of VDAs must have login right "Access this computer from the network". See Active Directory OU-based Controller discovery.

Client access

Client access is normally provided by deploying Citrix StoreFront. For more information on securing StoreFront, see StoreFront documentation.

To allow remote users to security connect to StoreFront and the VDAs, deploy a NetScaler® gateway.

Citrix recommends that clients connect to StoreFront using Citrix Workspace app. For more more information, see the security sections of the documentation for Citrix Workspace app for each operating system. Alternatively users may use a web browser to access StoreFront.

Consider providing users with thin clients where users have limited ability to run applications other than Citrix Workspace™ app. Where devices are managed by your organization you should put in policies to ensure deployment of operating system security updates and anti-virus software. However in many cases users need to be able to connect from un-managed device outside of the control of your organization. Consider using the following features:

- Endpoint Analysis to scan endpoints for security information such as operating system and anti-virus and denies access to clients that do not meet your security requirements.
- App Protection blocks key loggers and screen capture.

Mixed-version environments

Mixed-version environments, for instance where the VDAs have a different version to the Delivery Controller, are inevitable during some upgrades. Follow best-practice and minimize the time that Citrix components of different versions co-exist. In mixed-version environments, security policy, for example, might not be uniformly enforced.

> **Note:**
>
> This is typical of other software products. The use of an earlier version of Active Directory only partially enforces Group Policy with later versions of Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following scenario describes a security issue that can occur in a specific mixed-version Citrix environment. When Citrix Receiver 1.7 is used to connect to a virtual desktop running the VDA in XenApp and XenDesktop 7.6 Feature Pack 2, the policy setting **Allow file transfer between desktop and client** is enabled in the Site but cannot be disabled by a Delivery Controller running XenApp and XenDesktop 7.1. It does not recognize the policy setting, which was released in the later version of the product. This policy setting allows users to upload and download files to their virtual desktop, which is the security issue. To work around this, upgrade the Delivery Controller (or a standalone instance of Studio) to version 7.6 Feature Pack 2 and then use Group Policy to disable the policy setting. Alternatively, use local policy on all affected virtual desktops.

Remote PC Access security considerations

Remote PC Access implements the following security features:

- Smart card use is supported.
- When a remote session connects, the office PC's monitor appears as blank.
- Remote PC Access redirects all keyboard and mouse input to the remote session, except CTRL+ALT+DEL and USB-enabled smart cards and biometric devices.
- SmoothRoaming is supported for a single user only.
- When a user has a remote session connected to an office PC, only that user can resume local access of the office PC. To resume local access, the user presses Ctrl-Alt-Del on the local PC and then logs on with the same credentials used by the remote session. The user can also resume local access by inserting a smart card or leveraging biometrics, if your system has appropriate third-party Credential Provider integration. This default behavior can be overridden by enabling Fast User Switching via Group Policy Objects (GPOs) or by editing the registry.

> **Note:**
>
> Citrix recommends that you do not assign VDA administrator privileges to general session users.

Automatic assignments

By default, Remote PC Access supports automatic assignment of multiple users to a VDA. In XenDesktop 5.6 Feature Pack 1, administrators can override this behavior using the RemotePCAccess.ps1 PowerShell script. This release uses a registry entry to allow or prohibit multiple automatic remote PC assignments. This setting applies to the entire Site.

> **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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

To restrict automatic assignments to a single user:

On each Controller in the Site, set the following registry entry:

```
HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer
Name: AllowMultipleRemotePCAssignments
Type: REG_DWORD
Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
   multiple user assignment.
```

If there are any existing user assignments, remove them using SDK commands for the VDA to subsequently be eligible for a single automatic assignment.

- Remove all assigned users from the VDA: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- Remove the VDA from the Delivery Group: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

Restart the physical office PC.

Manage certificates

September 6, 2025

TLS uses certificates to establish trust between two parties. You must install a suitable certificate on each server providing a service, and ensure that machines connecting to that server trust that certificate. There are the following options for signing certificates:

- Self-signed certificates. These are not recommended. These are difficult to manage as you must manually copy this certificate to any other machine that must trust that certificate.
- Enterprise certification authority. If you have existing PKI in place, then this is normally the simplest option signing certificate for use between internal devices.
- Public certification authority. This requires that you prove ownership of the domain to the certificate authority. It has the advantage that unmanaged client devices are normally preconfigured to trust certificates from major public certification authorities.

Create a new certificate

Follow your organization's policies and procedures for creating certificates.

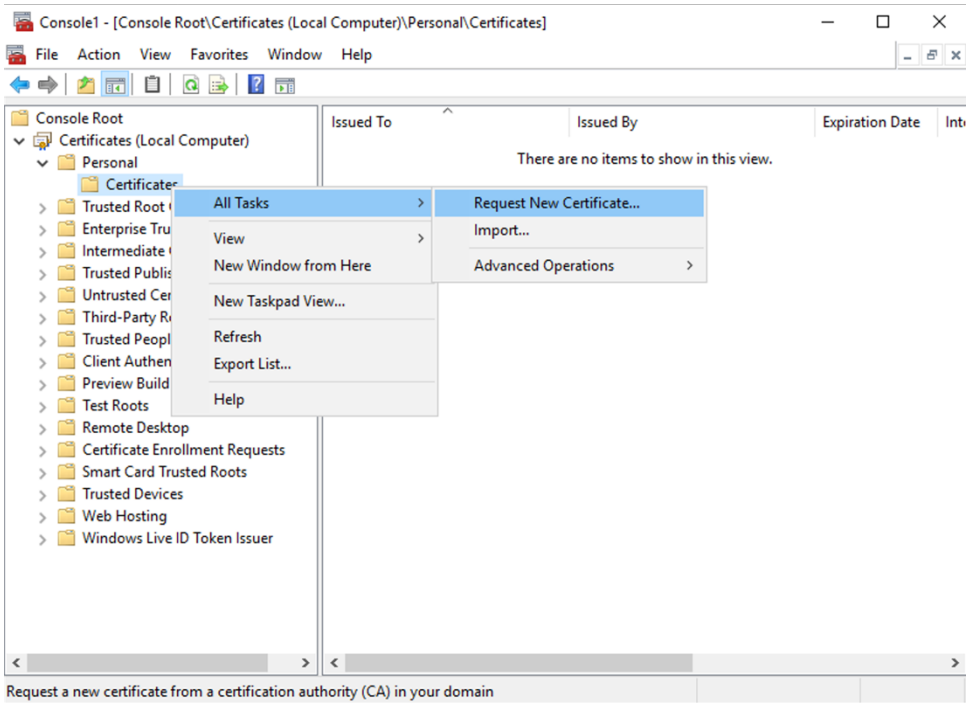
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create certificate using Microsoft Certificate Authority

If the Microsoft Certificate Authority is integrated into an Active Directory domain or into the trusted forest the Delivery Controllers are joined to, you can acquire a certificate from the Certificates MMC snap-in Certificate Enrollment wizard. The Microsoft Certificate Authority needs to have a certificate template published suitable for use by web servers.

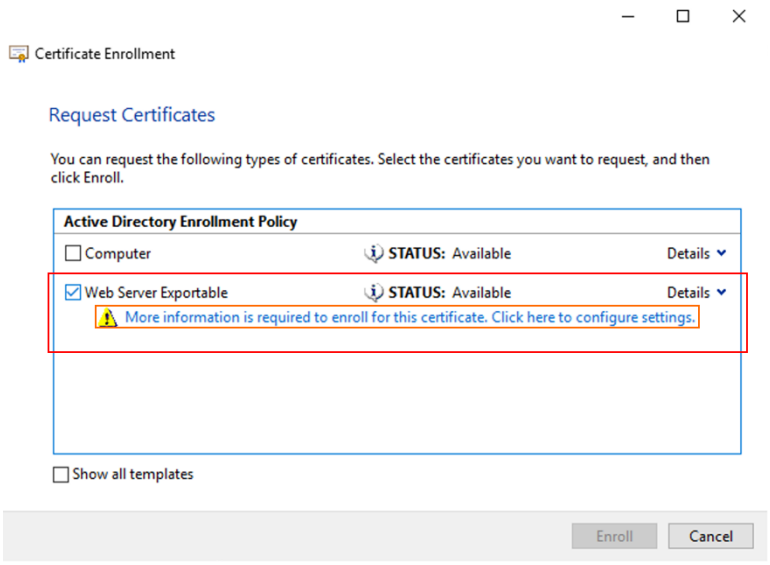
The root certificate is automatically deployed to other machine on the domain using group policy. Therefore all other machines on the domain trust certificates created using the Microsoft Certificate Authority. If you have machines not on the domain then you need to export the Root Certification Authority Certificate and import it into those machines.

1. On the server, open the MMC console and add the Certificates snap-in. When prompted select Computer account.
2. Expand **Personal > Certificates**, then use the **All Tasks > Request New Certificate** context menu command.



3. Click **Next** to begin, and **Next** to confirm that you are acquiring the certificate from Active Directory enrollment.
4. Select a suitable template such as **Web Server Exportable**. If the template has been set up to automatically provide the values for Subject you can click **Enroll** without providing more details. Otherwise click on **More information is required to enroll for this certificate. Click here to configure settings.**

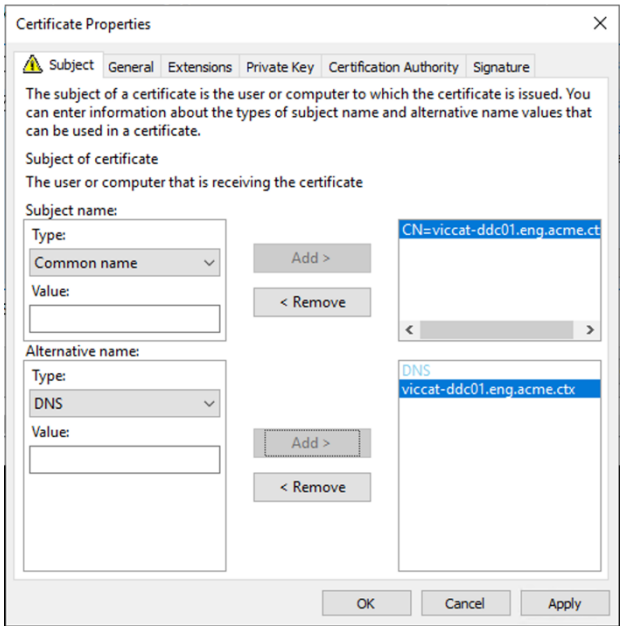
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. To provide more details for the certificate template, click the **Details** arrow button and configure the following:

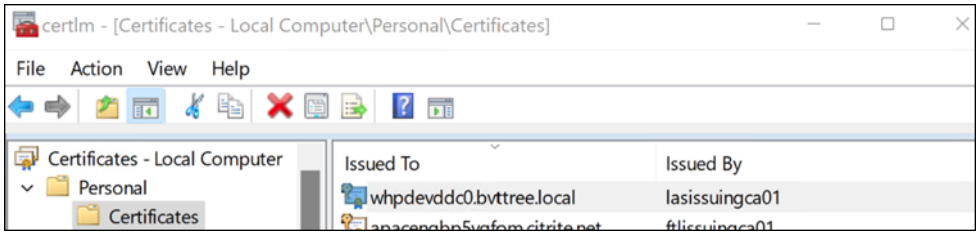
   Subject name: select Common Name and add the FQDN of the server.

   Alternative name: select DNS and add the FQDN of the server.



6. Press **OK**.
7. Press **Enroll** to create the certificate. It is displayed in the list of certificates.

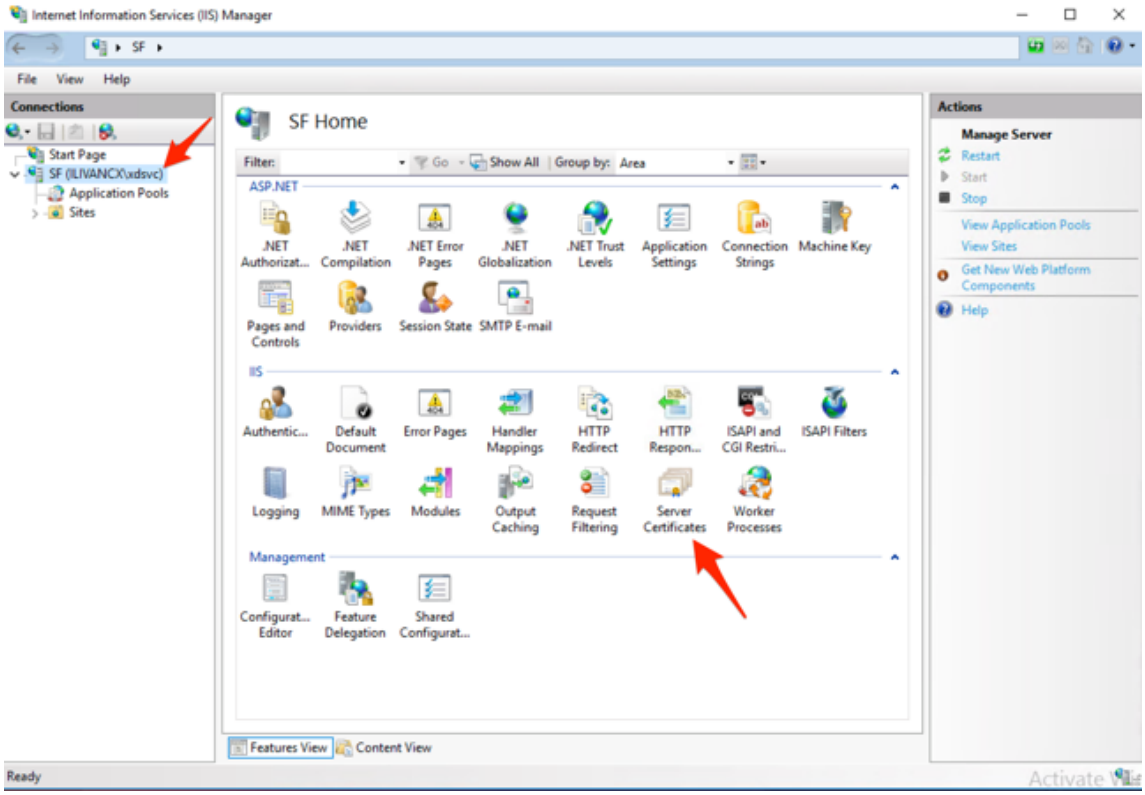
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a certificate request using IIS

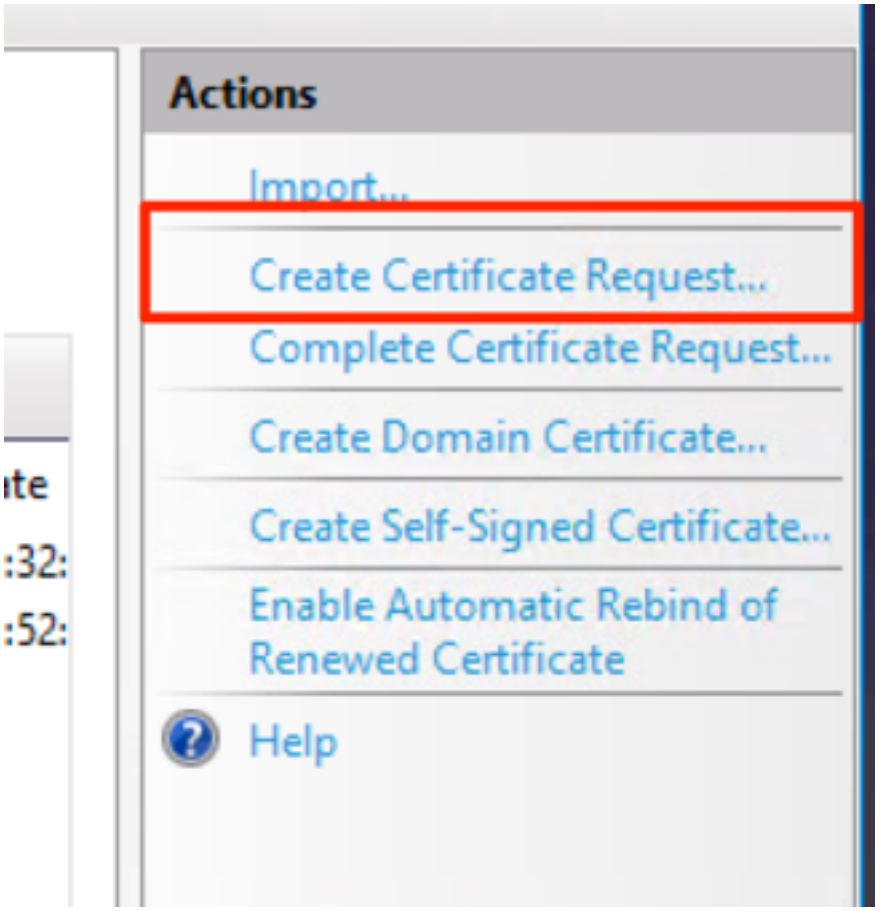
If IIS is installed on the server then complete the following steps:

1. Open **Internet Information Service (IIS) Manager**
2. Select the server node in the Connections list.
3. Open **Server Certificates**.



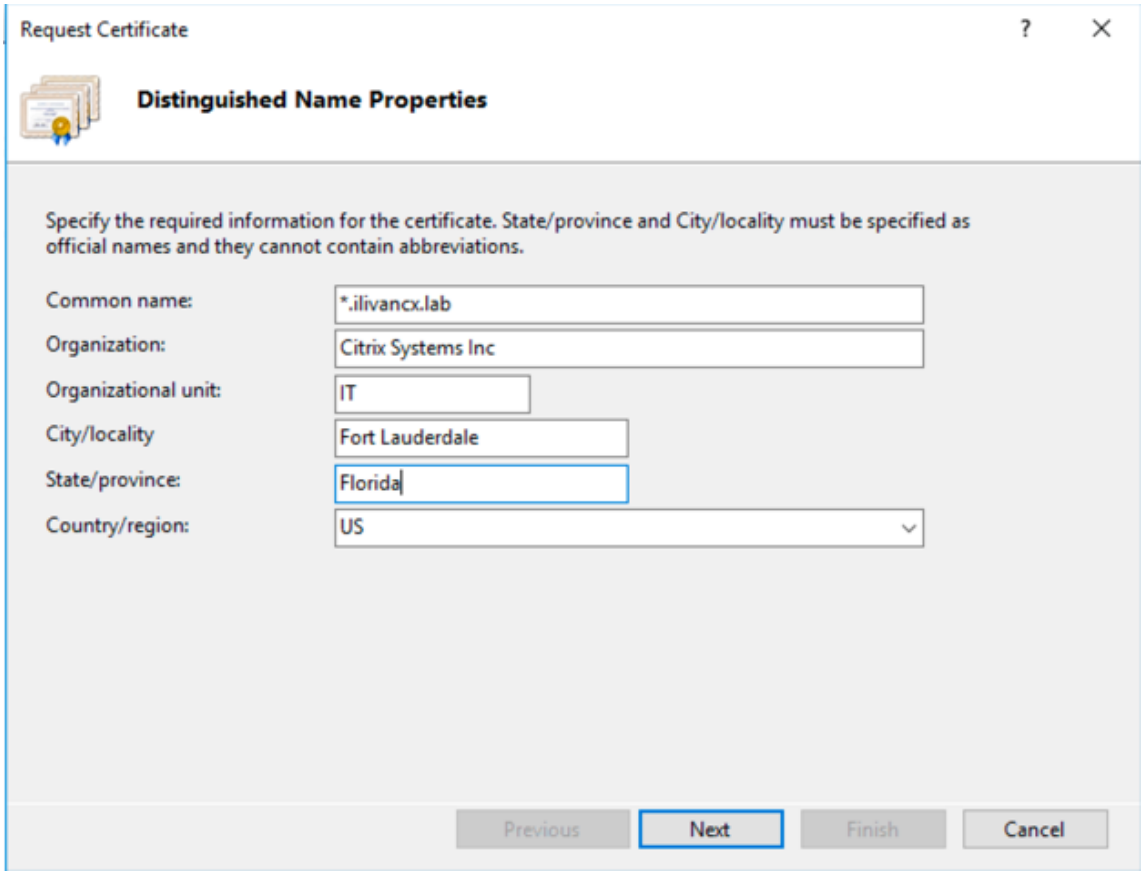
4. From the **Actions** pane, select **Create Certificate Request**....

© 1997–2026 Citrix Systems, Inc. All rights reserved.

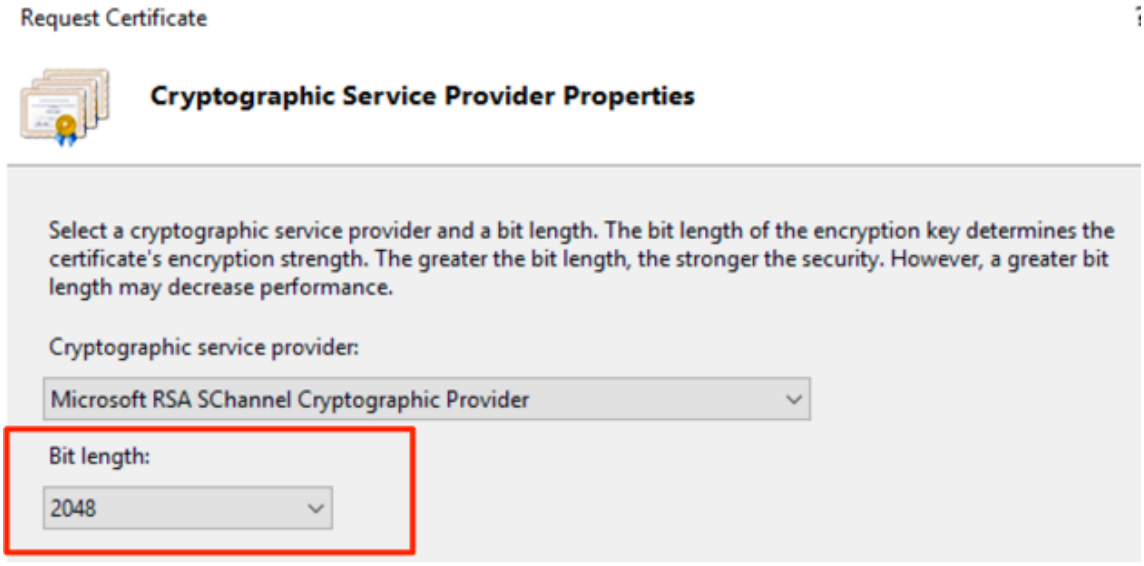


5. Enter the **Distinguished name properties**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

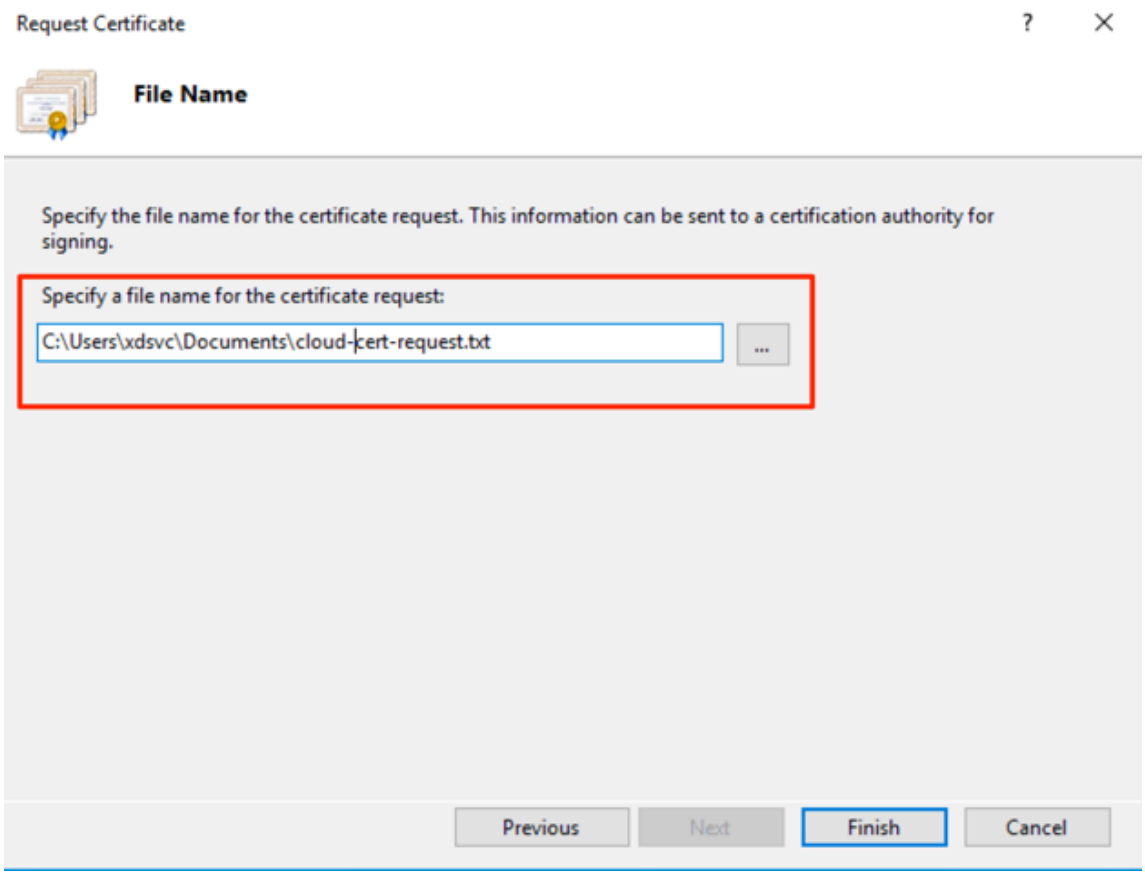


6. On the **Cryptographic Service Provider Properties** screen, leave the **Cryptographic service provider** as the default. Select a key size of **2048** or higher.



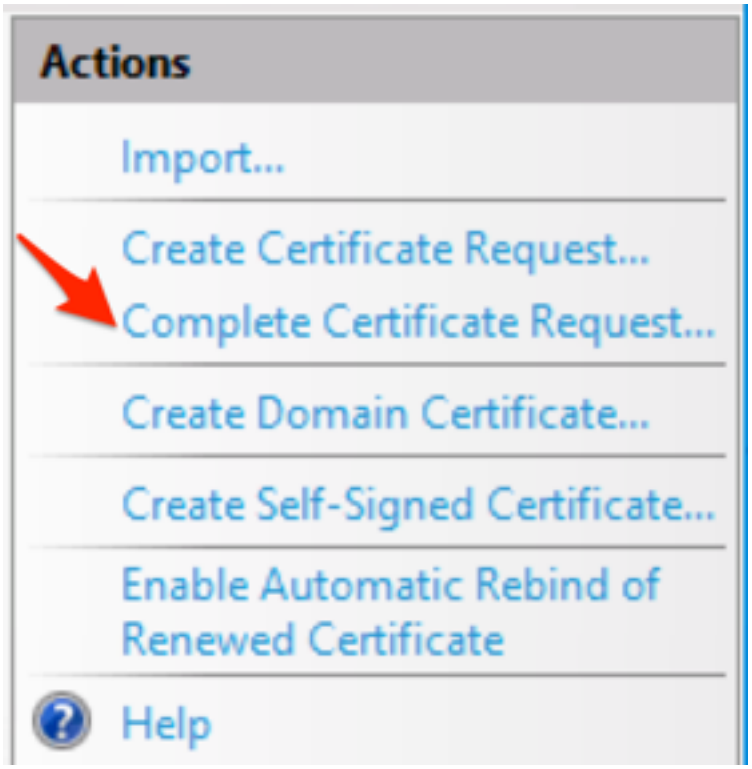
7. Choose a file name and press **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

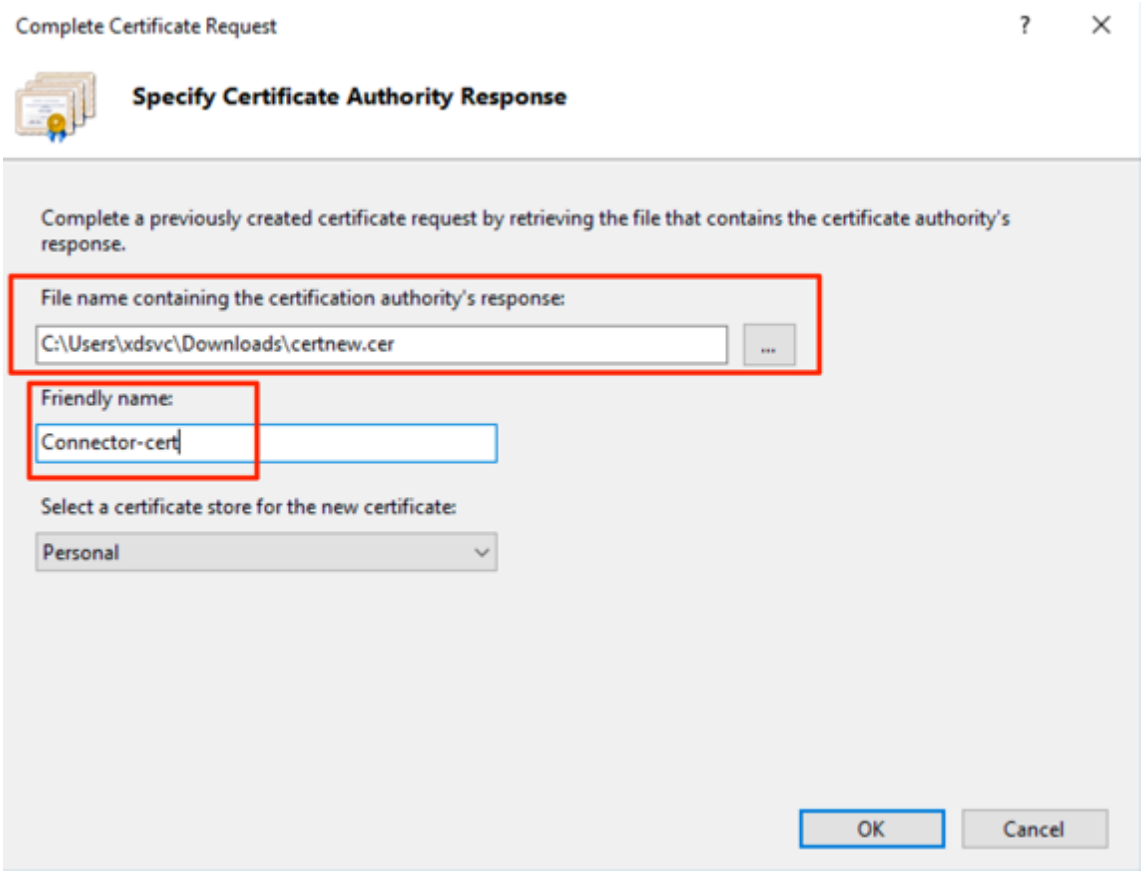


8. Upload your CSR to your certificate authority.
9. Once you have received the certificate, from the **Actions** pane, select **Complete Certificate Request…**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. Select the certificate, provide a **Friendly name** and press **OK**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

There is no way to set the subject alternative name. Therefore the certificate is limited to the server specified using the common name.

Create a certificate signing request from certificates snap-in

From within the Certificates mmc snap-in you can create a certificate signing request. This generates a file that you can send to a certificate authority who will provide the certificate. You must then import the certificate to combine it with the local private key.

1. On the server, open the MMC console and add the Certificates snap-in. When prompted select Computer account.
2. Expand **Personal** > **Certificates**
3. Select **All Tasks** > **Advanced Operations** > **Create Custom Request**.
4. On **Before You Begin**, select **Next**.
5. On the **Select Certificate Enrollment Policy** screen, select a suitable existing policy, or **Proceed without enrollment policy**.
6. On the **Custom request** screen, if using an enrolment policy, choose an appropriate template, if available, such as **Web Server Exportable**.
7. On the **Certificate Information** screen, expand **Details** and select **Properties**.
8. In the **Certificate Properties** window, on the **General** tab, enter a suitable friendly name.
9. On the **Subject tab**:
    a) Under **Subject name**, select **Common name** and enter the FQDN of the server. You can enter a wildcard. Select **Add**.
    b) Under **Subject name**, add appropriate values for Organization, Organizational Unit, Locality, State, Country.
    c) Under **Alternative name**, select **DNS**. Add the server FQDN. You may add multiple server FQDNs or a wildcard FQDN.
10. On the **Extensions** tab:
    - Under **Key usage** add **Digital signature** and **Key encipherment**.
    - Under **Extended Key Usage (application policies)**, add **Server Authentication** and **Client Authentication**.
11. On the **Private Key** tab.
    - Under **Select cryptographic Service Provider (CSP)** choose a suitable provider.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Under **Key options**, select a suitable key size. For RSA providers, at minimum use a key size of 2048. For greater security you may wish to choose 4096 but this will have a slight impact on performance.
- Under **Key options**, select **Make private key exportable**.

12. Select **OK**.
13. Select **Next**.
14. Select **Browse** and save your request.
15. Select **Finish**.
16. Upload your CSR to your certificate authority.
17. Once you have received the certificate, import it on the same server so it is linked to the private key.

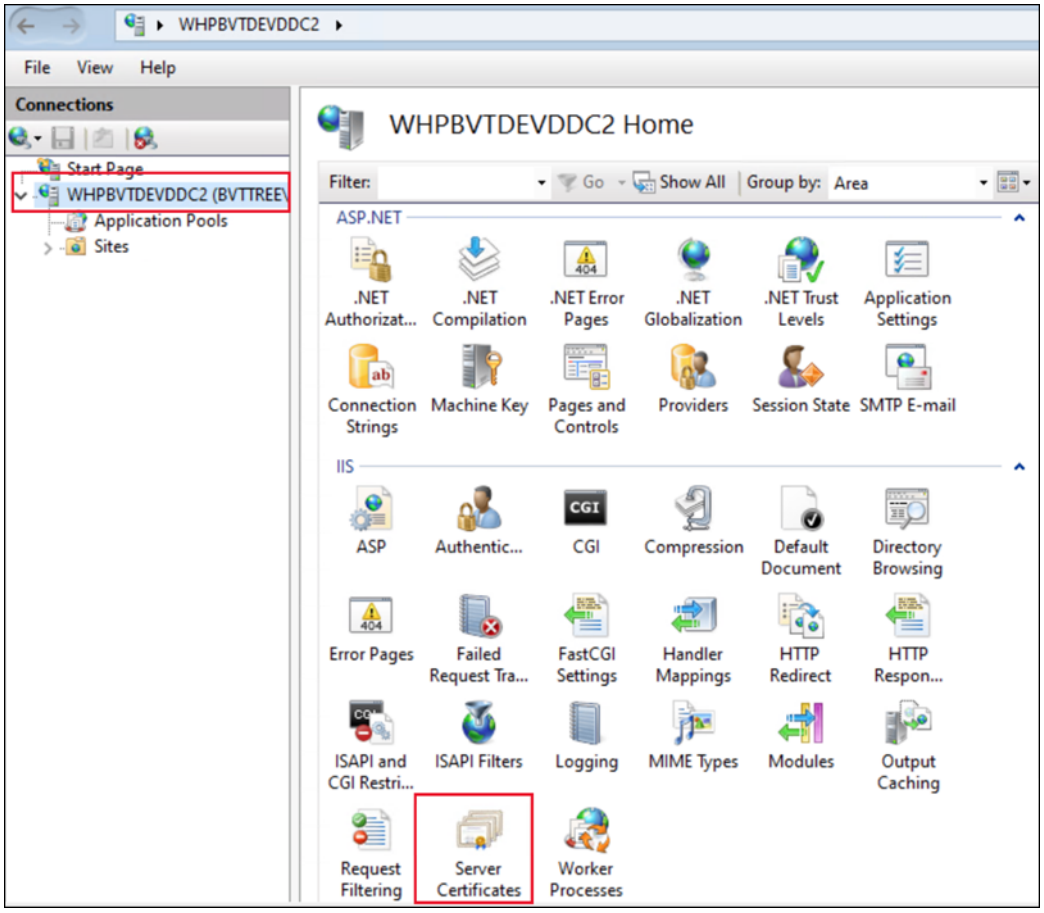
Create a new self-signed certificate

A self-signed certificate is created during installation of a delivery controller™ and web studio. You can generate a new self-signed certificate and use it to replace the existing one.

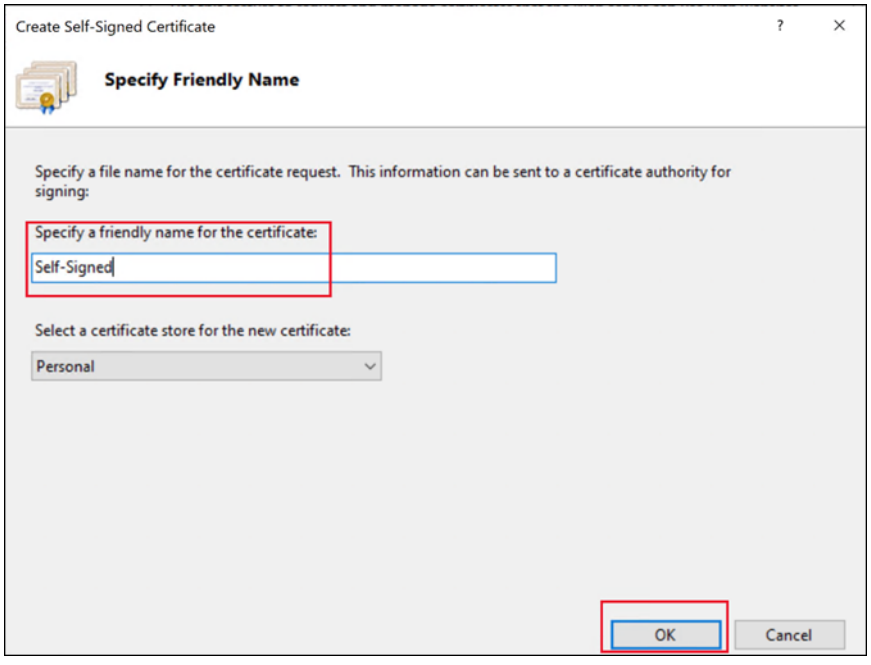
Using IIS manager If IIS is installed on the server then you can perform the following steps:

1. Log on to the server as an administrator.
2. Open the IIS Manager
3. Open **Server Certificates**
4. In the **Actions** pane, select **Create Self-Signed Certificate**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. In **Create Self-Signed Certificate**, enter a name for the certificate and click **OK**. The self-signed certificate is then created.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using PowerShell You can use PowerShell to create a self-signed certificate:

```
$certSubject = "CN=myddc.example.com" # The FQDN of the server.
$friendlyName = "Self-Signed-3"
$expireYears = 5

## Create new self-signed certificate under LocalMachine\My
$certificate = New-SelfSignedCertificate -Subject $certSubject -
    CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy
    Exportable -KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -
    HashAlgorithm SHA256 -FriendlyName $friendlyName -NotAfter $([System
    .DateTime]::Now.AddYears($expireYears))

# Add to trusted root certificates
$rootCertStore = Get-Item "Cert:\LocalMachine\Root\"
$rootCertStore.Open([System.Security.Cryptography.X509Certificates.
    OpenFlags]::ReadWrite)
$rootCertStore.Add($certificate)
```

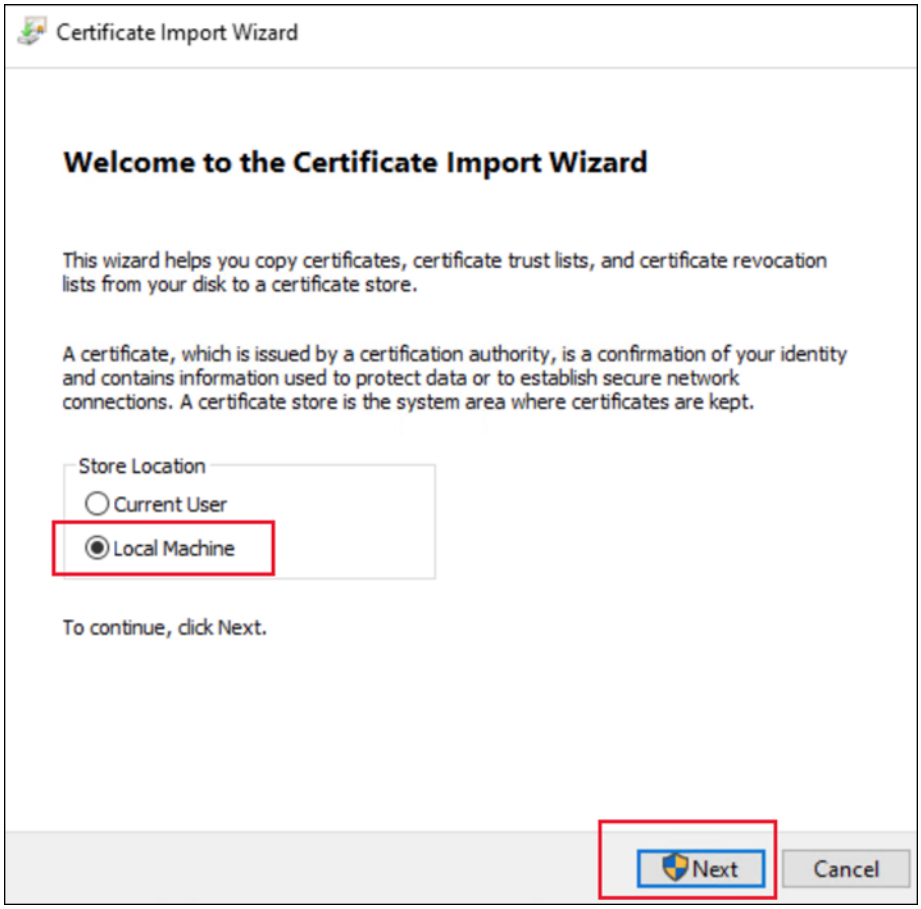
Import existing certificate

You can import an existing certificate into the server using any of the following methods.

Certificate import wizard

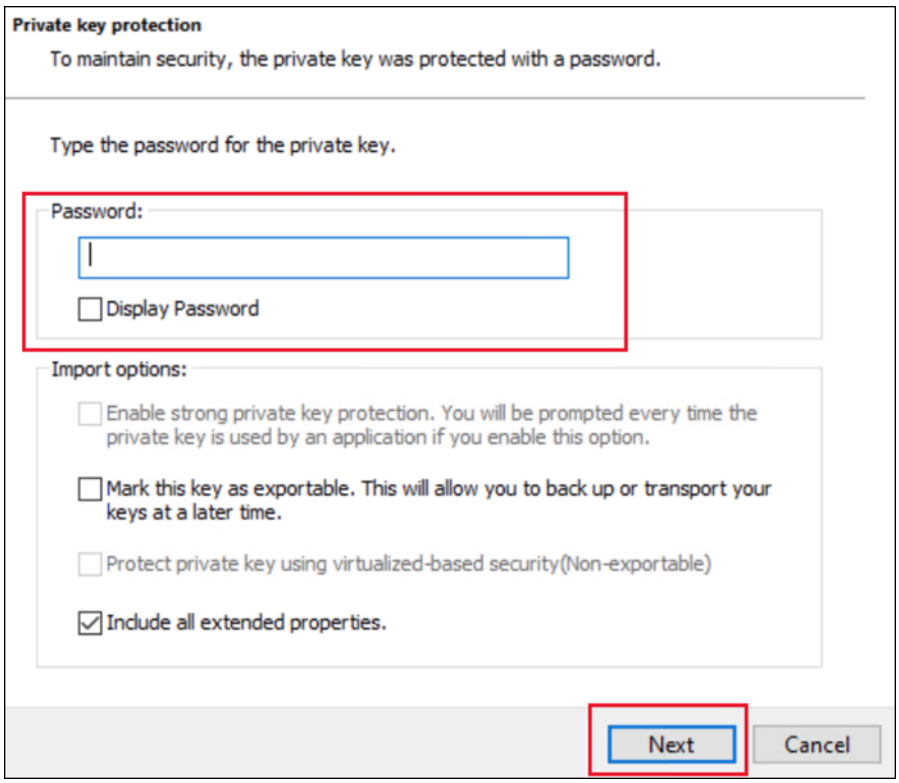
1. Double click the PFX file, or right click the file and select **Install PFX**. This opens the **Certificate Import Wizard**.
2. For **Store Location**, select **Local Machine**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



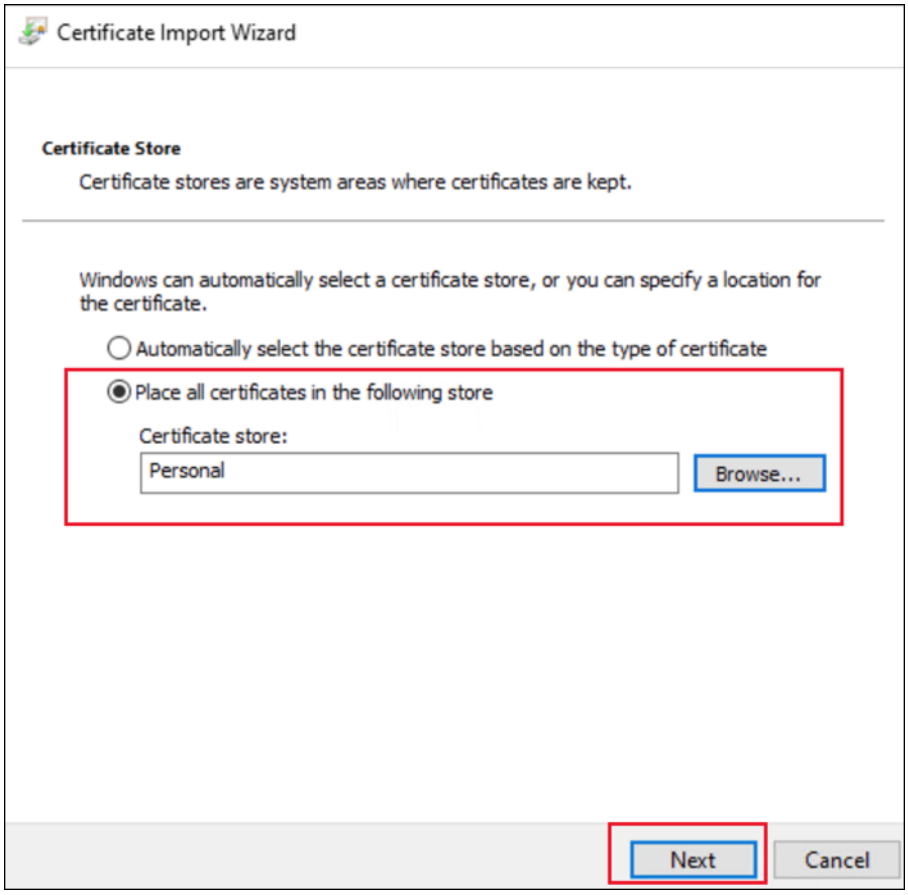
3. Enter the password if required.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



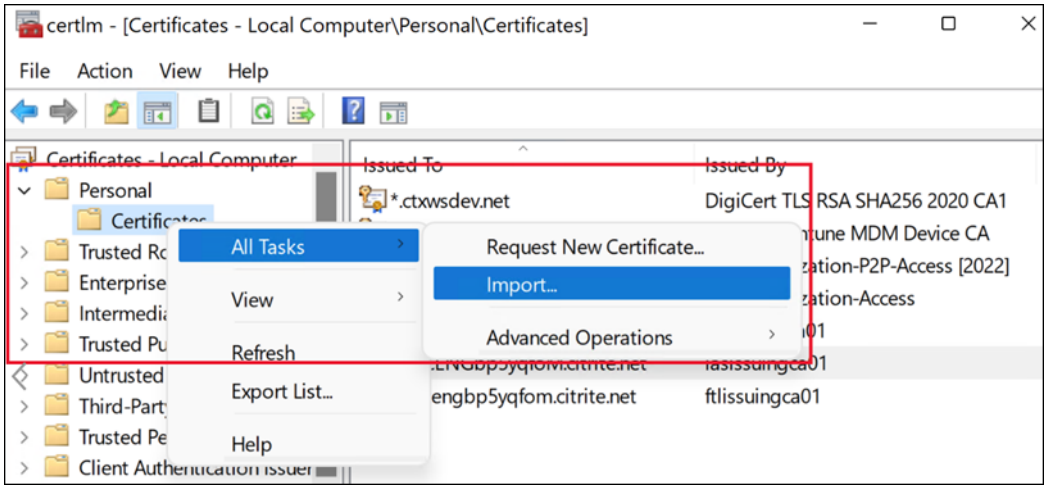
4. Select the **Certificate Store**. For server certificates, choose **Personal**. If this is a root certificate or self-signed certificate that you wish to trust from this machine then choose **Trusted Root Certification Authorities**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use the Manage Computer certificates console

1. Open the Manage Computer Certificates console and navigate to the appropriate certificate store. For server certificates this is normally. **Personal** > **Certificates**. To trust a root or self-signed certificate, choose **Trusted Root Certification Authorities** > **Certificates**.
2. Right click the certificate and select > **All Tasks** > **Import**....



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select **Browse...** and select the file.
4. Enter the password if required.

Use PowerShell

To import a certificate, use the PowerShell cmdlet Import-PfxCertificate. For example, to import certificate `certificate.pfx` with password 123456 into the personal certificate store, run the following command:

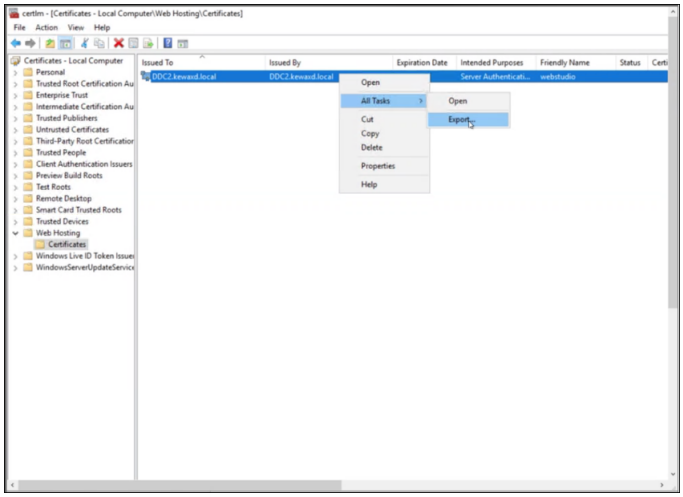
```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String "
    123456" -AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\
    My\ -FilePath .\Desktop\certificate.pfx
```

To import a trusted root certificate, set the `CertStoreLocation` to `Cert:\LocalMachine\Root\`.

Export certificate without private key

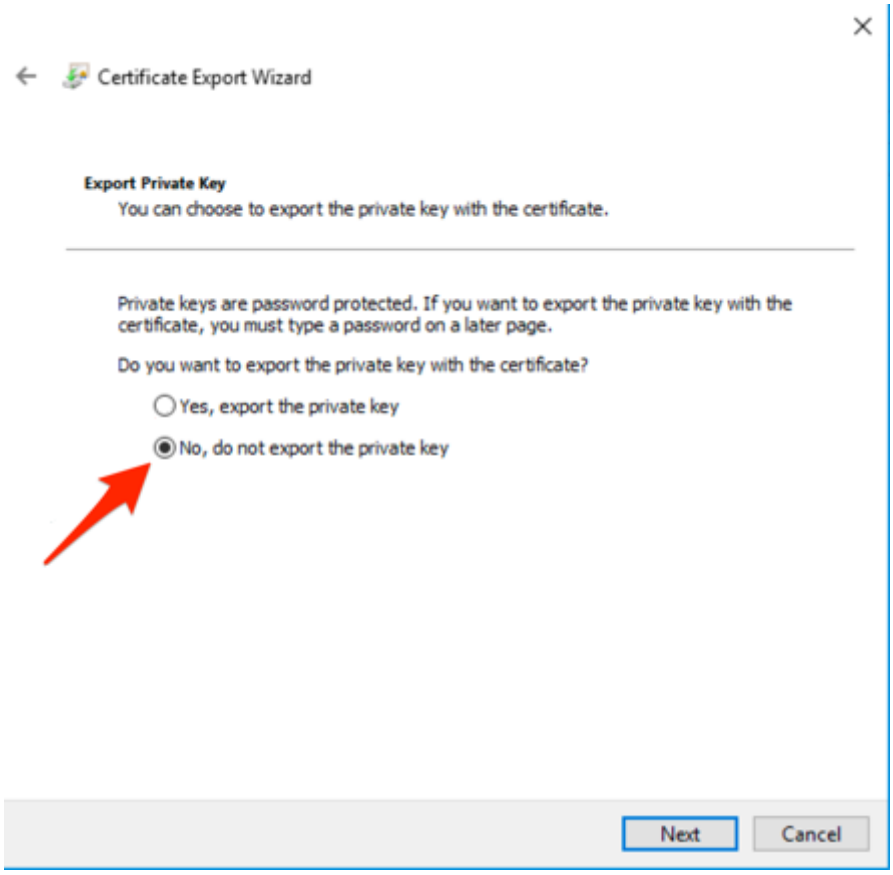
To export a certificate so that you can import it into other devices to trust the certificate, you should exclude the private key.

1. Open the Manage Computer Certificates. Navigate to **Personal** > **Certificates** and select the certificate you wish to export.
2. From the **Action** menu, select **All Tasks** then **Export**.

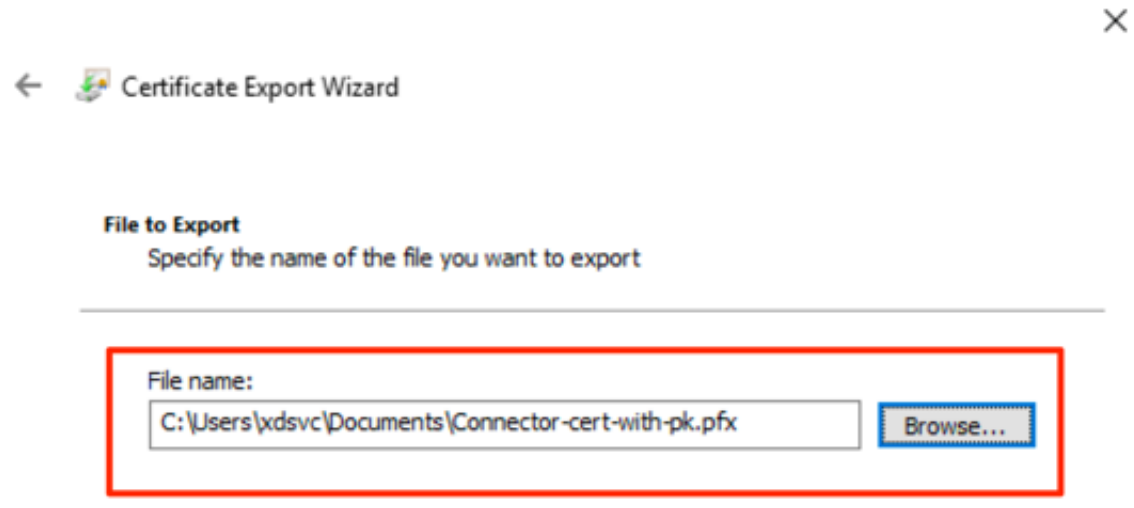


3. Choose **No, do not export the private key**, then press **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Select format **DER encoded binary X.509 (.CER)** (the default) and press **Next**.
5. Enter a file name and press **Next**.



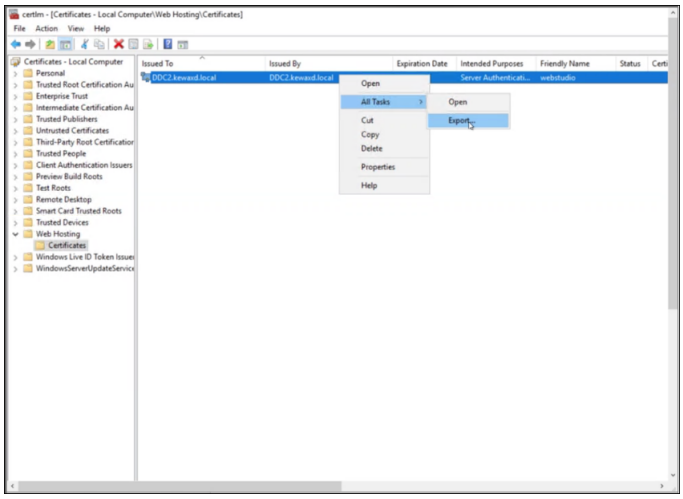
6. Select **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Export certificate with private key

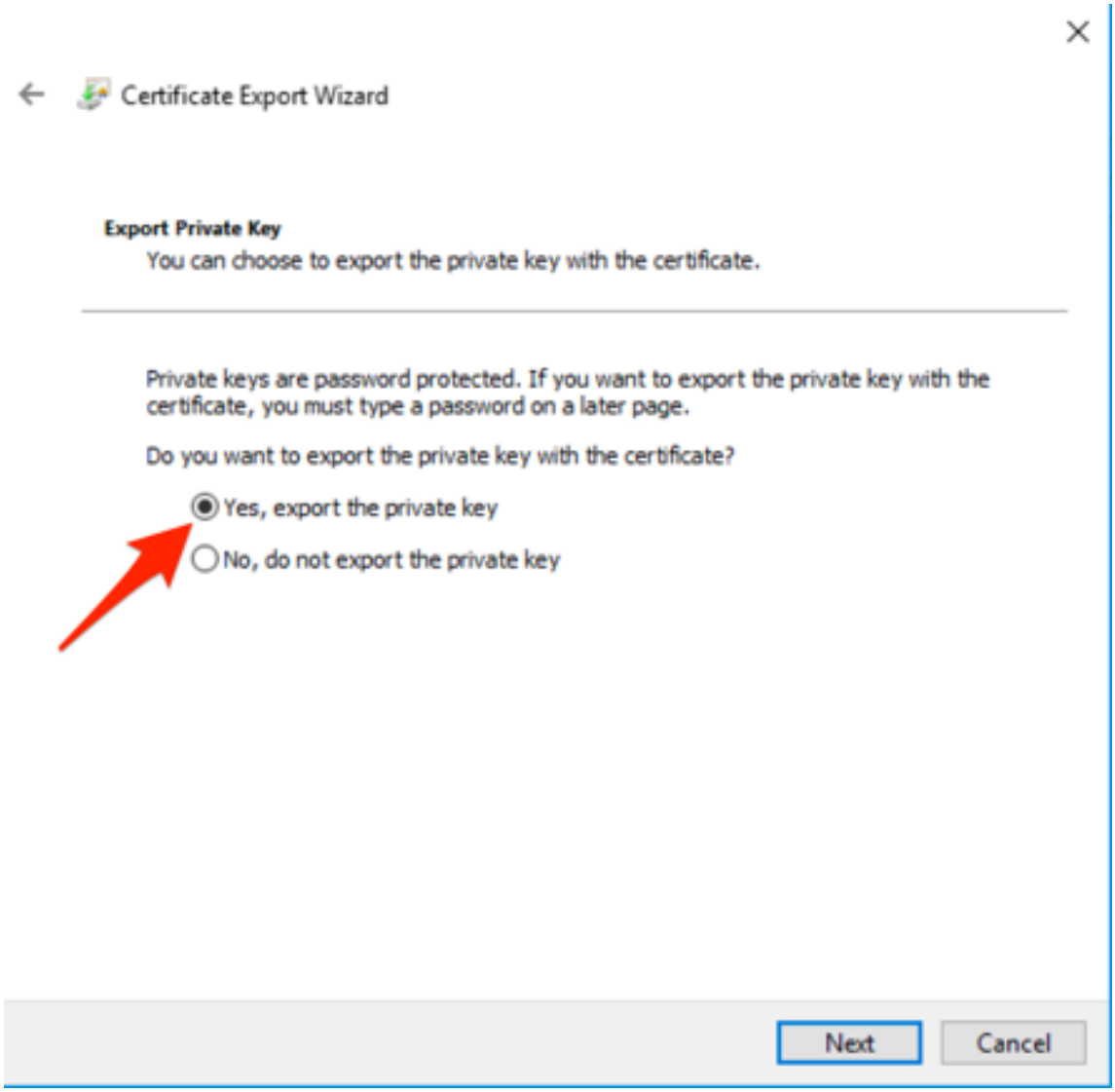
To export a certificate so that you can use it on other servers, you must include the private key.

1. Open the Manage Computer Certificates. Navigate to **Personal** > **Certificates** and select the certificate you wish to export.
2. From he **Action** menu, select **All Tasks** then **Export**.



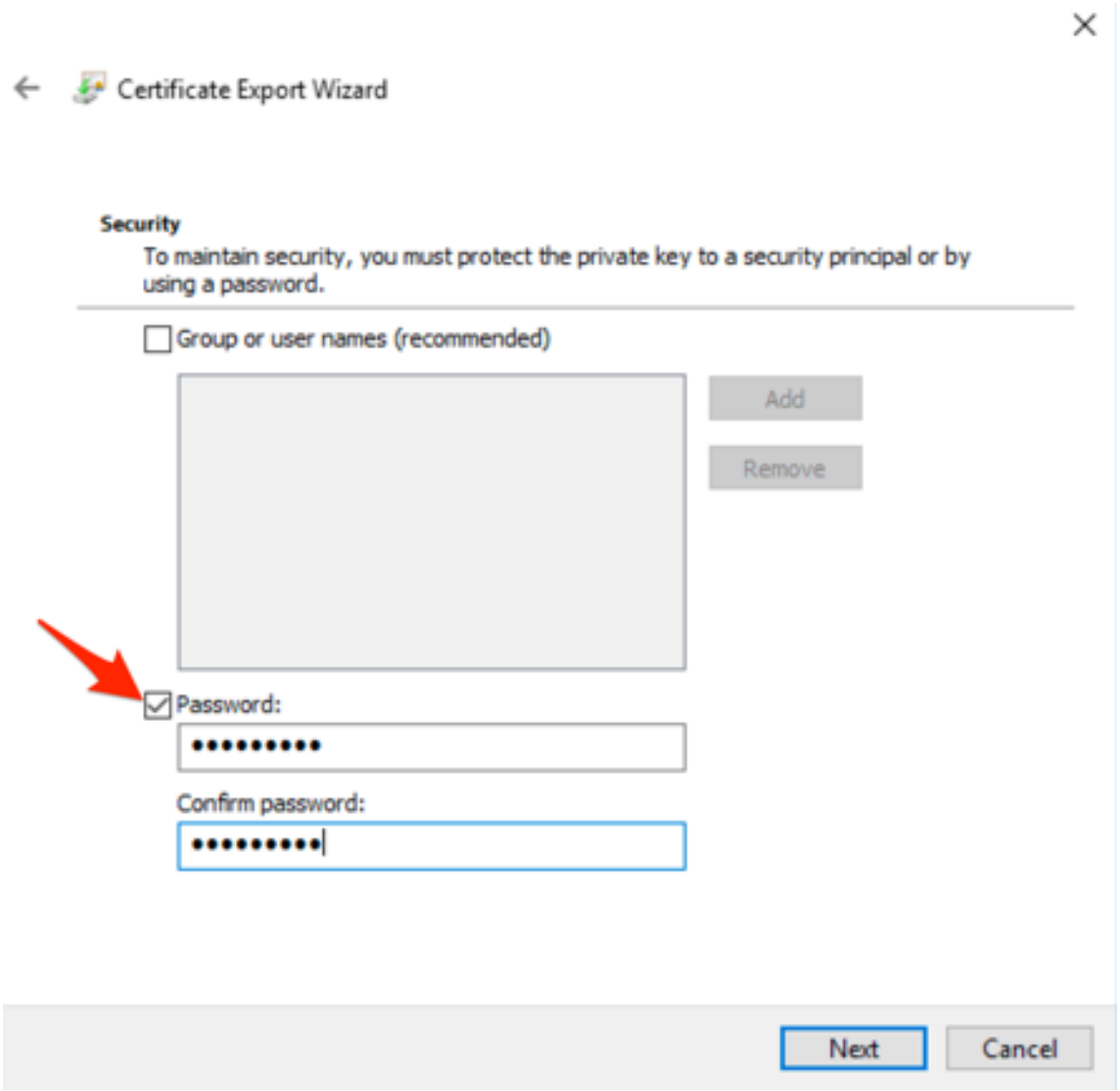
3. Choose **Yes, export the private key**, then select **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



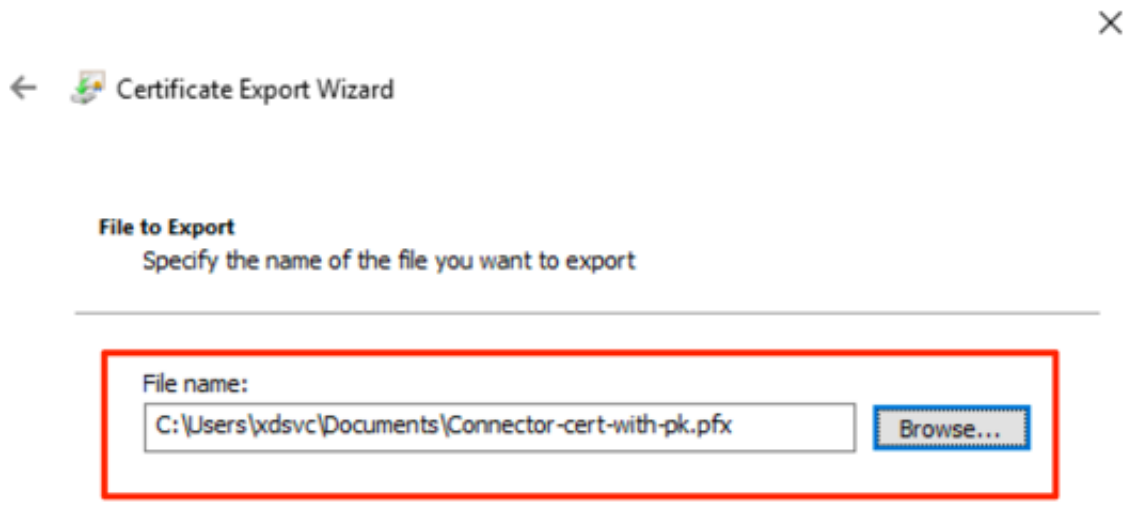
4. On the **Security** tab, enter a password then select **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Enter a file name and select **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Select **Finish**.

Convert certificate to PEM format

By default, Windows exports certificates in PKCS#12 format as a .pfx file in that includes the private key. To use the certificate on a NetScaler® Gateway or license server, you must extract the certificate and private keys into separate files in PEM format. You can do this using openssl.

To export the certificate in PEM format run:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
openssl pkcs12 -in name.pfx -clcerts -nokeys -out name.cer
```

It will ask you for the existing password and a new passphrase

To export the key in PEM format run:

```
openssl pkcs12 -in name.pfx -nocerts -out name.key
```

Trusting certificates

- If you use a certificate from a public certificate authority then devices are normally pre-configured with the root certificates.
- If you use an enterprise certificate authority then you must deploy the root certificate into any devices that must trust that certificate. If using Active Directory Certification Services, the root certificates are also deployed to all machines on the domain using Group Policy. You must manually import the root certificate onto non-domain-joined machines such as your NetScaler gateways, or machines on other domains.
- If you are using a self signed certificate then this must be manually installed onto any machine that needs to trust the certificate.

To export a self-signed or trusted root certificate from Windows, see export certificate without private key.

For Windows to trust the certificate, you must import the certificate into the **Trusted Root Certification Authorities** store. If using PowerShell, enter the store **Cert:\LocalMachine\Root**.

For NetScaler to trust the certificate, first convert the certificate to PEM format, then Install the root certificate.

Smart cards

September 6, 2025

Smart cards and equivalent technologies are supported within the guidelines described in this article. To use smart cards with Citrix Virtual Apps or Citrix Virtual Desktops™:

- Understand your organization's security policy concerning the use of smart cards. These policies might, for example, state how smart cards are issued and how users must safeguard them. Some aspects of these policies might need to be reassessed in a Citrix Virtual Apps™ or Citrix Virtual Desktops environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Determine which user device types, operating systems, and published applications are to be used with smart cards.
- Familiarize yourself with smart card technology and your selected smart card vendor hardware and software.
- Know how to deploy digital certificates in a distributed environment.

> **Note:**
>
> Smart card enrollment is not supported with fast smart card. Smart card enrollment might work when fast smart card is disabled, but depends on the type of smart card and middleware. Contact your smart card and middleware vendor for information on their integration with Citrix Virtual Apps and Desktops and support for smart card enrollment over virtual sessions.

Types of smart cards

Enterprise and consumer smart cards have the same dimensions, electrical connectors, and fit the same smart card readers.

Smart cards for enterprise use contain digital certificates. These smart cards support Windows Logon, and can also be used with applications for digital signing and encryption of documents and email. Citrix Virtual Apps and Desktops™ support these uses.

Smart cards for consumer use do not contain digital certificates; they contain a shared secret. These smart cards can support payments (such as a chip-and-signature or chip-and-PIN credit card). They do not support Windows Logon or typical Windows applications. Specialized Windows applications and a suitable software infrastructure (including, for example, a connection to a payment card network) are needed for use with these smart cards. Contact your Citrix representative for information on supporting these specialized applications on Citrix Virtual Apps or Citrix Virtual Desktops.

For enterprise smart cards, there are compatible equivalents that can be used in a similar way.

- A smart card-equivalent USB token connects directly to a USB port. These USB tokens are usually the size of a USB flash drive, but can be as small as a SIM card used in a mobile phone. They appear as the combination of a smart card plus a USB smart card reader.
- A virtual smart card using a Windows Trusted Platform Module (TPM) appears as a smart card. These virtual smart cards are supported for Windows 8 and Windows 10, using Citrix Workspace app (minimum version Citrix Receiver 4.3).
    - Versions of Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) earlier than XenApp and XenDesktop 7.6 FP3 do not support virtual smart cards.
    - For more information on virtual smart cards, see Virtual Smart Card Overview.

    Note: The term "virtual smart card"is also used to describe a digital certificate stored on the user computer. These digital certificates are not strictly equivalent to smart cards.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Apps and Desktops smart card support is based on the Microsoft Personal Computer/Smart Card (PC/SC) standard specifications. A minimum requirement is that smart cards and smart card devices must be supported by the underlying Windows operating system and must be approved by the Microsoft Windows Hardware Quality Labs (WHQL) to be used on computers running qualifying Windows operating systems. See the Microsoft documentation for additional information about hardware PC/SC compliance. Other types of user devices might comply with the PS/SC standard. For more information, refer to the Citrix Ready program.

Usually, a separate device driver is needed for each vendor's smart card or equivalent. However, if smart cards conform to a standard such as the NIST Personal Identity Verification (PIV) standard, it might be possible to use a single device driver for a range of smart cards. The device driver must be installed on both the user device and the Virtual Delivery Agent (VDA). The device driver is often supplied as part of a smart card middleware package available from a Citrix partner; the smart card middleware package offers advanced features. The device driver might also be described as a Cryptographic Service Provider (CSP), Key Storage Provider (KSP), or minidriver.

The following smart card and middleware combinations for Windows systems have been tested by Citrix as representative examples of their type. However, other smart cards and middleware can also be used. For more information about Citrix-compatible smart cards and middleware, see http://www.citrix.com/ready.

Middleware	Matching cards
Gemalto Mini Driver for .NET card	Gemalto .NET v2+

For information about smart card usage with other types of devices, see the Citrix Workspace™ app documentation for that device.

Remote PC Access

Smart cards are supported only for remote access to physical office PCs running Windows 10, Windows 8 or Windows 7.

The following smart cards were tested with Remote PC Access:

Middleware	Matching cards
Gemalto .NET minidriver	Gemalto .NET v2+

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fast smart card

Fast smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance when smart cards are used in high-latency WAN situations. When latency is high, the performance improvement can be significant (for example, 15 seconds for a Windows fast smart card logon versus more than 1 minute with the PC/SC-based smart card redirection).

Fast smart card is enabled by default on host machines with currently supported Windows VDAs. To disable Fast Smart Card on the host-side—for example for diagnostic purposes—set the 'Disable Cryptographic Redirection' registry setting to any non-zero value:

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
```

On the client side, to enable fast smart card, include the SmartCardCryptographicRedirection ICA parameter in the *default.ica* file of the associated StoreFront site:

```
[WFClient]
SmartCardCryptographicRedirection=On
```

In addition, on the client side, fast smart card can be force enabled or force disabled (for example, for diagnostic purposes) with the following registry settings:

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (as a non-zero DWORD)

Or

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (as a non-zero DWORD)

The 32-bit registry hive must be specified (using `WOW6432Node`) if the client machine is 64-bit.

Limitations:

- Only Citrix Workspace app for Windows supports fast smart card. If you configure fast smart cards in the default.ica file, Citrix Workspace apps that are not for Windows still use existing PC/SC Redirection.
- The only double-hop scenarios that fast smart card supports are ICA® > ICA with fast smart card enabled on both hops. Because fast smart card doesn't support ICA > RDP double-hop scenarios, those scenarios don't work.
- Fast smart card doesn't support Cryptography Next Generation. Thus, fast smart card doesn't support Elliptic Curve Cryptography (ECC) smart cards.
- Fast smart card supports only read-only key container operations.
- Fast smart card doesn't support changing the smart card PIN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Starting with VDA version 2203 and Citrix Workspace app version 2202 for Windows (or later) fast smart card is compatible with Cryptography Next Generation (CNG). In addition, Elliptic Curve Cryptography (ECC) smart cards are supported with the following curves: P-256, P-384, P-521 bits, for both ECDSA and ECDH.

Starting with VDA version 2203, fast smart card adds the ability to cache the smart card PIN between the applications from the same user's logon session. For example, if **Session PIN Caching** is enabled and the end user has previously provided their smart card PIN to Outlook, when Word is then used to sign a document, Word uses the already cached smart card PIN (submitted to Outlook). **Session PIN Caching** helps the user experience by reducing the number of times the user has to enter their smart card PIN. In addition, if the smart card is used to log on to the VDA, the Windows smart card logon PIN can optionally be saved to the **Session PIN Cache**. This can further improve the user experience.

Session PIN Caching is disabled by default. It can be enabled and controlled with the following registry settings on the VDA:

In HKLM\SOFTWARE\Citrix\SmartCard:

- `EnablePinSessionCache` as a DWORD (non-zero to enable)
- `EnableLogonPinSessionCache` as a DWORD (non-zero to enable)
- `PinSessionCacheEntryStaleTimeout` as a DWORD (number of seconds before an entry becomes stale, default is 1 hour)

Types of smart card readers

A smart card reader might be built in to the user device, or be separately attached to the user device (usually via USB or Bluetooth). Contact card readers that comply with the USB Chip/Smart Card Interface Devices (CCID) specification are supported. They contain a slot or swipe into which the user inserts the smart card. The Deutsche Kreditwirtschaft (DK) standard defines four classes of contact card readers.

- Class 1 smart card readers are the most common, and usually contain a slot. Class 1 smart card readers are supported, usually with a standard CCID device driver supplied with the operating system.
- Class 2 smart card readers also contain a secure keypad that cannot be accessed by the user device. Class 2 smart card readers might be built into a keyboard with an integrated secure keypad. For class 2 smart card readers, contact your Citrix representative; a reader-specific device driver might be required to enable the secure keypad capability.
- Class 3 smart card readers also contain a secure display. Class 3 smart card readers are not supported.
- Class 4 smart card readers also contain a secure transaction module. Class 4 smart card readers are not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The smart card reader class is unrelated to the USB device class.

Smart card readers must be installed with a corresponding device driver on the user device.

For information about supported smart card readers, see the documentation for the Citrix Workspace app you are using. In the Citrix Workspace app documentation, supported versions are listed in a smart card article or in the system requirements article.

User experience

Smart card support is integrated into Citrix Virtual Apps and Desktops, using a specific ICA/HDX smart card virtual channel that is enabled by default.

Important: Do not use generic USB redirection for smart card readers. This is disabled by default for smart card readers, and is not supported if enabled.

Multiple smart cards and multiple readers can be used on the same user device, but if pass-through authentication is in use, only one smart card must be inserted when the user starts a virtual desktop or application. When a smart card is used within an application (for example, for digital signing or encryption functions), there might be other prompts to insert a smart card or enter a PIN. This can occur if more than one smart card has been inserted at the same time.

- If users are prompted to insert a smart card when the smart card is already in the reader, they must select Cancel.
- If users are prompted for the PIN, they must enter the PIN again.

You can reset PINs using a card management system or vendor utility.

> **Important:**
>
> Within a Citrix Virtual Apps or Citrix Virtual Desktops session, using a smart card with the Microsoft Remote Desktop Connection application is not supported. This is sometimes described as a "double hop"use.

Before deploying smart cards

- Obtain a device driver for the smart card reader and install it on the user device. Many smart card readers can use the CCID device driver supplied by Microsoft.
- Obtain a device driver and cryptographic service provider (CSP) software from your smart card vendor, and install them on both user devices and virtual desktops. The driver and CSP software must be compatible with Citrix Virtual Apps and Desktops; check the vendor documentation for compatibility. For virtual desktops using smart cards that support and use the minidriver

© 1997–2026 Citrix Systems, Inc. All rights reserved.

model, smart card minidrivers download automatically, but you can also obtain them from http://catalog.update.microsoft.com or from your vendor. Also, if PKCS#11 middleware is required, obtain it from the card vendor.

- Important: Citrix recommends that you install and test the drivers and CSP software on a physical computer before installing Citrix software.
- Add the Citrix Receiver™ for Web URL to the Trusted Sites list for users who use smart cards in Internet Explorer with Windows 10. In Windows 10, Internet Explorer does not run in protected mode by default for trusted sites.
- Ensure that your public key infrastructure (PKI) is configured appropriately. This includes ensuring that certificate-to-account mapping is correctly configured for Active Directory environment and that user certificate validation can be performed successfully.
- Ensure that your deployment meets the system requirements of the other Citrix components used with smart cards, including Citrix Workspace app and StoreFront.
- Ensure access to the following servers in your Site:
    - The Active Directory domain controller for the user account that is associated with a logon certificate on the smart card
    - Delivery Controller™
    - Citrix StoreFront
    - Citrix Gateway/Citrix Access Gateway 10.x
    - VDA
    - (Optional for Remote PC Access): Microsoft Exchange Server

Enable smart card use

Step 1. Issue smart cards to users according to your card issuance policy.

Step 2. (Optional) Set up the smart cards to enable users for Remote PC Access.

Step 3. Install and configure the Delivery Controller and StoreFront (if not already installed) for smart card remoting.

Step 4. Enable StoreFront for smart card use. For details, see Configure smart card authentication in the StoreFront documentation.

Step 5. Enable Citrix Gateway/Access Gateway for smart card use. For details, see Configuring Authentication and Authorization and Configuring Smart Card Access with the Web Interface in the NetScaler documentation.

Step 6. Enable VDAs for smart card use.

- Ensure that the VDA has the required applications and updates.
- Install the middleware.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Set up smart card remoting, enabling the communication of smart card data between Citrix Workspace app on a user device and a virtual desktop session.

Step 7. Enable user devices (including domain-joined or non-domain-joined machines) for smart card use. See Configure smart card authentication in the StoreFront documentation for details.

- Import the certificate authority root certificate and the issuing certificate authority certificate into the device's keystore.
- Install your vendor's smart card middleware.
- Install and configure Citrix Workspace app for Windows, being sure to import icaclient.adm using the Group Policy Management Console and enable smart card authentication.

Step 8. Test the deployment. Ensure that the deployment is configured correctly by launching a virtual desktop with a test user's smart card. Test all possible access mechanisms (for example, accessing the desktop through Internet Explorer and Citrix Workspace app).

Track smart card reader insertion count

With smart card remoting, you can track the number of times a smart card has been inserted or removed from a reader using the SCardGetStatusChange function. The function updates an array of SCARD_READERSTATE data structures—one per each reader you monitor. The high word (16 bits) of the dwEventState field of each SCARD_READERSTATE contains the reader count. For more information, see the Microsoft articles SCardGetStatusChangeA function and SCARD_READERSTATEA structure.

The **Reader Insert Count Reporting** setting is disabled by default. To enable tracking, add the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

Name: EnableReaderInsertCountReporting

Type: DWORD

Value: Any non-zero value

When the session disconnects, the count resets to zero.

Reader Insert Count Reporting is compatible with third-party smart card middleware.

Smart card deployments

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following types of smart card deployments are supported by this product version and by mixed environments containing this version. Other configurations might work but are not supported.

Type	StoreFront™ connectivity
Local domain-joined computers	Directly connected
Remote access from domain-joined computers	Connected through Citrix Gateway
Non-domain-joined computers	Directly connected
Remote access from non-domain-joined computers	Connected through Citrix Gateway
Non-domain-joined computers and thin clients accessing the Desktop Appliance site	Connected through Desktop Appliance sites
Domain-joined computers and thin clients accessing StoreFront through the XenApp® Services URL	Connected through XenApp Services URLs

The deployment types are defined by the characteristics of the user device to which the smart card reader is connected:

- Whether the device is domain-joined or non-domain-joined.
- How the device is connected to StoreFront.
- What software is used to view virtual desktops and applications.

In addition, smart card-enabled applications such as Microsoft Word, and Microsoft Excel can be used in these deployments. Those applications allow users to digitally sign or encrypt documents.

Bimodal authentication

Where possible in each of these deployments, Receiver supports bimodal authentication by offering the user a choice between using a smart card and entering their user name and password. This is useful if the smart card cannot be used (for example, the user has left it at home or the logon certificate has expired).

Because users of non-domain-joined devices log on to Receiver for Windows directly, you can enable users to fall back to explicit authentication. If you configure bimodal authentication, users are initially prompted to log on using their smart cards and PINs but have the option to select explicit authentication if they experience any issues with their smart cards.

If you deploy Citrix Gateway, users log on to their devices and are prompted by Receiver for Windows to authenticate to Citrix Gateway. This applies to both domain-joined and non-domain-joined devices. Users can log on to Citrix Gateway using either their smart cards and PINs, or with explicit credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This enables you to provide users with bimodal authentication for Citrix Gateway logons. Configure pass-through authentication from Citrix Gateway to StoreFront and delegate credential validation to Citrix Gateway for smart card users so that users are silently authenticated to StoreFront.

Multiple Active Directory forest considerations

In a Citrix environment, smart cards are supported within a single forest. Smart card logons across forests require a direct two-way forest trust to all user accounts. More complex multi-forest deployments involving smart cards (that is, where trusts are only one-way or of different types) are not supported.

You can use smart cards in a Citrix environment that includes remote desktops. This feature can be installed locally (on the user device that the smart card is connected to) or remotely (on the remote desktop that the user device connects to).

Smart card removal policy

The smart card removal policy set on the product determines what happens if you remove the smart card from the reader during a session. The smart card removal policy is configured through and handled by the Windows operating system.

Policy setting	Desktop behavior
No action	No action.
Lock workstation	The desktop session is disconnected and the virtual desktop is locked.
Force logoff	The user is forced to log off. If the network connection is lost and this setting is enabled, the session may be logged off and the user may lose data.
Disconnect if a remote Terminal Services session	The session is disconnected and the virtual desktop is locked.

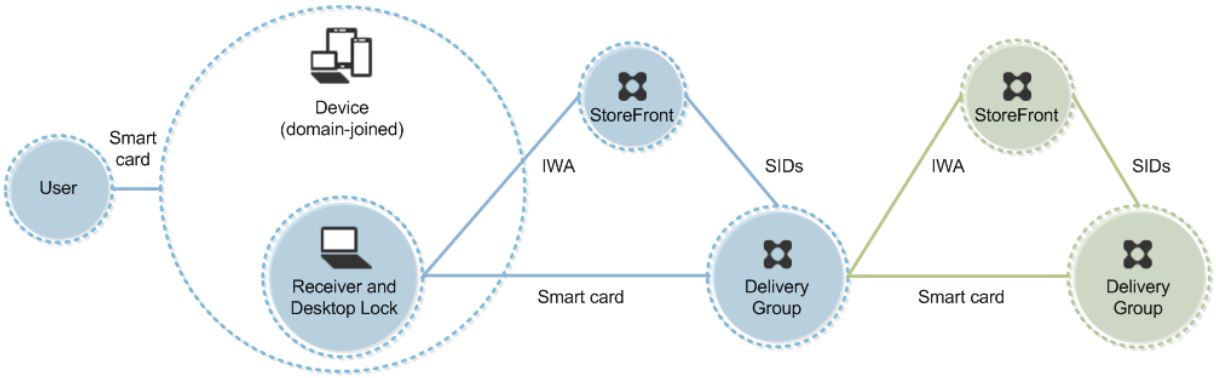
Certificate revocation checking

If certificate revocation checking is enabled and a user inserts a smart card with an invalid certificate into a card reader, the user cannot authenticate or access the desktop or application related to the certificate. For example, if the invalid certificate is used for email decryption, the email remains encrypted. If other certificates on the card, such as ones used for authentication, are still valid, those functions remain active.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deployment example: domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.

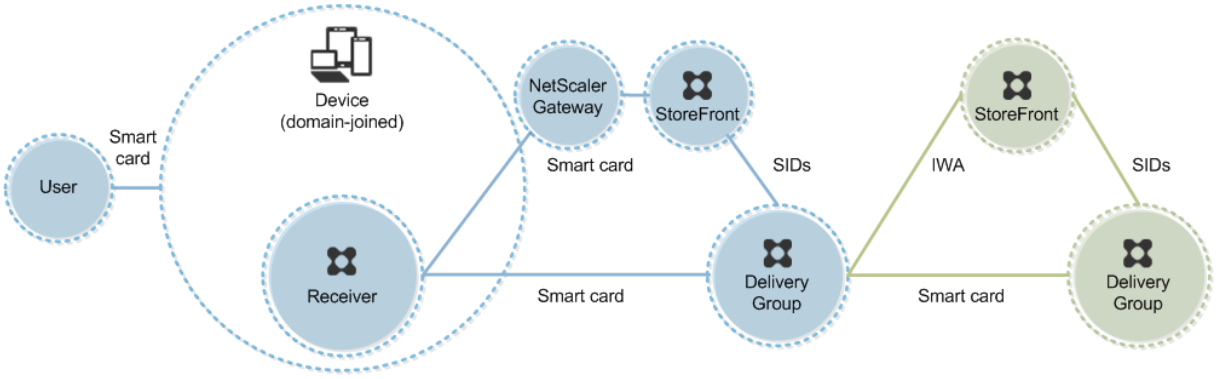


A user logs on to a device using a smart card and PIN. Receiver authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop or application, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: remote access from domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect to StoreFront through Citrix Gateway/Access Gateway.



A user logs on to a device using a smart card and PIN, and then logs on again to Citrix Gateway/Access Gateway. This second logon can be with either the smart card and PIN or a user name and password

© 1997–2026 Citrix Systems, Inc. All rights reserved.

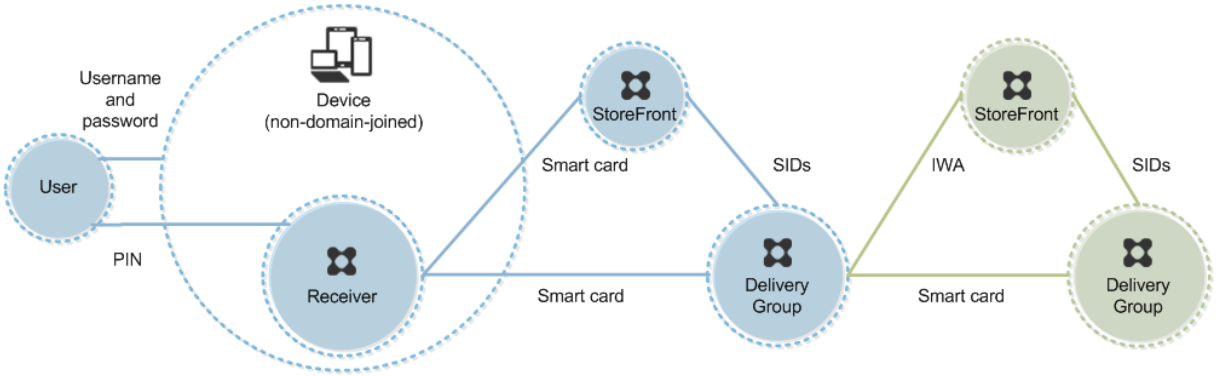
because Receiver allows bimodal authentication in this deployment.

The user is automatically logged on to StoreFront, which passes the user security identifiers (SIDs) to Citrix Virtual Apps™ or Citrix Virtual Desktops. When the user starts a virtual desktop or application, the user is not prompted again for a PIN because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second Store-Front server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: non-domain-joined computers

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user name and password. Receiver then authenticates to Storefront.

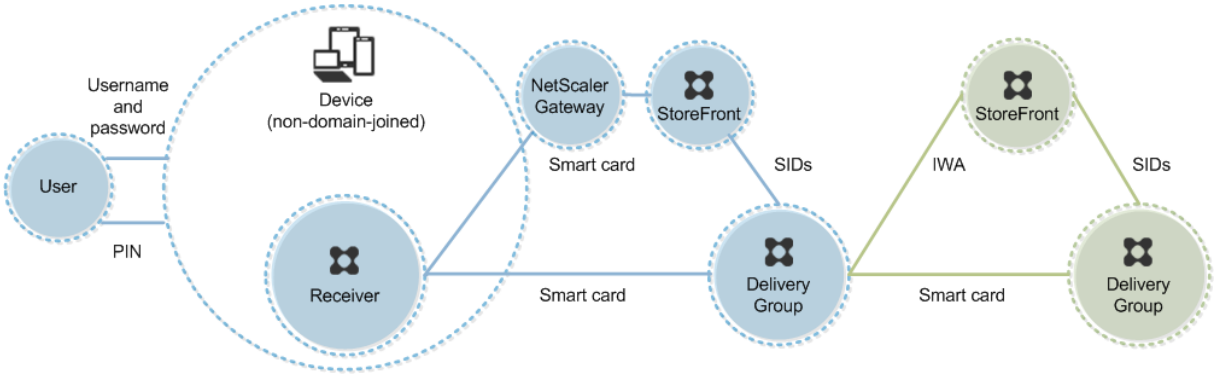
StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second Store-Front server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: remote access from non-domain-joined computers

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user name and password. Receiver then authenticates to Storefront.

StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

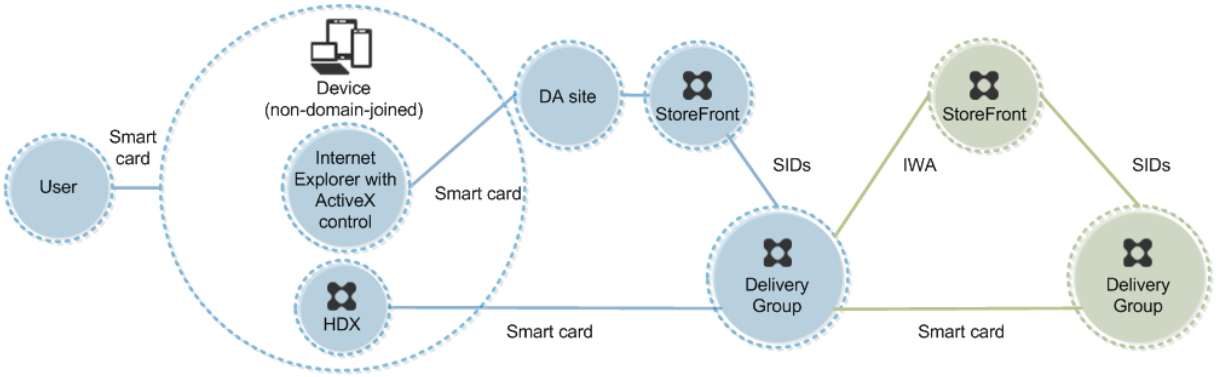
This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: non-domain-joined computers and thin clients accessing the Desktop Appliance site

This deployment involves non-domain-joined user devices that may run the Desktop Lock and connect to StoreFront through Desktop Appliance sites.

The Desktop Lock is a separate component that is released with Citrix Virtual Apps, Citrix Virtual Desktops, and VDI-in-a-Box. It is an alternative to the Desktop Viewer and is designed mainly for repurposed Windows computers and Windows thin clients. The Desktop Lock replaces the Windows shell and Task Manager in these user devices, preventing users from accessing the underlying devices. With the Desktop Lock, users can access Windows Server Machine desktops and Windows Desktop Machine desktops. Installation of Desktop Lock is optional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A user logs on to a device with a smart card. If Desktop Lock is running on the device, the device is configured to launch a Desktop Appliance site through Internet Explorer running in Kiosk Mode. An ActiveX control on the site prompts the user for a PIN, and sends it to StoreFront. StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. The first available desktop in the alphabetical list in an assigned Desktop Group starts.

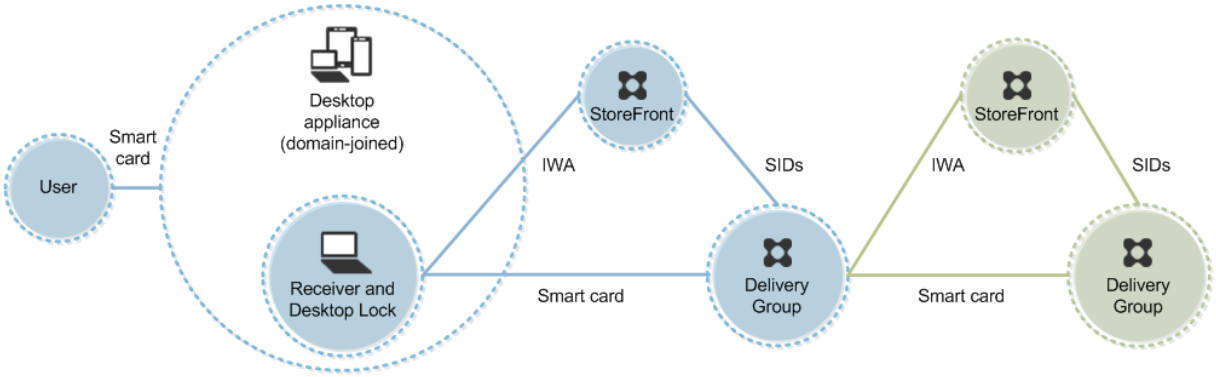
This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Deployment example: domain-joined computers and thin clients accessing StoreFront through the XenApp Services URL

This deployment involves domain-joined user devices that run the Desktop Lock and connect to StoreFront through XenApp Services URLs.

The Desktop Lock is a separate component that is released with Citrix Virtual Apps, Citrix Virtual Desktops, and VDI-in-a-Box. It is an alternative to the Desktop Viewer and is designed mainly for repurposed Windows computers and Windows thin clients. The Desktop Lock replaces the Windows shell and Task Manager in these user devices, preventing users from accessing the underlying devices. With the Desktop Lock, users can access Windows Server Machine desktops and Windows Desktop Machine desktops. Installation of Desktop Lock is optional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A user logs on to a device using a smart card and PIN. If Desktop Lock is running on the device, it authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to Citrix Virtual Apps or Citrix Virtual Desktops. When the user starts a virtual desktop, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

Pass-through authentication and single sign-on with smart cards

September 6, 2025

Pass-through authentication

Pass-through authentication with smart cards to virtual desktops is supported on user devices running Windows 10, Windows 8, and Windows 7 SP1 Enterprise and Professional Editions.

Pass-through authentication with smart cards to hosted applications is supported on servers running Windows Server 2012 and Windows Server 2008 R2 SP1.

To use pass-through authentication with smart cards hosted applications, ensure you enable the use of Kerberos when you configure Pass-through with smartcard as the authentication method for the site.

Note: The availability of pass-through authentication with smart cards depends on many factors including, but not limited to:

- Your organization's security policies regarding pass-through authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

Pass-through authentication with smart cards is configured on Citrix StoreFront. See the StoreFront documentation for details.

Single sign-on

Single sign-on is a Citrix feature that implements pass-through authentication with virtual desktop and application launches. You can use this feature in domain-joined, direct-to-StoreFront and domain-joined, NetScaler-to-StoreFront smart card deployments to reduce the number of times that users enter their PIN. To use single sign-on in these deployment types, edit the following parameters in the default.ica file, which is located on the StoreFront server:

- Domain-joined, direct-to-StoreFront smart card deployments —Set DisableCtrlAltDel to Off
- Domain-joined, NetScaler-to-StoreFront smart card deployments —Set UseLocalUserAndPassword to On

For more instructions on setting these parameters, see the StoreFront or Citrix Gateway documentation.

The availability of single sign-on functionality depends on many factors including, but not limited to:

- Your organization's security policies regarding single sign-on.
- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

> **Note:**
>
> When a user logs on to the Virtual Delivery Agent (VDA) on a machine with an attached smart card reader, a Windows tile may appear representing the previous successful mode of authentication, such as smart card or password. As a result, when single sign-on is enabled, the single sign-on tile may appear. To log on, the user must select **Switch Users** to select another tile because the single sign-on tile will not work.

Enable TLS on Delivery Controllers

December 9, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, both HTTP and HTTPS are enabled. HTTPS uses a self-signed certificate using the sever's FQDN as the common name, which is not trusted by StoreFront™ or web browsers.

To enable TLS on a delivery controller™, you must:

- Obtain, install, and register a server certificate on all Delivery Controllers. For details, see Requesting and installing a certificate.
- Configure a port with the TLS certificate. For details, see Installing a certificate.
- Enable HTTPS for the monitor service.
- Enforce HTTPS traffic by disabling HTTP. For more details, see Enforce HTTPS traffic onlyEnforce HTTPS traffic only.
- Optionally, you can change the ports the Controller uses to listen for HTTP and HTTPS traffic. For more details, see Change HTTP or HTTPS ports.

Requesting and installing a certificate

To use TLS, you must install a certificate whose Common Name or Subject Alternative Name matches the server's FQDN. If you are using a load balancer in front of the delivery controllers then include both the server and the load balancer's FQDNs as Subject Alternative Names. For more information, see Certificates. For StoreFront to connect to the delivery controller you must use a RSA digital signature algorithm. StoreFront does not support certificates using the ECDSA algorithm.

Configuring SSL/TLS listener port

If the IIS Windows component is installed on the same server, which is installed as part of Web Studio and Director, you can configure TLS using IIS. For more information, see Enable TLS on Web Studio and Director. Otherwise, to configure the certificate using PowerShell:

1. To check if there is an existing certificate bound, open an command prompt and run `netsh http show sslcert`:

   ```
   1 netsh http show sslcert
   ```

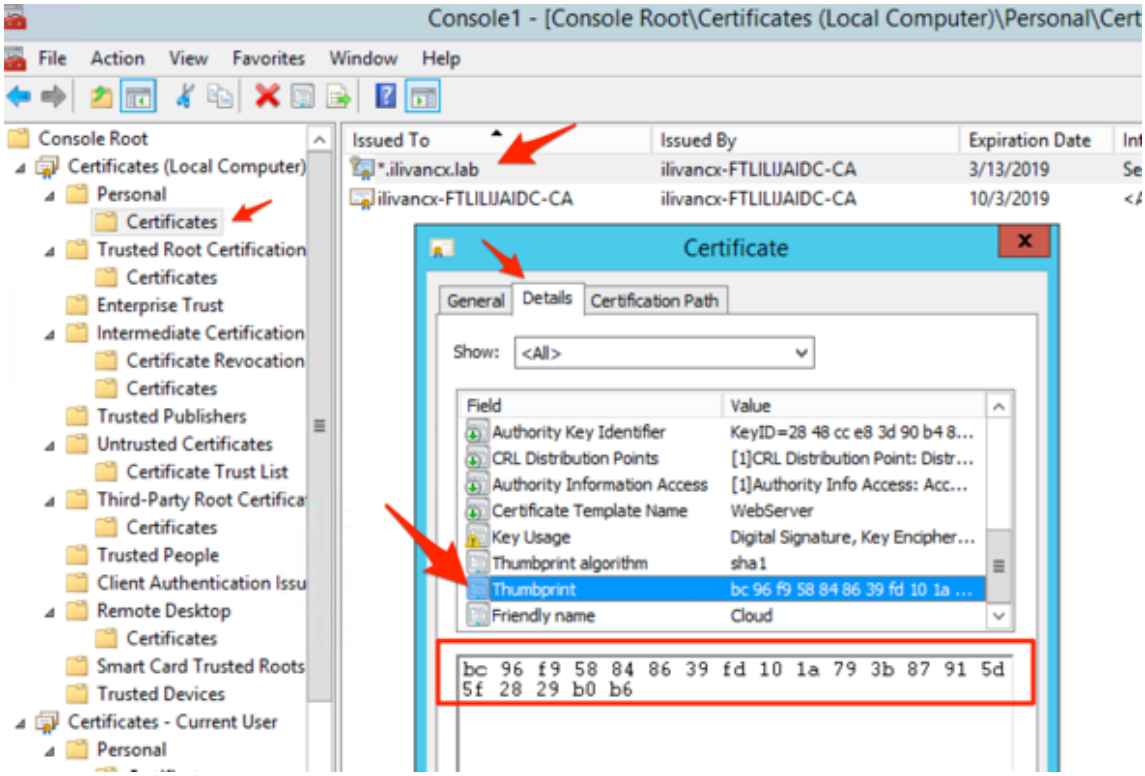
2. If there is an existing binding then delete it.

   ```
   1 netsh http delete sslcert ipport=0.0.0.0:443
   ```

   Replacing `0.0.0.0:443` with a specific IP address and port if there was one specified in the existing binding.

3. Find the thumbprint of the certificate you installed previously. To view the thumbprint, open **Manage computer certificates**, browse to the certificate and open it and go to the **Details** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alternatively you can use PowerShell. For example the following script looks for a certificate whose common name matches the server's host name and prints the thumbnail:

```
$HostName = ([System.Net.Dns]::GetHostByName(($env:computerName)))
    .Hostname
$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
    Object {
 $_.Subject -match ("CN=" + $HostName) }
 ).Thumbprint -join ';'
Write-Host -Object "Certificate Thumbprint for $($HostName): $(
    $Thumbprint)" -Foreground Yellow
```

If the certificate common name does not match the host names then this will fail. If there are multiple certificates for the host name then this returns multiple thumbprints concatenated together and you must choose the appropriate thumbprint.

The following example looks for a certificate by friendly name:

```
$friendlyName = "My certificate name"
$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
    Object {
 $_.FriendlyName -eq $friendlyNam }
 ).Thumbprint -join ';'
Write-Host -Object "Certificate Thumbprint for $friendlyName: $(
    $Thumbprint)" -Foreground Yellow
```

If there are multiple certificates with the specified friendly name then this returns multiple

© 1997–2026 Citrix Systems, Inc. All rights reserved.

thumbprints concatenated together and you must choose the appropriate thumbprint.

4. To bind the certificate to the port, use the `netsh http add sslcert` command:

```
netsh http add sslcert ipport=[IP address]:443 certhash=[
    certificate hash] appid=[application GUID] disablelegacytls=
    enable
```

- `ipport`: The IP address and port. Using 0.0.0.0:443 applies this to all IP addresses. You can instead specify a specific IP address.
- `certhash`: The thumbprint of the certificate you identified in the previous step.
- `appid`: The GUID of the Citrix Broker Service.

> **Note:**
>
> When renewing a certificate or rebinding, use the specific `appid` associated with the Broker Service rather than an arbitrary GUID.

To find the correct `appid` for the Citrix Broker Service:

a) Open a PowerShell command window as an administrator and run the following command:

```
Get-WmiObject -Class Win32_Product | Select-String -
    Pattern "broker"
```

b) Locate the IdentifyingNumber (GUID) for the Citrix Broker Service in the output (for example, `{ D333C884-187F-447C-8C67-463F33989C8F }`). Use this GUID for the `appid` parameter.

- `disablelegacytls=enable`: Disables legacy versions of TLS. This parameter is available on Windows 2022 and higher. Windows 2022 it disables TLS 1.0 and 1.1. On Windows 2025 this is unnecessary as TLS 1.0 and 1.1 are disabled by default.

For example, run the following command to bind the certificate with thumbprint `bc96f958848639fd101` to port 443 on all IP addresses:

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=
    bc96f958848639fd101a793b87915d5f2829b0b6 appid={
 91fe7386-e0c2-471b-a252-1e0a805febac }
  disablelegacytls=enable
```

Once HTTPS is enabled, you should configure any StoreFront deployments and Netscaler Gateways to use HTTPS instead of HTTP to connect to the delivery controller.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Monitor Service OData API for HTTPS

The monitor service provides OData v3 and v4 APIs to allow Citrix® and third party applications to query data. Director connects to the monitoring service using the OData API V3. To configure the monitor OData APIs for HTTPS complete the following steps:

1. Run the following PowerShell:

```
$serviceGroup = Get-ConfigRegisteredServiceInstance -ServiceType
    Monitor | Select -First 1 ServiceGroupUid
Remove-ConfigServiceGroup -ServiceGroupUid $serviceGroup.
    ServiceGroupUid
& 'C:\Program Files\Citrix\Monitor\Service\citrix.monitor.exe' -
    ConfigureFirewall -RequireODataTls –OdataPort 443 -
    RequireODataSdkTls –OdataSdkPort 443
get-MonitorServiceInstance | register-ConfigServiceInstance
Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-
    MonitorServiceGroupMembership
```

2. Open file `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` with a text editor. Find the element `<add key="owin:baseAddress "value="http://localhost/citrix/monitor/odata/v4"/>` and change it to `<add key="owin:baseAddress"value="https://localhost/citrix/monitor/odata/v4"/>`.

Configure cipher suites

The cipher suite order list must include the `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`, or `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` cipher suites (or both); and these cipher suites must precede any `TLS_DHE_` cipher suites.

1. Using the Microsoft Group Policy Editor, browse to **Computer Configuration > Administrative Templates > Network > SSL Configuration Settings**.
2. Edit the policy "SSL Cipher Suite Order". By default, this policy is set to "Not Configured". Set this policy to Enabled.
3. Arrange suites in the correct order; remove any cipher suites suites you do not want to use.

Ensure that either `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`, or `TLS_ECDHE_RSA_WITH_AES_128` precedes any `TLS_DHE_` cipher suites.

On Microsoft Learn, see also Configuring TLS Cipher Suite Order.

Enforce HTTPS traffic only

It is recommended that you configure the XML Service to ignore HTTP traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Run `regedit`
2. Open `HKLM\Software\Citrix\DesktopServer\`
3. Create a new DWORD value with name `XmlServicesEnableNonSsl` and set it to 0.
4. Restart the Broker Service.

There is a corresponding registry DWORD value `XmlServicesEnableSsl` you can create to ignore HTTPS traffic. Ensure that it is not set to 0.

Change HTTP or HTTPS ports

By default, the XML Service on the Controller listens on port 80 for HTTP traffic and port 443 for HTTPS traffic. Although you can use non-default ports, be aware of the security risks of exposing a Controller to untrusted networks. Deploying a standalone StoreFront server is preferable to changing the defaults.

To change the default HTTP or HTTPS ports used by the Controller, run the following command from Studio:

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

where <http-port> is the port number for HTTP traffic and <https-port> is the port number for HTTPS traffic.

> **Note:**
>
> After changing a port, Studio might display a message about license compatibility and upgrading. To resolve the issue, re-register service instances using the following PowerShell cmdlet sequence:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS |
Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
Register-ConfigServiceInstance
```

Enable TLS on Web Studio and Director

September 6, 2025

We recommend always using TLS to secure connections to Web Studio and Director by enabling HTTPS. This article explains how to configure Web Studio and Director to use a trusted certificate and ensure secure access over HTTPS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Default behavior

When you install Web Studio, the installer creates a self-signed certificate and binds it to port 443 on the current server. You can access Web Studio and Director from a web browser over HTTPS on the local server.

However, if you try to access Web Studio or Director from another machine over HTTPS, the browser shows a security error because it doesn't trust the certificate.

> **Note:**
>
> If you install Director without Web Studio, the installer doesn't create a self-signed certificate.

Enable secure access over HTTPS

To allow access to Web Studio or Director over HTTPS from machines other than the Web Studio server, follow these steps:

1. Create or import a trusted certificate.
2. Bind the certificate to port 443 in IIS.
3. (Optional) Enable HTTP Strict Transport Security (HSTS).
4. If Web Studio isn't configured as a proxy (client machines connect to both Web Studio and the Delivery Controllers), enable TLS on Delivery Controllers.

> **Note:**
>
> Using the self-signed certificate isn't recommended because it requires manual configuration on each machine. For more information, see Use the self-signed certificate.

Create or import a trusted certificate

We recommend using a certificate from an enterprise or public certificate authority that is trusted by machines connecting to the server.

For more information, see Create a new certificate and Import existing certificate. The certificate's common name or subject alternative name must match the FQDN that the users use to connect to Web Studio or Director. If a load balancer is deployed in front of the server, use the FQDN of the load balancer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

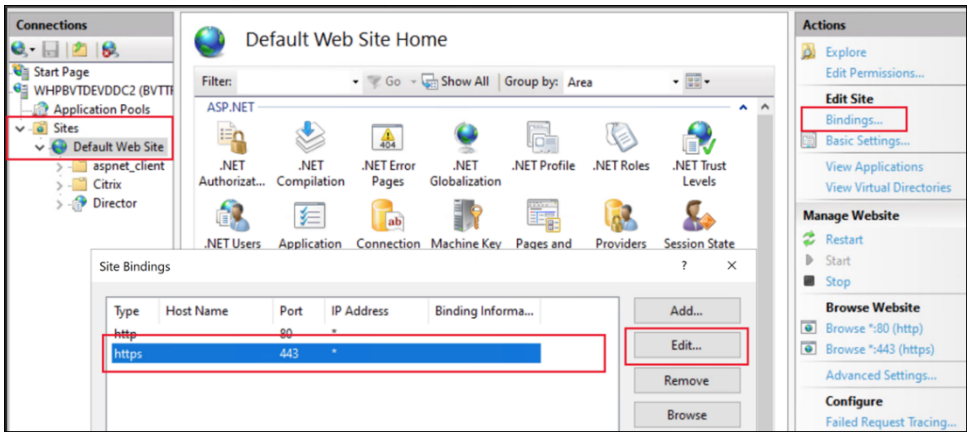
Bind the certificate to port 443

After creating or importing a trusted certificate, bind it to port 443 in IIS. You can do that either before or after installation. If certificate binding is already configured for port 443, the installer makes no changes.

> **Note:**
>
> By default, Web Studio and Director use port 443 for secure HTTPS access. You can change the port number if needed. See Change the default port number for details.

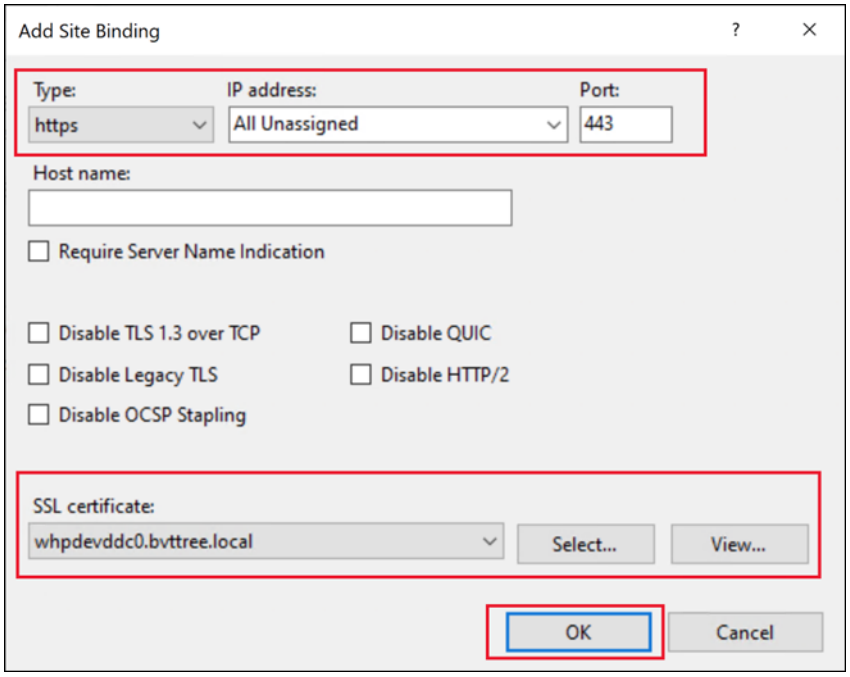
To bind the certificate to port 443, follow these steps:

1. Log on to the server as an administrator.
2. Open the IIS Manager, and browse to **Sites > Default Web Site > Bindings**.
3. If there is an existing binding of type **https** then select it and click **Edit...**. If there is no **https** binding then click **Add**.



4. Create or edit the site binding:
   a) For a new binding, set the type to **https** and the port to 443.
   b) Select the appropriate SSL certificate.
   c) On Windows Server 2022 or higher, optionally select **Disable Legacy TLS** to ensure that users can only connect using modern TLS versions.
   d) Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alternatively, you can change the certificate using PowerShell. For example the following script looks for a certificate with a given common name and binds it to all IP addresses, port 443, and disables legacy TLS versions.

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
    certificate
$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {
 $_.Subject -eq $certSName }

netsh http add sslcert ipport=0.0.0.0:443 certhash=$($certificate.
    Thumbprint) certstorename=My appid="{
 91fe7386-e0c2-471b-a252-1e0a805febac }
 " disablelegacytls=enable
```

Note that `appid` is an arbitrary GUID that can be used to identify which application added the certificate.

Use the self-signed certificate

You can use the existing self-signed certificate, but it's not recommended because it requires manually configuring each machine that accesses the server.

To install the self-signed certificate on machines that need to connect to Web Studio:

1. Export the existing self-signed certificate from the Web Studio and Delivery Controller servers.
2. Import the certificate into the **Trusted Root Certificate** store of machines that must access the server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(Optional) Enable HTTP Strict Transport Security (HSTS)

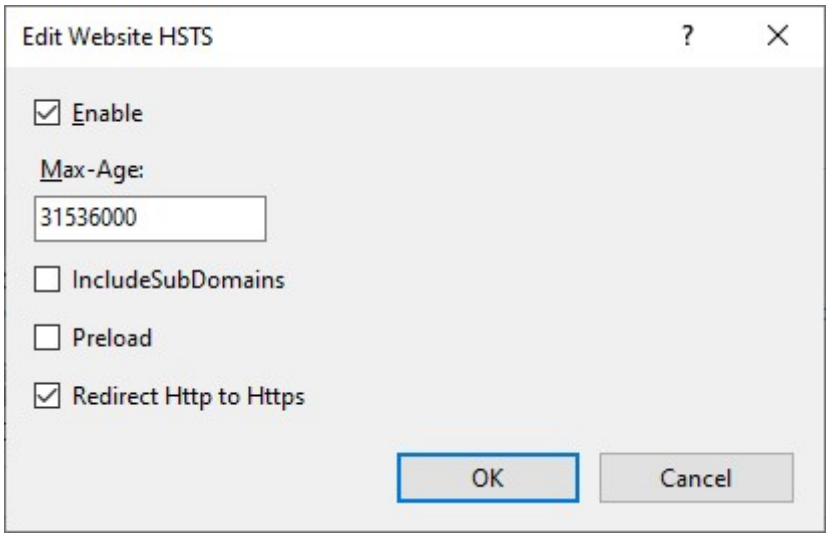
HTTP Strict Transport Security (HSTS) tells web browsers to only use HTTPS when accessing the site. If a user tries to access the URL using HTTP, the browser automatically switches to HTTPS. This setting ensures secure connection validation on both the client and server sides. The browser maintains this validation for the configured period.

On Windows Server 2019 and later, you can configure HSTS in IIS:

1. Open **Internet Information Services (IIS) Manager**.
2. Select **Default Web Site** (or the appropriate website).
3. In the **Actions** pane on the right side, select **HSTS…**.
4. Select **Enable** and enter a max age, for example 31536000 for one year.
5. Select **Redirect Http to Https**.

   > **Note:**
   >
   > Web Studio automatically configures a **URL Rewrite** rule to redirect HTTP to HTTPS when accessing the Studio website. However, this option also applies to Director and any other applications on the IIS site.

6. Click **OK**.



(Optional) Change the default port number

By default, Web Studio and Director use port 443 for secure HTTPS access. To change this port number, follow these steps to create a site binding for the desired port on `Default Web Site`.

Steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. On the server hosting Web Studio, open **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server node and select **Default Web Site** under **Sites**.
3. In the **Actions** pane on the right, click **Bindings**.
4. In the **Site Bindings** window, click **Add**.
5. In the Add Site Binding window, set the following for the new binding:

    a) **Type**: Select **https**.
    b) **IP address**: Select the appropriate IP address, or leave as All Unassigned if applicable.
    c) **Port**: Enter the desired port number (for example, 444).
    d) **SSL certificate**: Select the appropriate SSL certificate for secure communication.

    > **Note:**
    >
    > If the Delivery Controller™ and Web Studio are installed on separate machines, and the server doesn't have other services or websites deployed, you can remove port 443. Otherwise, keep this port to avoid communication issues with the Orchestration service and other FMA services.

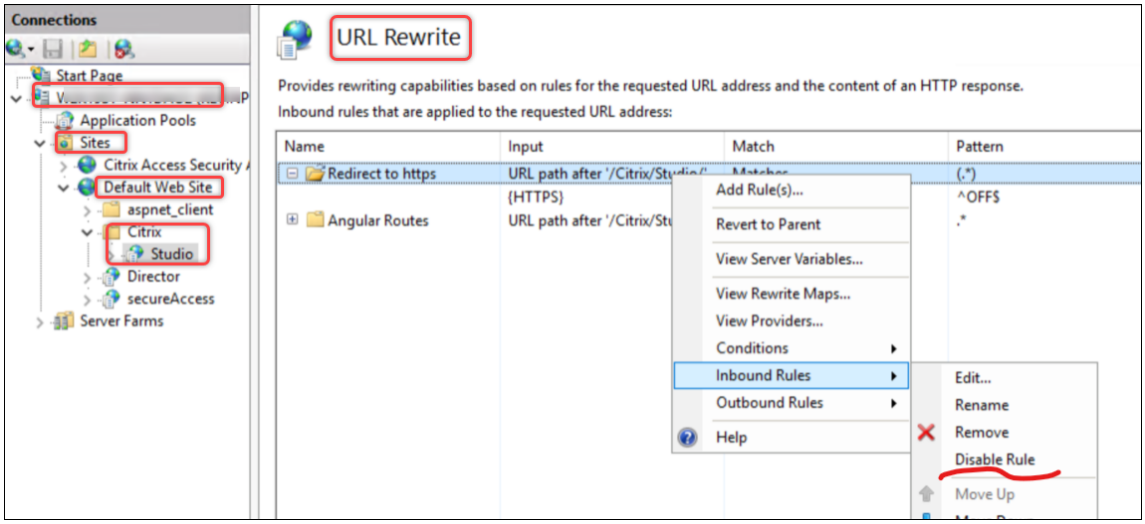
6. Click **OK** to save the binding, and then close the **Site Bindings** window.
7. In **IIS Manager**, click the server node, then in the **Actions** pane, click **Restart** to apply the new binding.

(Optional) Disable HTTPS redirection

When you install Web Studio, by default, any HTTP access is auto-redirected to HTTPS. It is possible to disable this redirection to allow HTTP access. This approach is recommended only if you have taken other measures to block HTTP access. In the case you have a TLS terminating load balance in front of Web Studio, it is still recommended to use HTTPS between your load balancer and Web Studio.

1. Log on to the Web Studio server.
2. Open **Internet Information Services (IIS) Manager**, and go to *Server_name* **> Sites > Default Web Site > URL Rewrite**.
3. Disable **Inbound Rules** for **Redirection to https**, as shown in the following screenshot.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If you have enabled HSTS in IIS then you must also clear **Redirect Http to Https**.

Enable TLS / DTLS on VDAs

September 6, 2025

Enable TLS connections between Citrix Workspace™ app and Virtual Delivery Agents (VDAs) by completing the following tasks:

- Install certificates on the VDAs. For details, see requesting and installing a certificate
- Configure TLS on the machines where the VDAs are installed. (For convenience, further references to machines where VDAs are installed are simply called "VDAs."). It is highly recommended that you use the Citrix supplied PowerShell script to configure TLS/DTLS. For details, see Configure TLS on a VDA using the PowerShell script. However, if you want to configure TLS/DTLS manually, see Manually configure TLS on a VDA.
- Configure TLS in the Delivery Groups containing the VDAs by running a set of PowerShell cmdlets in Studio. For details, see Configure TLS on Delivery Groups.

Requirements and considerations:

- Configure TLS in the Delivery Groups and on the VDAs after you install components, create a Site, create machine catalogs, and create Delivery Groups.
- To configure TLS in the Delivery Groups, you must have permission to change Controller access rules. A Full Administrator has this permission.
- To configure TLS on the VDAs, you must be a Windows administrator on the machine where the VDA is installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On pooled VDAs that are provisioned by Machine Creation Services™ or Provisioning Services, the VDA machine image is reset on restart, causing previous TLS settings to be lost. Run the PowerShell script each time the VDA is restarted to reconfigure the TLS settings.

A Delivery Group cannot have a mixture of some VDAs with TLS configured and some VDAs without TLS configured. Before you configure TLS for a Delivery Group, ensure that you have already configured TLS for all the VDAs in that Delivery Group

When you configure TLS on VDAs, permissions on the installed TLS certificate are changed, giving the ICA® Service read access to the certificate's private key, and informing the ICA Service of the following:

- Which certificate in the certificate store to use for TLS.
- Which TCP port number to use for TLS connections.

  The Windows Firewall (if enabled) must be configured to allow incoming connection on this TCP port. This configuration is done for you when you use the PowerShell script.
- Which versions of the TLS protocol to allow.

  > **Important:**
  >
  > Citrix recommends using TLS 1.2 or higher. SSL and older versions of TLS are deprecated.

  The supported TLS protocol versions follow a hierarchy (lowest to highest): SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. Specify the minimum allowed version; all protocol connections using that version or a higher version are allowed.

  For example, if you specify TLS 1.1 as the minimum version, then TLS 1.1, TLS 1.2 and TLS 1.3 protocol connections are allowed. If you specify SSL 3.0 as the minimum version, then connections for all the supported versions are allowed. If you specify TLS 1.3 as the minimum version, only TLS 1.3 connections are allowed.
- Which TLS cipher suites to allow.

  A cipher suite selects the encryption that is used for a connection. Clients and VDAs can support different sets of cipher suites. When a client (Citrix Workspace app) connects and sends a list of supported TLS cipher suites, the VDA matches one of the client's cipher suites with one of the cipher suites in its own list of configured cipher suites, and accepts the connection. If there is no matching cipher suite, the VDA rejects the connection.

  The VDA supports three sets of cipher suites (also known as compliance modes): GOV(ernment), COM(mercial), and ALL. The acceptable cipher suites also depend on the Windows FIPS mode; see http://support.microsoft.com/kb/811833 for information about Windows FIPS mode. The following table lists the cipher suites in each set:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cipher Suite	ALL	COM	GOV	ALL	COM	GOV
FIPS Mode	Off	Off	Off	On	On	On
TLS_AES_256_GCM_SHA384	X		X	X		X
TLS_AES_128_GCM_SHA256	X			X		X
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X			X	X	

> **Note:**
>
> The VDA does not support DHE ciphersuites (for example, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_DHE_RSA_WITH_AES_128_CBC_SHA.) If selected by Windows, the connection will fail.
>
> If you are using a NetScaler Gateway, refer to the NetScaler documentation for information on cipher suite support for back-end communication. For information on TLS cipher suite support, see Ciphers available on the Citrix ADC appliances. For information on DTLS cipher suite support, see DTLS cipher support.

Requesting and installing a certificate

To use TLS, you must install a certificate whose Alternative Name includes the VDA's FQDN. The certificate must be trusted by any clients connecting directly to the VDA (not via a Citrix Gateway). To allow un-managed devices where you cannot easily deploy certificates to connect to the VDA, consider deploying a NetScaler® Gateway.

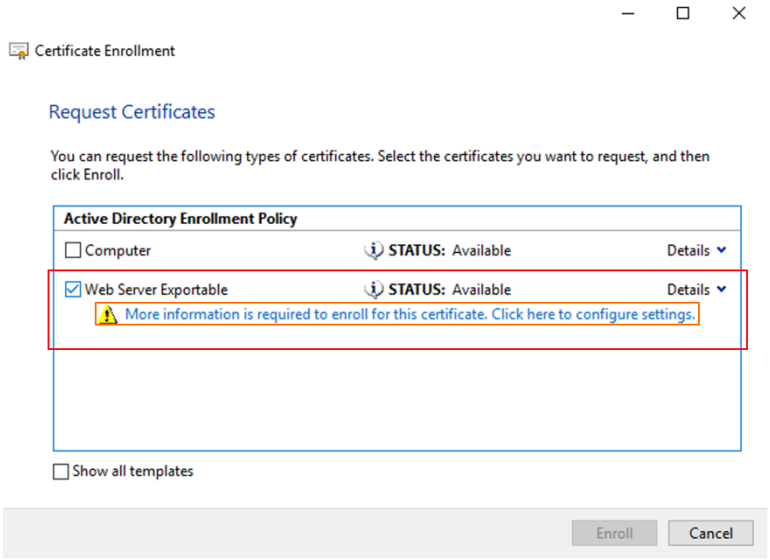
Create certificate using Microsoft Certificate Authority

If your clients and VDAs are on a trusted forest and it has a Microsoft Certificate Authority, you can acquire a certificate from the Certificates MMC snap-in Certificate Enrollment wizard.

1. On the VDA, open the MMC console and add the Certificates snap-in. When prompted select Computer account.
2. Expand **Personal > Certificates**, then use the context menu command **All Tasks > Request New Certificate**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

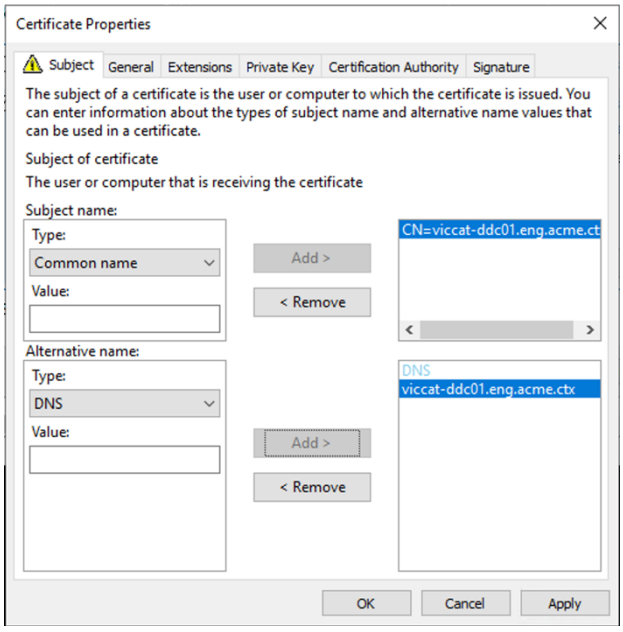
3. Click **Next** to begin, and **Next** to confirm that you are acquiring the certificate from Active Directory enrollment.
4. Select the template for Server Authentication certificate. Both the default Windows **Computer** or **Web Server Exportable** are acceptable. If the template has been set up to automatically provide the values for Subject, you can click **Enroll** without providing more details.



5. To provide more details for the certificate template, click **Details** and configure the following:

   Subject name —select type **Common name** and add the FQDN of the VDA

   Alternative name —select type **DNS** and add the FQDN of the VDA



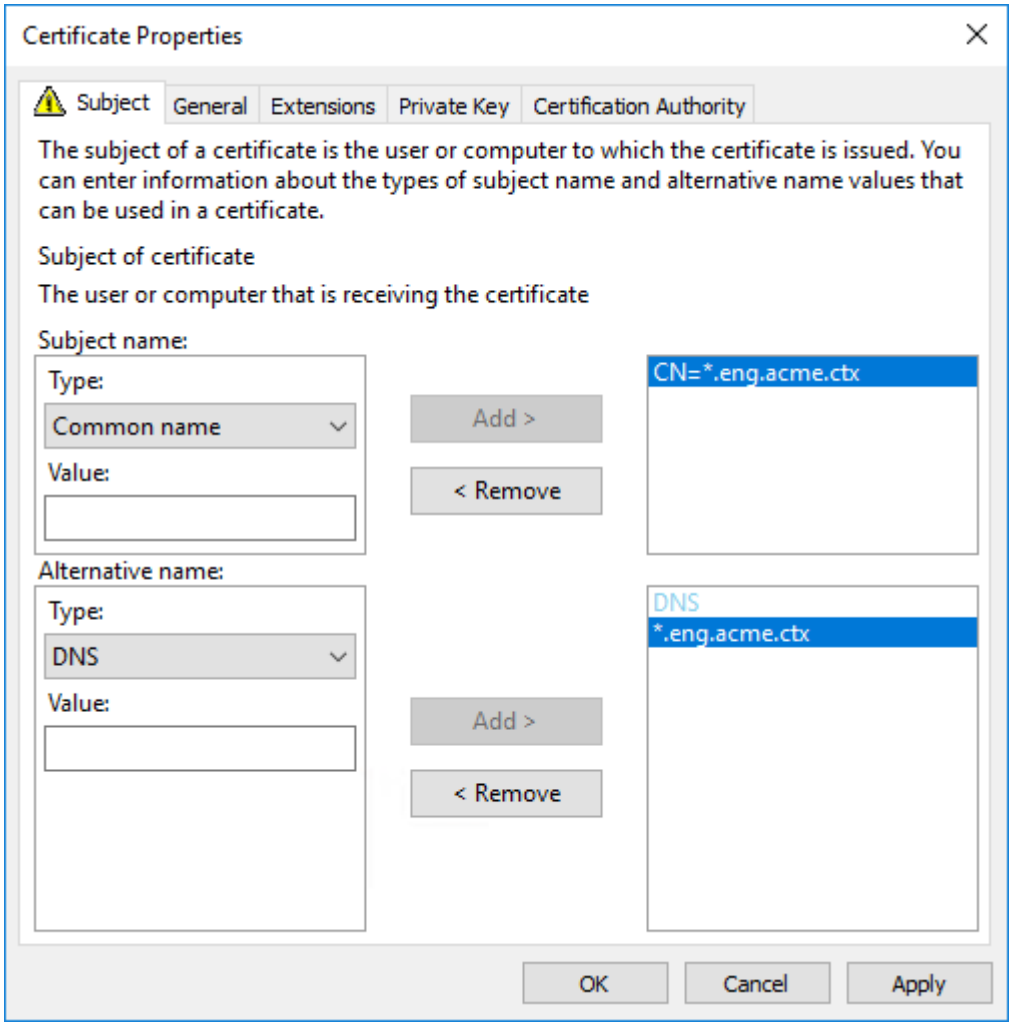
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Use Active Directory Certificate Services Certificate Auto-Enrollment to automate issuing and deploying certificates to the VDAs. This is described in Enable certificate auto-enrollment).

You can use wildcard certificates to allow a single certificate to secure multiple VDAs:

Subject name —select type **Common name** and enter the *.primary.domain of the VDAs

Alternative name —select type **DNS** and add the *.primary.domain of the VDAs

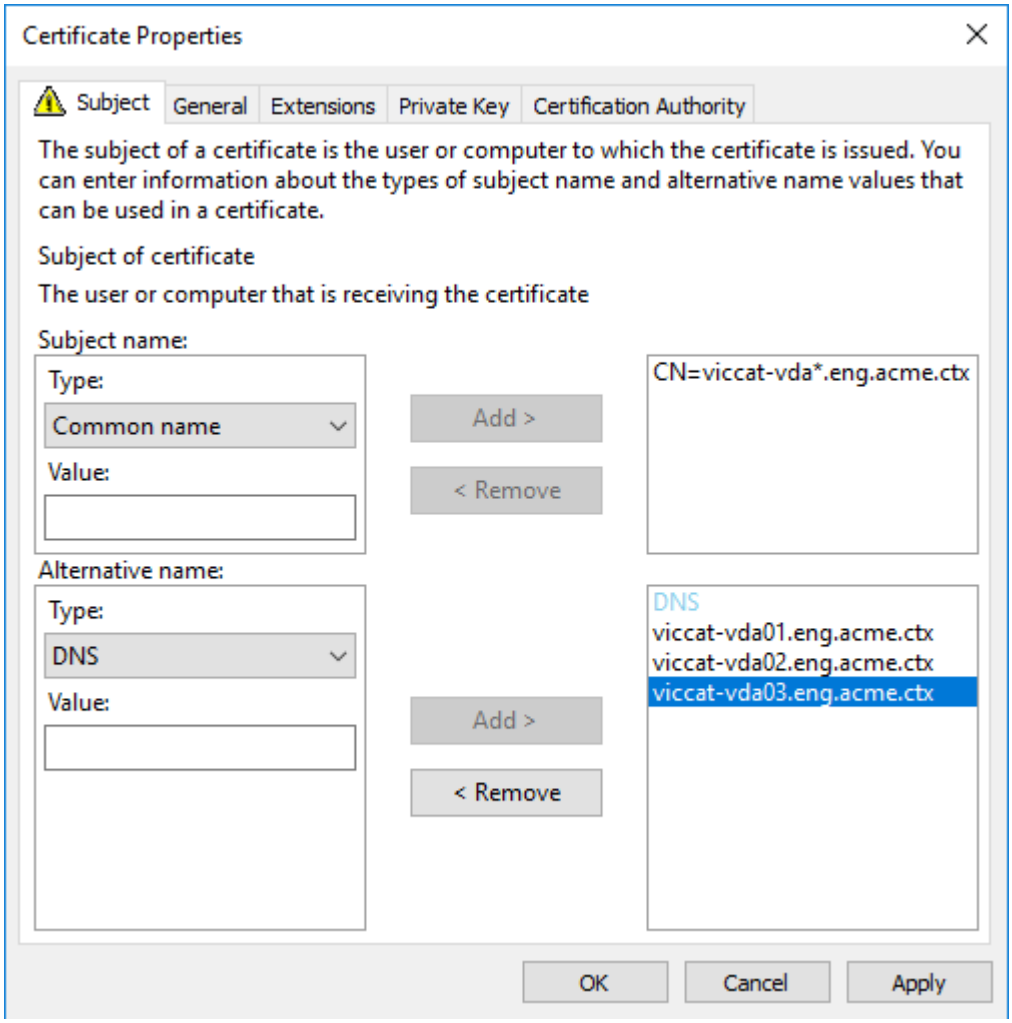


You can use SAN certificates to allow a single certificate to secure multiple specific VDAs:

Subject name —select type **Common name** and enter a string to help identify the certificate usage

Alternative name —select type **DNS** and add an entry for the FQDN of each VDA. Keep the number of Alternative names to a minimum to ensure optimal TLS negotiation.

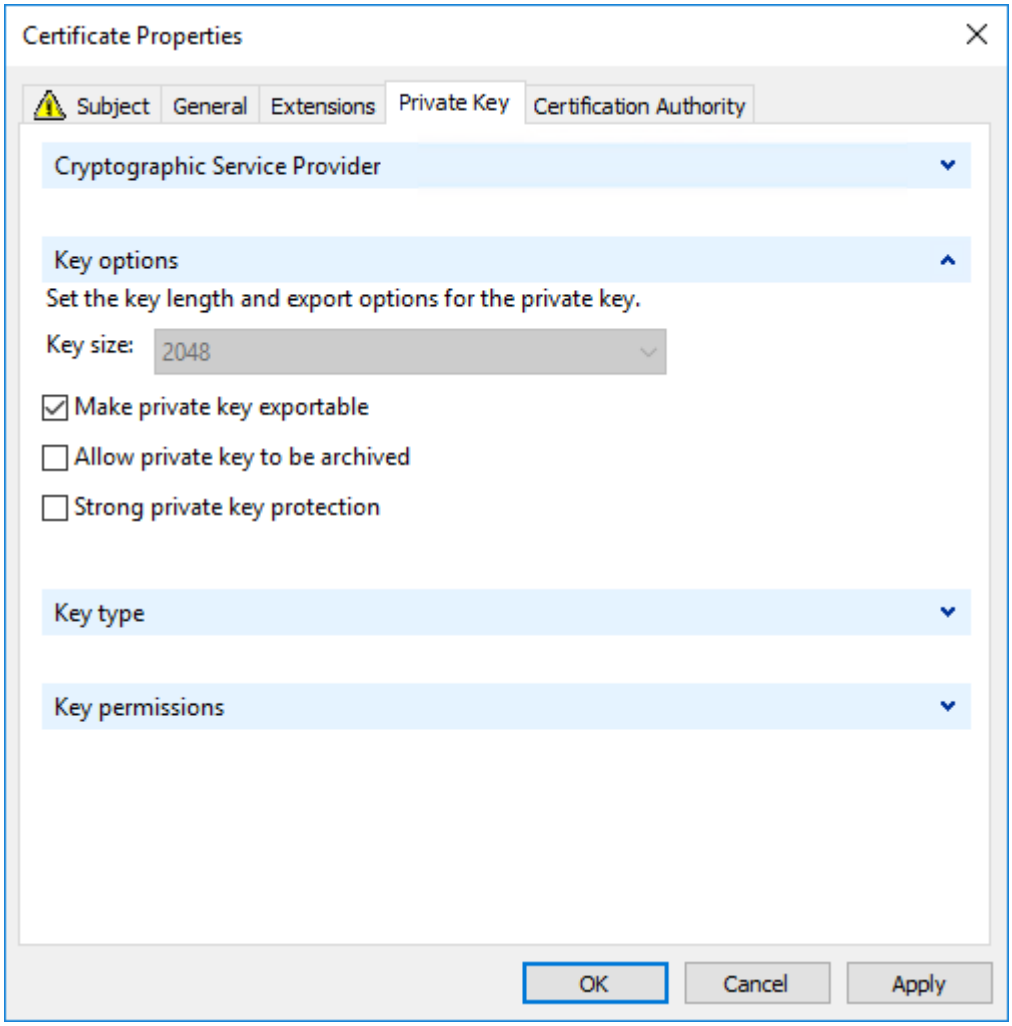
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Note:

Both wildcard and SAN certificates require **Make private key exportable** on the Private Key tab to be selected:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure TLS on a VDA using the PowerShell script

Install the TLS Certificate in the Local Computer > Personal > Certificates area of the certificate store. If more than one certificate resides in that location, supply the thumbprint of the certificate to the PowerShell script.

> **Note:**
>
> Starting with XenApp and XenDesktop 7.15 LTSR, the PowerShell script finds the correct certificate based on the FQDN of the VDA. You do not need to supply the thumbprint when only a single certificate is present for the VDA FQDN.

The Enable-VdaSSL.ps1 script enables or disables the TLS listener on a VDA. This script is available in the *Support* > *Tools* > *SslSupport* folder on the installation media.

When you enable TLS, DHE cipher suites are disabled. ECDHE cipher suites are not affected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you enable TLS, the script disables all existing Windows Firewall rules for the specified TCP port. It then adds a new rule that allows the ICA Service to accept incoming connections only on the TLS TCP and UDP ports. It also disables the Windows Firewall rules for:

- Citrix ICA (default: 1494)
- Citrix CGP (default: 2598)
- Citrix WebSocket (default: 8008)

The effect is that users can only connect using TLS or DTLS. They cannot use ICA/HDX, ICA/HDX with Session Reliability, or HDX over WebSocket, without TLS or DTLS.

> **Note:**
>
> DTLS is not supported with ICA/HDX Audio over UDP Real-time Transport, or with ICA/HDX Framehawk.

See Network ports.

The script contains the following syntax descriptions, plus extra examples; you can use a tool such as Notepad++ to review this information.

> **Important:**
>
> Specify either the Enable or Disable parameter, and the CertificateThumbPrint parameter. The other parameters are optional.

Syntax

```
Enable-VdaSSL { -Enable | -Disable } -CertificateThumbPrint "<thumbprint
>"[-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite
"\<suite>"]
```

Parameter	Description
Enable	Installs and enables the TLS listener on the VDA. Either this parameter or the Disable parameter is required.
Disable	Disables the TLS listener on the VDA. Either this parameter or the Enable parameter is required. If you specify this parameter, no other parameters are valid.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter	Description
CertificateThumbPrint “”	Thumbprint of the TLS certificate in the certificate store, enclosed in quotation marks. The script uses the specified thumbprint to select the certificate you want to use. If this parameter is omitted, an incorrect certificate is selected.
SSLPort	TLS port. Default: 443
SSLMinVersion “”	Minimum TLS protocol version, enclosed in quotation marks. Valid values: `SSL_3.0`, `TLS_1.0` (default), `TLS_1.1`, `TLS_1.2` and `TLS_1.3`. `TLS_1.3` requires Windows 11 or Windows Server 2022 or higher.
SSLCipherSuite “”	TLS cipher suite, enclosed in quotation marks. Valid values: “GOV”, “COM”, and “ALL”(default).

Examples

The following script installs and enables the TLS protocol version value. The thumbprint (represented as “12345678987654321”in this example) is used to select the certificate to use.

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

The following script installs and enables the TLS listener, and specifies TLS port 400, the GOV cipher suite, and a minimum TLS 1.2 protocol value. The thumbprint (represented as “12345678987654321” in this example) is used to select the certificate to use.

```
Enable-VdaSSL -Enable
-CertificateThumbPrint "12345678987654321"
-SSLPort 400 -SSLMinVersion "TLS_1.2"
-SSLCipherSuite "All"
```

The following script disables the TLS listener on the VDA.

```
Enable-VdaSSL -Disable
```

Manually configure TLS on a VDA

When configuring TLS on a VDA manually, you grant generic read access to the private key of the TLS certificate for the appropriate service on each VDA: NT SERVICE\PorticaService for a VDA for Windows

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Single-session OS, or NT SERVICE\TermService for a VDA for Windows Multi-session OS. On the machine where the VDA is installed:

STEP 1. Launch the Microsoft management console (MMC): Start > Run > mmc.exe.

STEP 2. Add the Certificates snap-in to the MMC:

1. Select File > Add/Remove Snap-in.
2. Select Certificates and then click Add.
3. When prompted with "This snap-in will always manage certificates for:"choose "Computer account"and then click Next.
4. When prompted with "Select the computer you want this snap-in to manage"choose "Local computer"and then click Finish.

STEP 3. Under Certificates (Local Computer) > Personal > Certificates, right–click the certificate and then select All Tasks > Manage Private Keys.

STEP 4. The Access Control List Editor displays "Permissions for (FriendlyName) private keys"where (FriendlyName) is the name of your TLS certificate. Add one of the following services and give it Read access:

- For a VDA for Windows Single-session OS, "PORTICASERVICE"
- For a VDA for Windows Multi-session OS, "TERMSERVICE"

STEP 5. Double-click the installed TLS certificate. In the certificate dialog, select the Details tab and then scroll to the bottom. Click Thumbprint.

STEP 6. Run regedit and go to HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Edit the SSL Thumbprint key and copy the value of the TLS certificate's thumbprint into this binary value. You can safely ignore unknown items in the Edit Binary Value dialog box (such as '0000'and special characters).
2. Edit the SSLEnabled key and change the DWORD value to 1. (To disable SSL later, change the DWORD value to 0.)
3. If you want to change the default settings (optional), use the following in the same registry path:

   SSLPort DWORD –SSL port number. Default: 443.

   SSLMinVersion DWORD –1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2, 5 = TLS 1.3. Default: 2 (TLS 1.0).

   SSLCipherSuite DWORD –1 = GOV, 2 = COM, 3 = ALL. Default: 3 (ALL).

STEP 7. Ensure that the TLS TCP and UDP ports are that open in the Windows Firewall if they are not the default 443. (When you create the inbound rule in Windows Firewall, ensure its properties have the "Allow the connection"and "Enabled"entries selected.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STEP 8. Ensure that no other applications or services (such as IIS) are using the TLS TCP port.

STEP 9. For multi-session VDAs, restart the machine for the changes to take effect. (You do not need to restart single-session VDA machines.)

STEP 10. Modify the Windows cipher suite preference so that the VDA-supported cipher suites have the highest priority in order to avoid connection issues.

> **Important:**
>
> The Group Policy changes outlined below only take effect after the system is restarted.
>
> If you are using non-persistent session hosts provisioned with MCS or PVS, you must apply these settings in the master image.

Option 1:

Using the Group Policy Editor, go to Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order. Ensure the following cipher suites are at the top of the list:

```
TLS_AES_256_GCM_SHA384_P384
TLS_AES_256_GCM_SHA384_P256
TLS_AES_128_GCM_SHA256_P384
TLS_AES_128_GCM_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> **Note:**
>
> TLS_AES_256_GCM_SHA384 and TLS_AES_128_GCM_SHA256 only apply to Windows 11 and Windows Server 2022 or newer. If you are using older operating systems, please do not include these cipher suites in your list.
>
> Note that the listed cipher suites also specify the elliptic curve, P384 or P256, to ensure that "curve25519"is not selected. FIPS Mode does not prevent the use of "curve25519".
>
> It is not necessary to remove any cipher suites from the list. Note that these settings apply to the entire system, so if you decide to remove any cipher suites, you must ensure they are not required by any applications or services running on your session hosts.

Option 2:

Using the Group Policy Editor, go to Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order. Ensure the following cipher suites are at the top of the list:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

> **Note:**
>
> TLS_AES_256_GCM_SHA384 and TLS_AES_128_GCM_SHA256 only apply to Windows 11 and Windows Server 2022, or newer. If you are using older operating systems, please do not include these cipher suites in your list.
>
> It is not necessary to remove any cipher suites from the list. Note that these settings apply to the entire system, so if you decide to remove any cipher suites, you must ensure they are not required by any applications or services running on your session hosts.

Using the Group Policy Editor, go to Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings > ECC Curve Order. Enable the setting and include the following curves in the list:

```
NistP384
NistP256
```

> **Note:**
>
> This ensure that "curve25519"is not selected. FIPS Mode does not prevent the use of "curve25519".

The VDA selects a cipher suite only if appears in both lists: the Group Policy list and the list for the selected compliance mode (COM, GOV, or ALL). The cipher suite must also appear in the list sent by the client (Citrix Workspace app).

Configure TLS on Delivery Groups

Complete this procedure for each Delivery Group that contains VDAs you have configured for TLS connections.

1. From Studio, open the PowerShell console.
2. Run **Get-BrokerAccessPolicyRule -DesktopGroupName '*<delivery-group-name>*'| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
3. Run **Set-BrokerSite -DnsResolutionEnabled $true**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enabling SSL for Pooled VDAs using Auto-Enrolment

When using pooled VDAs, if you add a certificate to the master image then all VDAs share the same image. You can use a wildcard certificate but a disadvantage is that if any one of the VDAs becomes compromised, this all powerful certificate would mean HDX™ connections belonging to all VDAs would be at risk.

Instead a secure alternative is to leverage Microsoft Active Directory Certificate Services to provisioning certificates automatically using group policy. You can use a startup script on the VDA to dynamically provision a fresh certificate and enables SSL to the VDA.

Note that this approach will only work for single-session Desktop VDAs. For multi-session VDAs, the ICA listener is brought up too early during the boot process, before certificates can be automatically provisioned.

Since Active Directory Certificate Services uses an internal Enterprise Certificate Authority, it won't be automatically trusted by all Windows installations. If the clients are managed by the corporation and part of a domain forest, the trusted CA certificates can be distributed automatically using group policy. For BYOD and other non-domain joined devices you need to distribute the trusted CA certificates to your users by some other mechanism (such as offering a download link), or use a NetScaler gateway.

Enable Certificate Auto-Enrollment

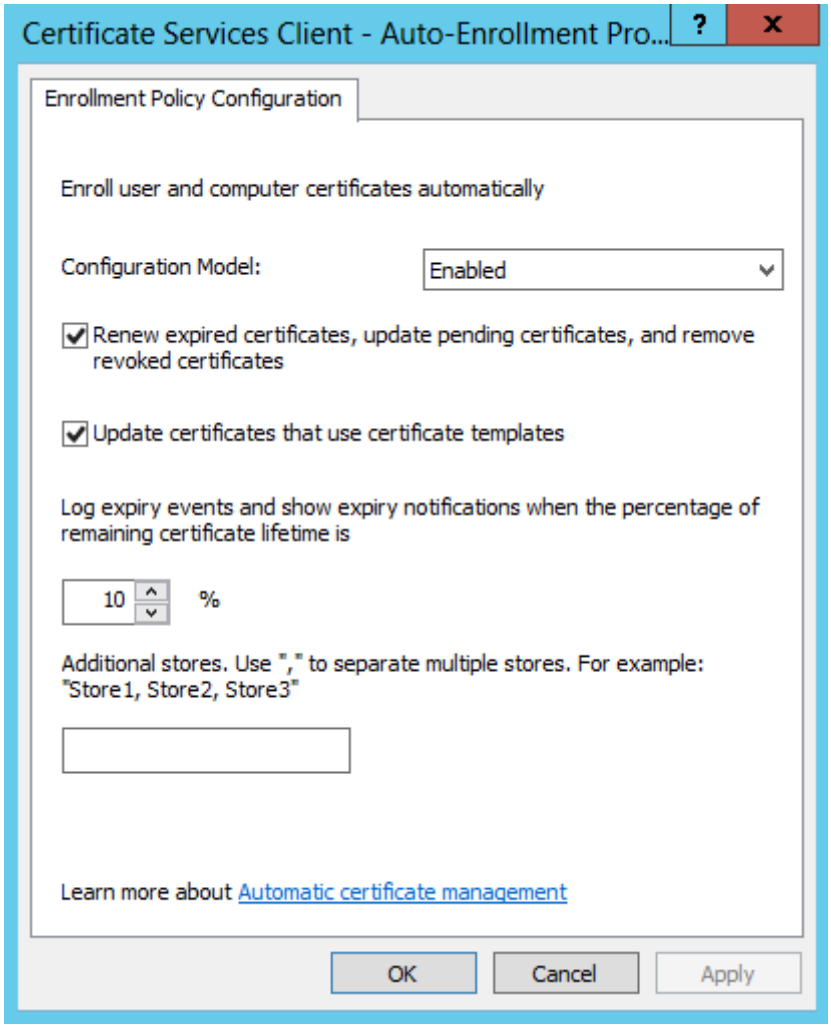
First ensure you have Active Directory Certificate Services role installed on a server in your VDA domain forest providing an Enterprise CA, otherwise auto-enrollment will not be possible.

Note that this may put considerable higher load than usual on your Enterprise CA, since VDAs will be submitting a certificate request on every boot. Make sure to allocate sufficient CPU and memory on the CA server to cope with the load, and as ever test the scalability of the deployment in a lab environment before moving into production.

In the Group Policy Management Editor, create a new policy which applies to the Organizational Unit that will contain your pooled VDAs with SSL enabled as follows:

1. Expand Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Public Key Policies
2. Edit the 'Certificate Services Client –Auto Enrollment Policy' object properties
3. Configure as shown in the screenshot below.
4. Right-click the Automatic Certificate Request container and select New -> Automatic Certificate Request…
5. In the Automatic Certificate Request Setup Wizard, click Next
6. Ensure the Computer certificate template is selected, click Next
7. Click Finish

© 1997–2026 Citrix Systems, Inc. All rights reserved.

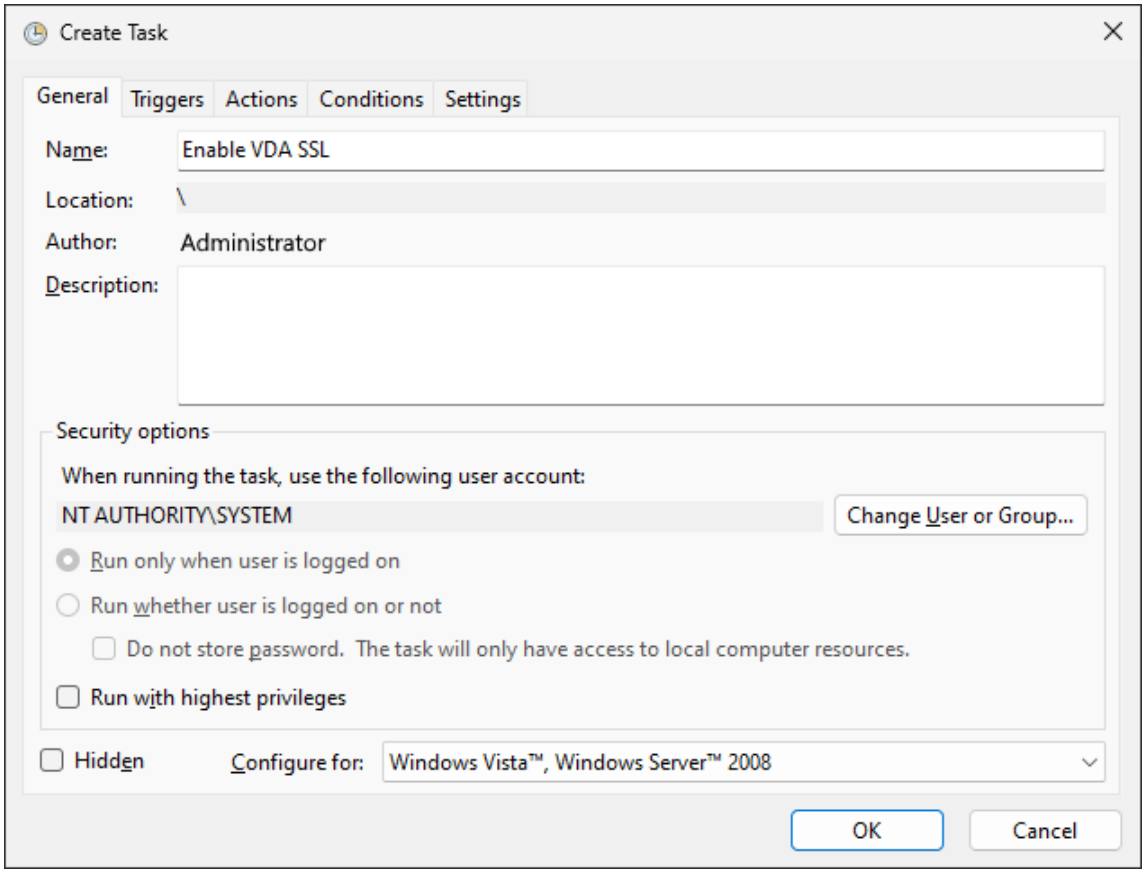


Preparing the Windows Master Image

Copy the Enable-VdaSsl.ps1 script from the product installation media in the `Support\Tools\SslSupport` folder to the VDA master image. Note the master image should not contain any certificates to be used for HDX SSL connections. The certificates will be provisioned when the MCS or PVS machine catalog is created. Now create a new scheduled task as follows (do not run the scheduled task now):

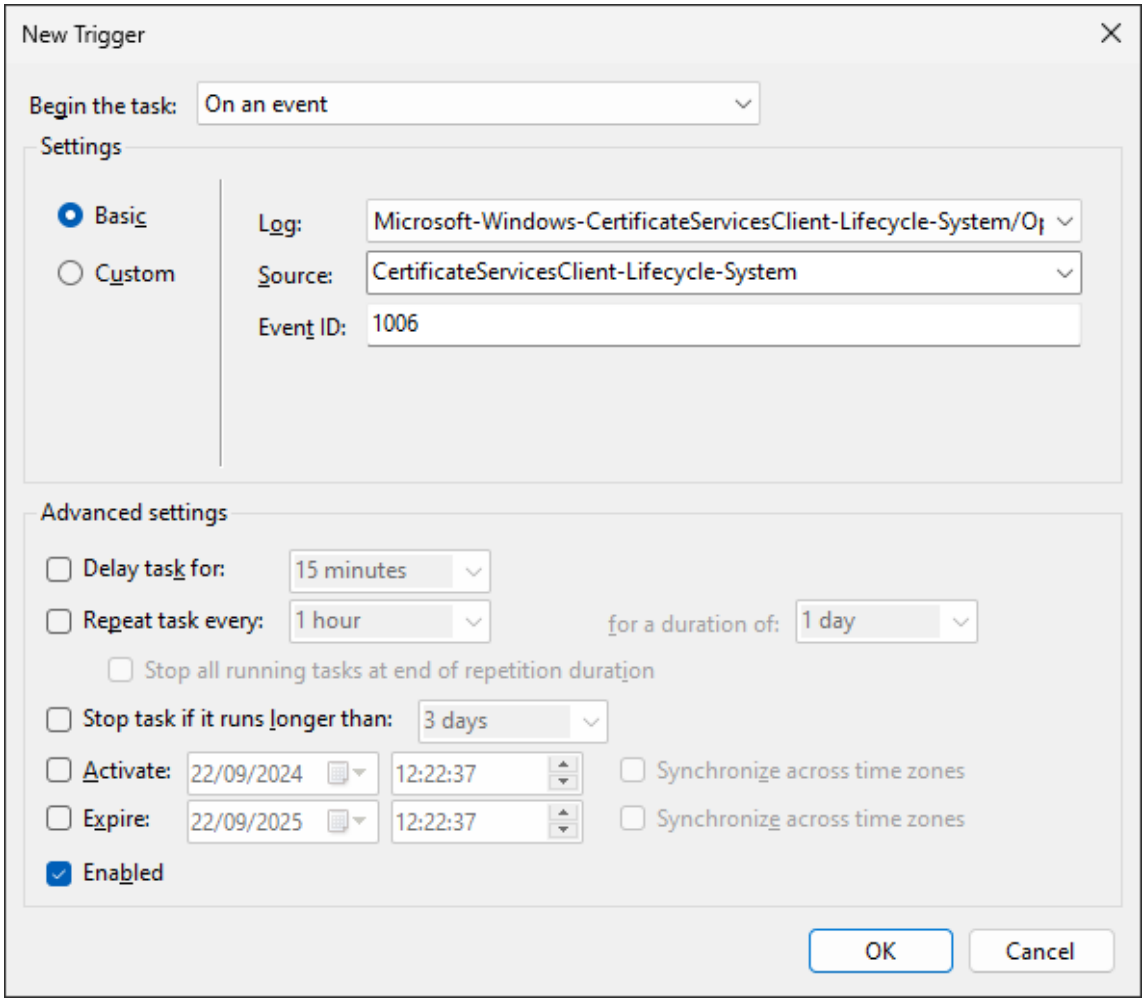
1. Open Task Scheduler.
2. In the **Actions** pane, press **Create Task...**
3. On the general tab:
    - Enter a **Name** such as `Enable VDA SSL`
    - Click **Change User or Group...** and in the Select User or Group dialog box enter `SYSTEM` and click **OK**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



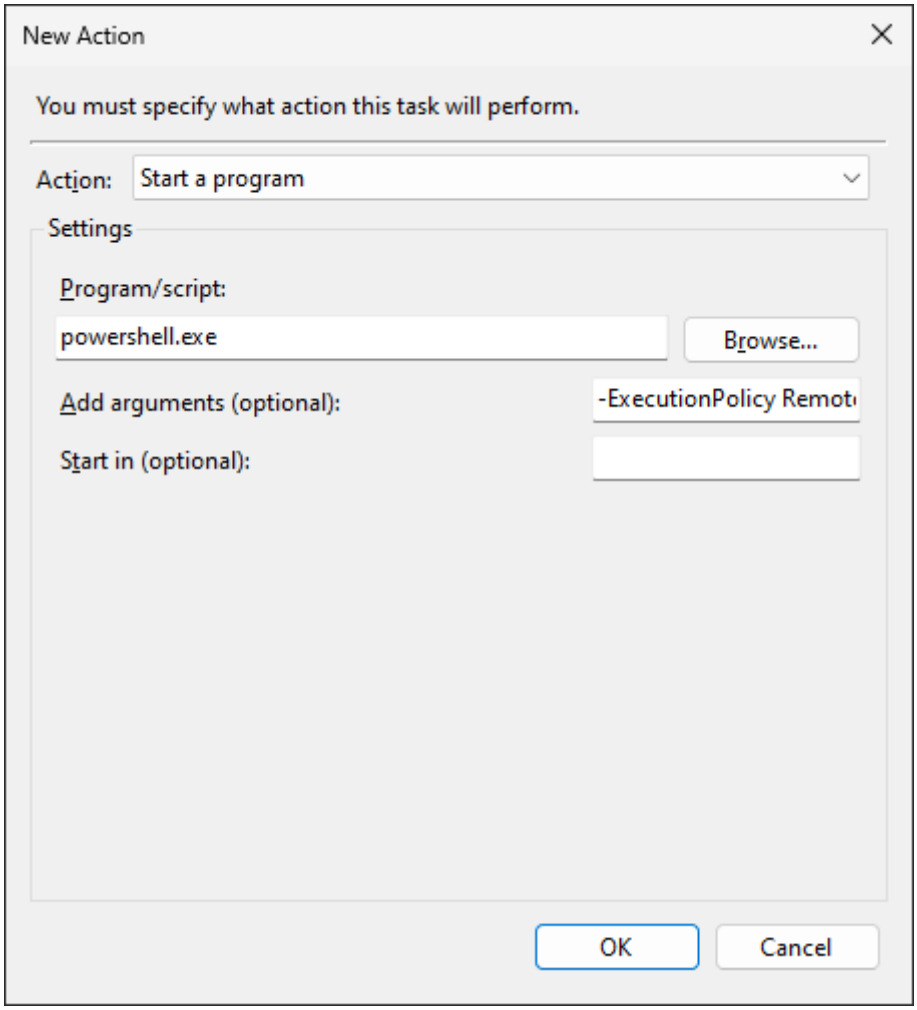
4. Select the Triggers tab
5. Click **New...**. In the **New Trigger** dialog:
    a) Set **Begin the task** to **On an event**
    b) Set **Log** to **Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational**
    c) Set **Source** to **Microsoft-Windows-CertificateServicesClient-Lifecycle-System**
    d) Set **Event ID** to `1006`
    e) Click **OK** to save the trigger

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Select the **Actions** tab
7. Click **New...**
8. In the **New Action** dialog:
    a) Set **Action** to **Start a program**
    b) In the Program/script field, enter `powershell.exe`
    c) In the Add arguments field, enter `-ExecutionPolicy RemoteSigned Enable-VdaSsl.ps1 -Enable -Confirm:$False`, including the path to the powershell script.
    d) Press **OK** to save the action

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. Press **OK** to save the task

Troubleshooting

If a connection error occurs, check the system event log on the VDA.

When using Citrix Workspace app for Windows, if you receive a connection error that indicates a TLS error, disable Desktop Viewer and then try connecting again. Although the connection still fails an explanation of the underlying TLS issue might be provided. For example, you specified an incorrect template when requesting a certificate from the certificate authority.)

Most configurations that use HDX Adaptive Transport work successfully with DTLS, including those using the latest versions of Citrix Workspace app, Citrix Gateway, and the VDA. Some configurations which use DTLS between Citrix Workspace app and Citrix Gateway, and which use DTLS between Citrix Gateway and the VDA, require additional action.

Additional action is needed if:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- the Citrix Receiver version supports HDX Adaptive Transport and DTLS: Receiver for Windows (4.7, 4.8, 4.9), Receiver for Mac (12.5, 12.6, 12.7), Receiver for iOS (7.2, 7.3.x) or Receiver for Linux (13.7)

and either of the following also applies:

- the Citrix Gateway version supports DTLS to the VDA, but the VDA version does not support DTLS (version 7.15 or earlier),
- the VDA version supports DTLS (version 7.16 or later), but the Citrix Gateway version does not support DTLS to the VDA.

To avoid connections from Citrix Receiver™ failing, do one of the following:

- update Citrix Receiver, to Receiver for Windows version 4.10 or later, Receiver for Mac 12.8 or later, or Receiver for iOS version 7.5 or later; or,
- update the Citrix Gateway to a version that supports DTLS to the VDA; or,
- update the VDA, to version 7.16 or later; or,
- disable DTLS at the VDA; or,
- disable HDX Adaptive Transport.

> **Note:**
>
> A suitable update for Receiver for Linux is not yet available. Receiver for Android (version 3.12.3) does not support HDX Adaptive Transport and DTLS via Citrix Gateway, and is therefore not affected.
>
> To disable DTLS at the VDA, modify the VDA firewall configuration to disable UDP port 443. See Network ports.

TLS and HTML5 video redirection, and browser content redirection

You can use HTML5 video redirection and browser content redirection to redirect HTTPS websites. The JavaScript injected into those websites must establish a TLS connection to the Citrix HDX HTML5 Video Redirection Service running on the VDA. To achieve this, the HTML5 Video Redirection Service generates two custom certificates in the certificate store on the VDA. Stopping the service removes the certificates.

The HTML5 video redirection policy is disabled by default.

The browser content redirection is enabled by default.

For more information on HTML5 video redirection, see Multimedia policy settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable TLS on Universal Print Server

September 6, 2025

The Transport Layer Security (TLS) protocol is supported for TCP-based connections between the Virtual Delivery Agent (VDA) and the Universal Print Server.

> **Warning:**
>
> For tasks that include working in the Windows registry—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.

Types of printing connections between the VDA and Universal Print Server

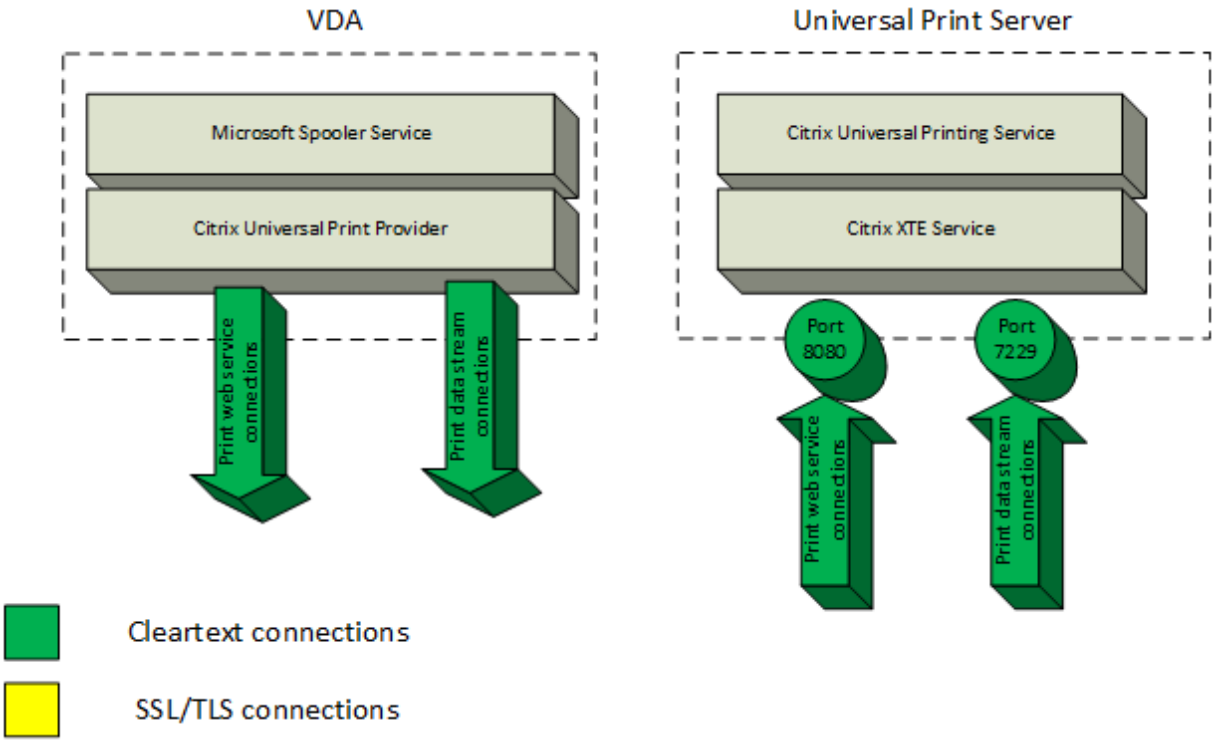
Cleartext connections

The following connections related to printing originate from the VDA and connect to ports on the Universal Print Server. These connections are made only when the **SSL enabled** policy setting is set to **Disabled** (the default).

- Cleartext print web service connections (TCP port 8080)
- Cleartext print data stream (CGP) connections (TCP port 7229)

The Microsoft support article Service overview and network port requirements for Windows describes the ports used by the Microsoft Windows Print Spooler Service. The SSL/TLS settings in this document do not apply to the NetBIOS and RPC connections made by the Windows Print Spooler service. The VDA uses the Windows Network Print Provider (win32spl.dll) as a fallback if the **Universal Print Server enable** policy setting is set to **Enabled with fallback to Windows'native remote printing**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

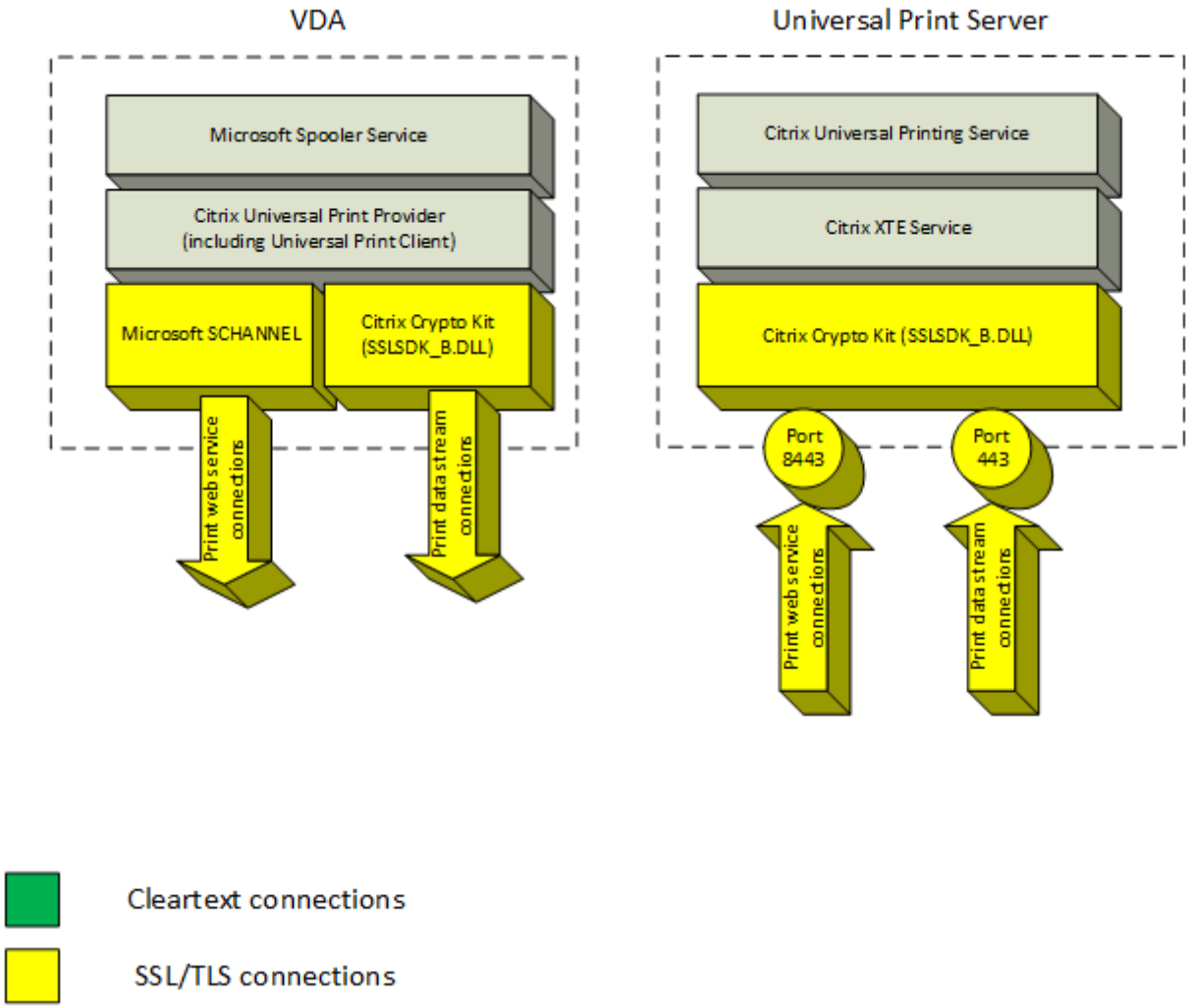


Encrypted connections

These SSL/TLS connections related to printing originate from the VDA and connect to ports on the Universal Print Server. These connections are made only when the **SSL enabled** policy setting is set to **Enabled**.

- Encrypted print web service connections (TCP port 8443)
- Encrypted print data stream (CGP) connections (TCP port 443)

© 1997–2026 Citrix Systems, Inc. All rights reserved.



SSL/TLS client configuration

The VDA functions as the SSL/TLS client.

Use Microsoft Group Policy and the registry to configure Microsoft SCHANNEL SSP for encrypted print web service connections (TCP port 8443). The Microsoft support article TLS Registry Settings describes the registry settings for Microsoft SCHANNEL SSP.

Using the Group Policy Editor on the VDA, go to **Computer Configuration > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order**. Select the following order when TLS 1.3 is set:

TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256

Select the following order when TLS 1.2 is set:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **Note:**
>
> When this Group Policy setting is configured, the VDA selects a cipher suite for encrypted print web service connections (default port: 8443) only if the connections appear in both SSL cipher suite lists:
>
> - Group Policy SSL cipher suite order list
> - List corresponding to the selected SSL Cipher Suite policy setting (COM, GOV, or ALL)
>
> This Group Policy configuration also affects other TLS applications and services on the VDA. If your applications require specific cipher suites, you might need to add them to this Group Policy Cipher Suite Order list.
>
> **Important:**
>
> Group Policy changes for TLS configuration take effect only after an operating system restart.
>
> Use a Citrix policy to configure SSL/TLS settings for encrypted print data stream (CGP) connections (TCP port 443).

SSL/TLS server configuration

The Universal Print Server functions as the SSL/TLS server.

Use the `Enable-UpsSsl.ps1` PowerShell script to configure SSL/TLS settings.

Install a TLS certificate on the Universal Print Server

For HTTPS, you must install an SSL server certificate on the Universal Print Server that is trusted by the VDAs. Use Microsoft Active Directory Certificate Services or another certification authority to request a certificate for the Universal Print Server.

Keep in mind the following considerations when enrolling/requesting a certificate using Microsoft Active Directory Certificate Services:

1. Place the certificate in the Local Computer **Personal** certificate store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Set the **Common Name** attribute of the Subject Distinguished Name (Subject DN) of the certificate to the fully qualified domain name (FQDN) of the Universal Print Server. Specify this in the certificate template.
3. Set the Cryptographic Service Provider (CSP) used to generate the certificate request and private key to **Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**. Specify this in the certificate template.
4. Set the Key Size to at least 2048 bits. Specify this in the certificate template.

For more information on creating and installing certificates, see Manage certificates.

Configuring SSL on the Universal Print Server

The XTE Service on the Universal Print Server listens for incoming connections. It functions as an SSL server when SSL is enabled. The incoming connections have two types: print web service connections, which contain printing commands, and print data stream connections, which contain print jobs. SSL can be enabled on these connections. SSL protects the confidentiality and integrity of these connections. By default, SSL is disabled.

The PowerShell script used to configure SSL is on the installation media and has this file name: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

Configuring listening port numbers on the Universal Print Server

These are the default ports for the XTE Service:

- Cleartext print web service (HTTP) TCP port: 8080
- Cleartext print data stream (CGP) TCP port: 7229
- Encrypted print web service (HTTPS) TCP port: 8443
- Encrypted print data stream (CGP) TCP port: 443

To change the ports used by the XTE Service on the Universal Print Server, run the following commands in PowerShell as administrator (see the later section for notes on the usage of the Enable-UpsSsl.ps1 PowerShell script):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` or `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TLS settings on Universal Print Server

If you have multiple Universal Print Servers in a load-balanced configuration, ensure that the **TLS** settings are configured consistently across all Universal Print Servers.

When you configure TLS on Universal Print Server, permissions on the installed TLS certificate are changed, giving the Universal Printing Service read access to the certificate's private key, and informing the Universal Printing Service of the following:

- Which certificate in the certificate store to use for TLS.
- Which TCP port numbers to use for TLS connections.

The Windows Firewall (if enabled) must be configured to allow incoming connections on these TCP ports. This configuration is done for you when you use the Enable-UpsSsl.ps1 PowerShell script.

- Which versions of the TLS protocol to allow.

Universal Print Server supports TLS protocol versions 1.3 and 1.2. Specify the minimum allowed version.

The default TLS protocol version is 1.2.

> **Note:**
>
> TLS 1.1 and 1.0 are no longer supported from Citrix Virtual Apps and Desktops version 2311.

- Which TLS cipher suites to allow.

A cipher suite selects the cryptographic algorithms that are used for a connection. VDAs and Universal Print Server can support different sets of cipher suites. When a VDA connects and sends a list of supported TLS cipher suites, the Universal Print Server matches one of the client's cipher suites with one of the cipher suites in its own list of configured cipher suites and accepts the connection. If there is no matching cipher suite, the Universal Print Server rejects the connection.

The Universal Print Server supports the following sets of cipher suites named GOV(ernment), COM(mercial), and ALL for the OPEN, FIPS, and SP800-52 native Crypto Kit modes. The acceptable cipher suites also depend on the **SSL FIPS Mode** policy setting and on the Windows FIPS Mode. See this Microsoft support article for information about Windows FIPS mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cipher suite (in decreasing priority order)	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

Configure TLS on a Universal Print Server using the PowerShell script

Install the TLS Certificate in the **Local Computer > Personal > Certificates** area of the certificate store. If more than one certificate resides in that location, supply the thumbprint of the certificate to the `Enable-UpsSsl.ps1` PowerShell script.

> **Note:**
>
> The PowerShell script finds the correct certificate based on the FQDN of the Universal Print Server. You do not need to supply the certificate thumbprint when only a single certificate is present for the Universal Print Server FQDN.

The `Enable-UpsSsl.ps1` script enables or disables TLS connections originating from the VDA to the Universal Print Server. This script is available in the **Support > Tools > SslSupport** folder on the installation media.

When you enable TLS, the script disables all existing Windows Firewall rules for the Universal Print Server's TCP ports. It then adds new rules that allow the XTE Service to accept incoming connections only on the TLS TCP and UDP ports. It also disables the Windows Firewall rules for:

- Cleartext print web service connections (default: 8080)
- Cleartext print data stream (CGP) connections (default: 7229)

The effect is that the VDA can make these connections only when using TLS.

> **Note:**
>
> Enabling TLS does not affect Windows Print Spooler RPC/SMB connections originating from the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> VDA and going to the Universal Print Server.
>
> **Important:**
>
> Specify either **Enable** or **Disable** as the first parameter. The CertificateThumbprint parameter is optional if only one certificate in the Local Computer Personal certificate store has the Universal Print Server's FQDN. The other parameters are optional.

Syntax

```
1 Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
      HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
      SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
      FIPSMode <Boolean>] [-ComplianceMode <mode>]
2 Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

Parameter	Description
Enable	Enables SSL/TLS on the XTE Server. Either this parameter or the Disable parameter is required.
Disable	Disables SSL/TLS on the XTE Server. Either this parameter or the Enable parameter is required.
CertificateThumbprint "<thumbprint>"	Thumbprint of the TLS certificate in the Local Computer Personal certificate store, enclosed in quotation marks. The script uses the specified thumbprint to select the certificate you want to use.
HTTPPort <port>	Cleartext print web service (HTTP/SOAP) port. Default: 8080
CGPPort <port>	Cleartext print data stream (CGP) port. Default: 7229
HTTPSPort <port>	Encrypted print web service (HTTPS/SOAP) port. Default: 8443
CGPSSLPort <port>	Encrypted print data stream (CGP) port. Default: 443
SSLMinVersion "<version>"	Minimum TLS protocol version, enclosed in quotation marks. Valid values: "TLS_1.2"and "TLS_1.3". Default: TLS_1.2.
SSLCipherSuite "<name>"	Name of TLS cipher suite package, enclosed in quotation marks. Valid values: "GOV", "COM", and "ALL"(default).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter	Description
FIPSMode <Boolean>	Enables or disables FIPS 140 mode in the XTE Server. Valid values: $true to enable FIPS 140 mode, $false to disable FIPS 140 mode.

Examples

The following script enables TLS. The thumbprint (represented as "12345678987654321"in this example) is used to select the certificate to use.

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

The following script disables TLS.

```
Enable-UpsSsl.ps1 –Disable
```

Configuring FIPS mode

Enabling US Federal Information Processing Standards (FIPS) mode ensures that only FIPS 140 compliant cryptography is used for Universal Print Server encrypted connections.

Configure FIPS mode on the server before configuring FIPS mode on the client.

Consult Microsoft's documentation site for enabling/disabling Windows FIPS mode.

Enabling FIPS mode on the client

On the Delivery Controller™, run Web Studio and set the **UPS FIPS Mode** Citrix policy setting to **Enabled**. Enable the Citrix policy.

Do this on each VDA:

1. Enable Windows FIPS mode.
2. Restart the VDA.

Enabling FIPS mode on the server

Do this on each Universal Print Server:

1. Enable Windows FIPS mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run this PowerShell command as Administrator: `stop-service CitrixXTEServer, UpSvc`
3. Run the `Enable-UpsSsl.ps1` script with the `-Enable -FIPSMode $true` parameters.
4. Restart the Universal Print Server.

Disabling FIPS mode on the client

On Web Studio, set the **UPS FIPS Mode** Citrix policy setting to **Disabled**. Enable the Citrix policy. You can also delete the **UPS FIPS Mode** Citrix policy setting.

Do this on each VDA:

1. Disable Windows FIPS mode.
2. Restart the VDA.

Disabling FIPS mode on the server

Do this on each Universal Print Server:

1. Disable Windows FIPS mode.
2. Run this PowerShell command as Administrator: `stop-service CitrixXTEServer, UpSvc`
3. Run the `Enable-UpsSsl.ps1` script with the `-Enable -FIPSMode $false` parameters.
4. Restart the Universal Print Server.

> **Note:**
>
> FIPS mode is not supported when the SSL protocol version is set to TLS 1.3.

Configuring SSL/TLS protocol version

The default SSL/TLS protocol version is TLS 1.2. TLS 1.2 and TLS 1.3 are the recommended SSL/TLS protocol versions for production use. For troubleshooting, it might be necessary to temporarily change the SSL/TLS protocol version in a non-production environment.

SSL 2.0 and SSL 3.0 are not supported on the Universal Print Server.

Setting SSL/TLS protocol version on the server

Do this on each Universal Print Server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Run this PowerShell command as Administrator: `stop-service CitrixXTEServer, UpSvc`
2. Run the `Enable-UpsSsl.ps1` script with the `-Enable -SSLMinVersion` version parameters. Remember to set this back to TLS 1.2 or TLS 1.3 when you are done testing.
3. Restart the Universal Print Server.

Setting SSL/TLS protocol version on the client

In Studio, set the **SSL Protocol Version** policy setting to the desired protocol version and enable the policy.

Ensure that the VDA's operating system supports the selected TLS version. For supported TLS versions on Windows, see Microsoft Learn - TLS protocol version support. To configure the registry to override defaults, see Microsoft Learn - TLS, DTLS, and SSL protocol version settings.

Troubleshooting

If a connection error occurs, check the C:\Program Files (x86)\Citrix\XTE\logs\error.log file on the Universal Print Server.

The error message **SSL handshake from client failed** appears in this log file if the SSL/TLS handshake fails. Such failures can occur if the SSL/TLS protocol version on the VDA and the Universal Print Server do not match.

Use the Universal Print Server FQDN in the following policy settings that contain Universal Print Server host names:

- Session printers
- Printer assignments
- Universal Print Servers for load balancing

Ensure that the system clock (date, time, and time zone) are correct on the Universal Print Servers and the VDAs.

Virtual channel allow list

September 13, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
```

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.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `%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.
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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`

WebSocket communication between VDA and Delivery Controller™

September 6, 2025

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.

How it works

The following sections describes the workflow for the WebSocket connection between a Delivery Controller and a VDA:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

During normal brokering operation

1. Citrix Virtual Apps and Desktops™ 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 VDAs 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 the service key signed by the private key.
5. The Delivery Controller verifies the signed service key authorization 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.

When LHC mode becomes active

If you enable the Websocket support for LHC, then during the LHC mode, when a VDA tries to establish a Websocket connection with the High Availability Service, the High Availability Service verifies the signed service key authorization header with the public key from the local database. This authenticates the Websocket connection and the WebSocket connection between the VDA and Delivery Controller is successful even in LHC mode.

WebSocket support

Before you begin

1. Configure your site. For more information, see Create a site.
2. Install TLS certificates on the Delivery Controllers. For more information, see Install TLS server certificates on Controllers.
3. Install root CA and intermediate CA on VDA to trust the Delivery Controller.

Procedure

Follow the instructions to set up a WebSocket connection:

1. Enable WebSocket connection on the Delivery Controller. Run the following command on each Delivery Controller present on your site:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy
"-Name "WebSocket_Enabled"-PropertyType "DWord"-Value 1 -Force
```

2. Restart the Broker Service after enabling the WebSocket.
3. Enable websocket support for the LHC mode. Run the following command on each Delivery Controller present on your site:

```
1 New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\LHC" -Name "
    WebSocketEnabledLhc" -PropertyType "DWord" -Value 1 -Force
```

4. Create a machine catalog for AD-joined VDAs with MCS provisioning. For more information, see Create machine catalog.
5. Create a delivery group and add your VDA to it. For more information, see Create delivery groups.
6. Enable WebSocket connection on the VDA. Run the following PowerShell command on the VDA:

```
1 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:

     ```
     1 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
         CitrixBrokerAgent\WebSocket
     ```

     Name: Enabled

     Type: REG_DWORD

     Value: 1

HDX™ connectivity

September 6, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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

September 13, 2025

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.
- **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.

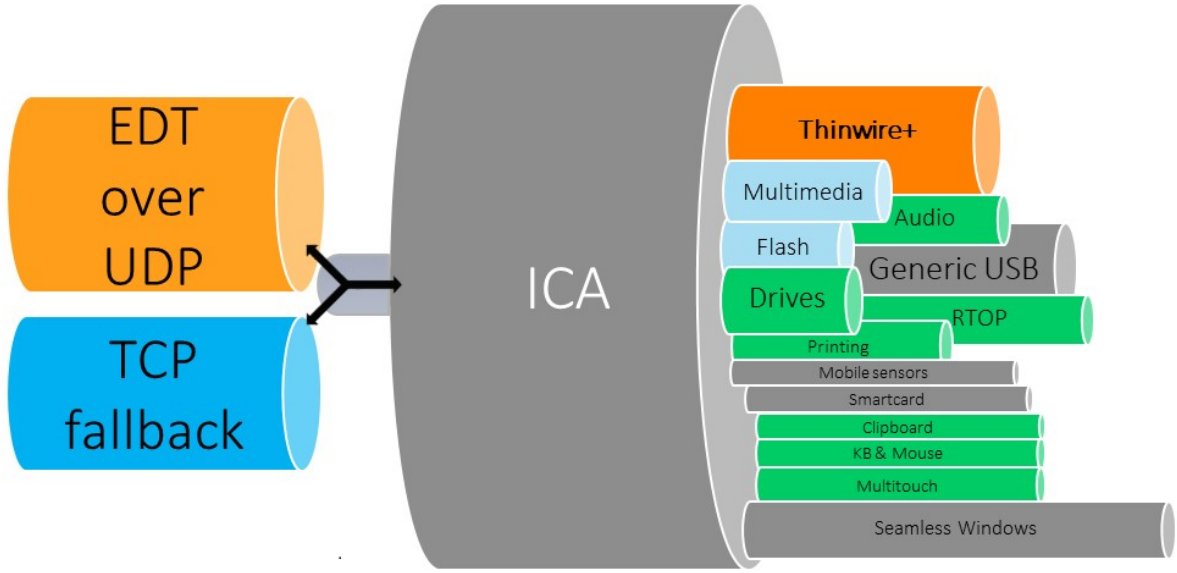
How it works

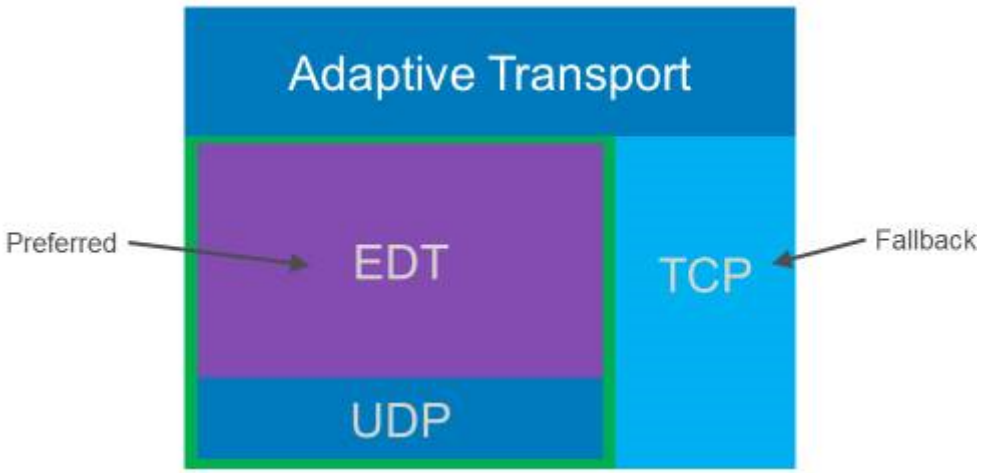
When **Adaptive Transport** is set to `Preferred`, the client attempts to connect to the session with both the preferred protocol and TCP in parallel. This allows optimizing the connection time if it's not possible to connect with the preferred protocol and the client must fall back to using TCP. If the connection is established using TCP, the client attempts to connect with the preferred protocol in the background every five minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.





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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Virtual Delivery Agent
  - Windows: currently supported version (2402 or later is recommended)
  - Linux: currently supported version (2402 or later is recommended)
- Citrix Workspace™ app
  - Windows: currently supported version (2402 or later is recommended)
  - Linux: currently supported version (2402 or later is recommended)
  - Mac: currently supported version (2402 or later is 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)

> **Note:**
>
> For details on Linux VDA, 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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 Reliability enabled	UDP	Client network	VDA network	2598
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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Description	Protocol	Source	Destination	Destination port
Internal connection - Session Reliability enabled	UDP	Client IP	VDA network	2598
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

September 6, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When **Adaptive Transport** is enabled, EDT is the preferred protocol.

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.

In scenarios where dynamic routing through asymmetrical paths may cause the MTU for the session to change, MTU Discovery can also detect and adjust the session's MTU accordingly. Rediscovery is disabled by default. To enable it, see HDX features managed through the registry.

> **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.

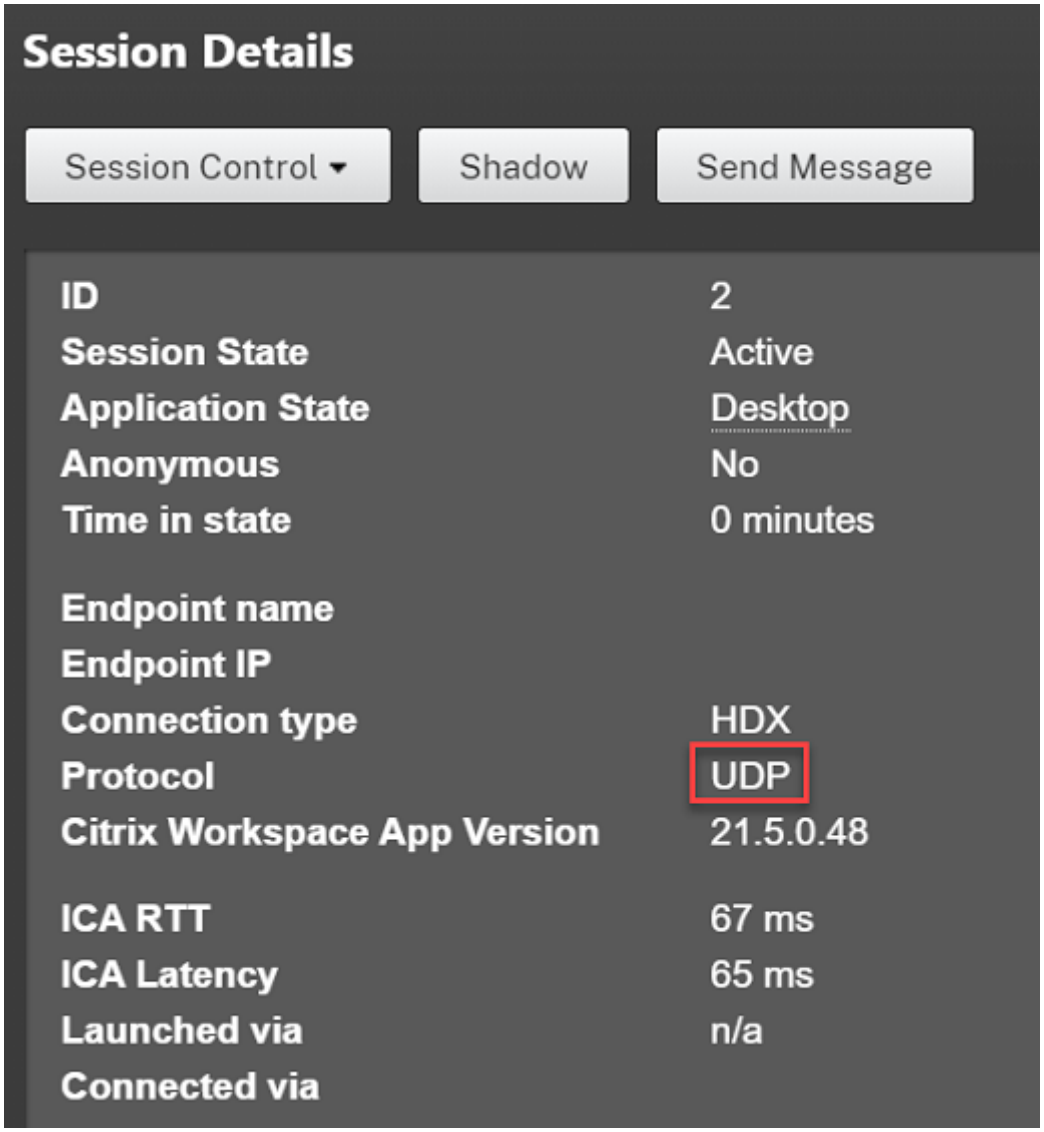
Troubleshooting

September 13, 2025

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.

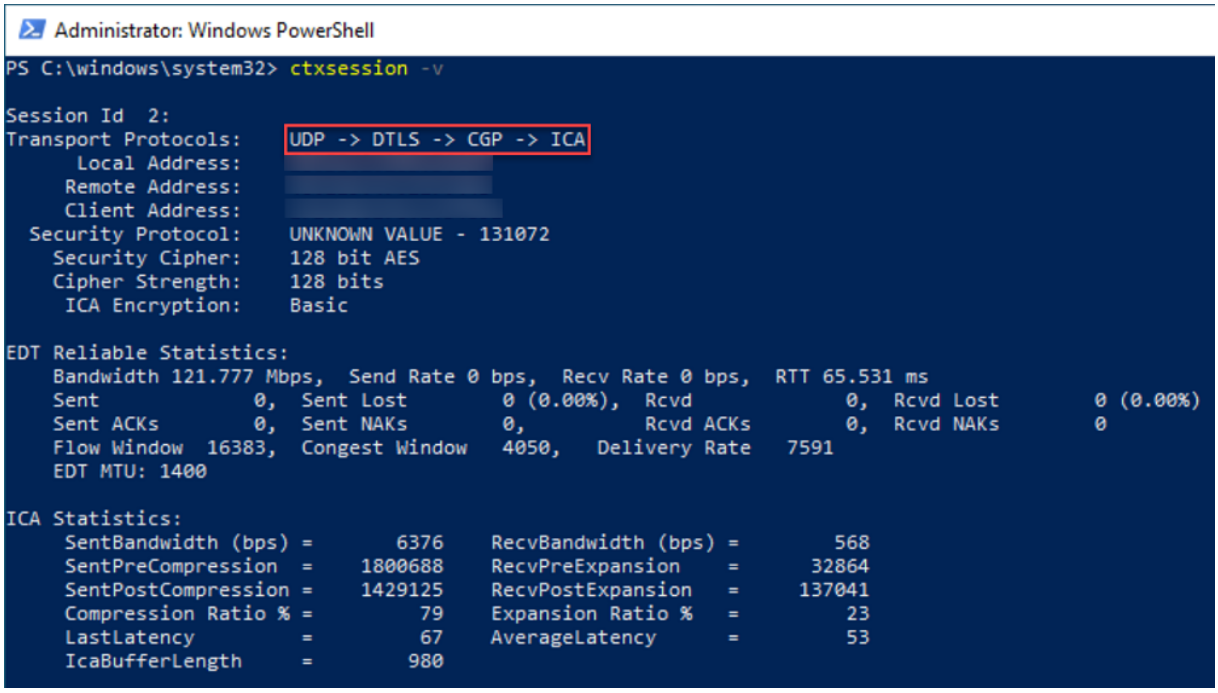
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. If EDT works for direct internal connections and not for sessions going through NetScaler Gateway or Citrix Gateway Service:

    - 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. [CVADHELP-16654]
- 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. [CGOP-18438]
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX™ Direct

September 6, 2025

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
- Access tier
  - Citrix Workspace™
  - 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **HDX Direct port range**: Defines the port range that the VDA uses for connections from external clients.

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.

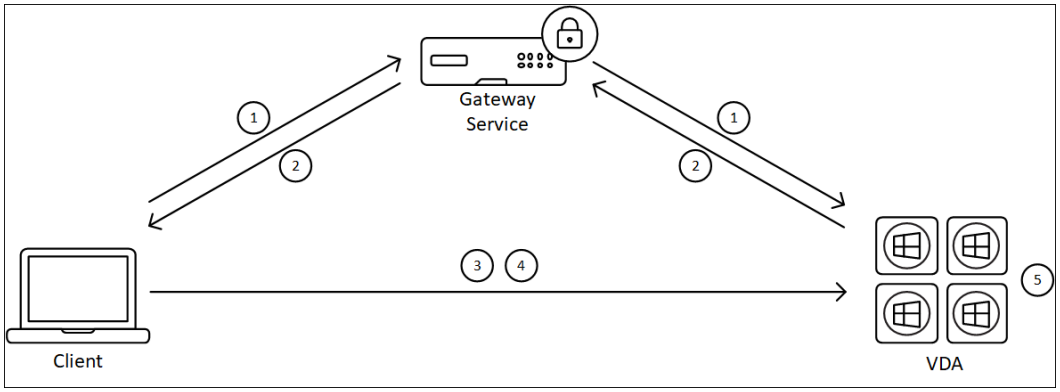
How it works

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. The client establishes an HDX session through the Gateway Service.
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.

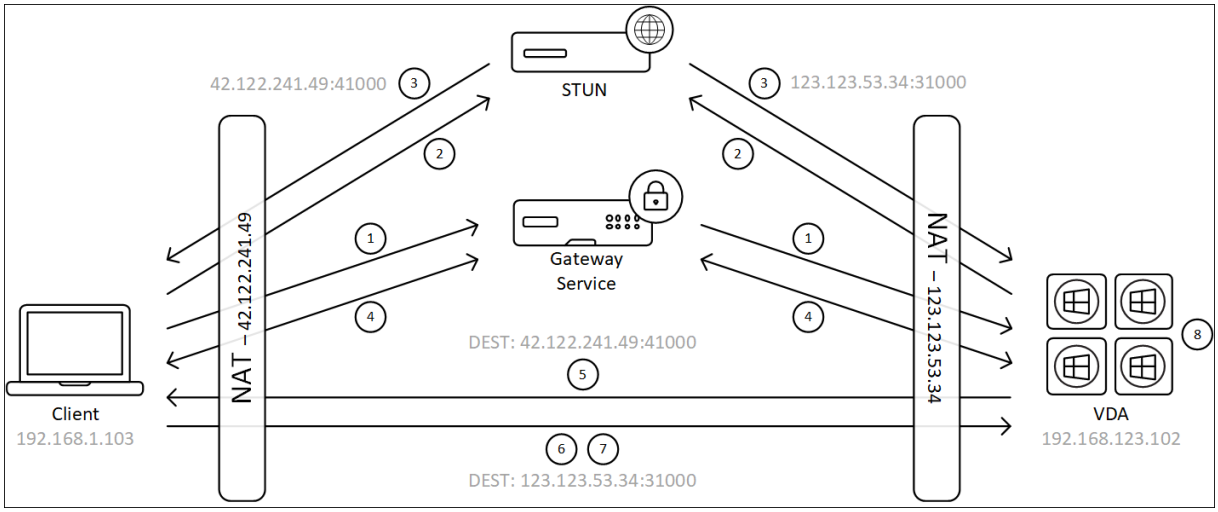
Traditional direct connections When using Storefront, Workspace with Direct Workload Connection, or Workspace configured for internal-only connectivity, direct connections are established between the client and the session host without the need to route through a Gateway first.

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

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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.

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 Workspace or 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\Ter**
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\Ter**
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:

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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

September 6, 2025

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 to perform NAT binding and behavior test:
   `stunclient.exe stunserver2025.stunprotocol.org --mode behavior`
4. If the binding and behavior tests are successful, both **binding test** and **behavior test** report the success and a NAT behavior is specified:

   If the tests fail, **binding test** and/or **behavior test** report the failure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Run the following command to perform NAT binding and filtering test:
   `stunclient.exe stunserver2025.stunprotocol.org --mode filtering`
6. If the binding and filtering tests are successful, both **binding test** and **filtering test** report the success and a NAT filtering type is specified:

   If the tests fail, **binding test** and/or **filtering test** report the failure.

After performing the tests above, check the following table to determine if HDX Direct for external users is expected to work based on the NAT behavior and filtering combination:

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
Endpoint Independent Mapping	Address Dependent Filtering	Address Dedependent Mapping	Any	No
Endpoint Independent Mapping	Address and Port Dependent Filtering	Address Dedependent Mapping	Any	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 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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

September 6, 2025

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`.

```
PS C:\Users\                > ctxsession -v

Session Id  1:
Transport Protocols:    UDP -> DTLS -> CGP -> ICA
      Local Address:                :55000
     Remote Address:                :60410
     Client Address:                :63274
  Security Protocol:    DTLS 1.2
    Security Cipher:    256 bit AES
    Cipher Strength:    256 bits
     ICA Encryption:    Transport Only
 Rendezvous Version:    None
   HDX Direct State:    Connected - External
    Reducer Version:    4.0

EDT Reliable Statistics:
    Bandwidth 301.904 Mbps,  RTT 57.690 ms,  EDT MTU: 1480

EDT Unreliable Statistics:
    Bandwidth 7.544 Kbps,  RTT 1 us,  EDT MTU: 1480

EDT Reliable Basic FEC Statistics:
    Bandwidth 92.090 Mbps,  RTT 35.164 ms,  EDT MTU: 1480

ICA Statistics:
     SentBandwidth (bps)      =          0
     HDX Latency              =         63
     IcaBufferLength          =       1436
```

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
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-Citrix-Certificate-Manager`
    b) Issued by: `CA-Citrix-Certificate-Manager`
    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-Citrix-Certificate-Manager`
    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 that the session host contains the list of STUN servers:
        - 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
    b) 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c) 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.

d) Ensure that your network firewalls have the appropriate rules configured to allow all necessary traffic. See the Network Requirements section for details.

e) 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.

Known issues

- HDX Direct for external users may fail in environments that use Workspace with Gateway Service if Rendezvous is disabled. To resolve this issue, ensure that Rendezvous is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.
  8. Start the **Citrix Certificate Manager Service**.

Secure HDX™

June 25, 2026

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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
- Access tier
  - Citrix Workspace
  - 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> support)
> - Connections using IPv4

Considerations

The following are considerations for using Secure HDX:

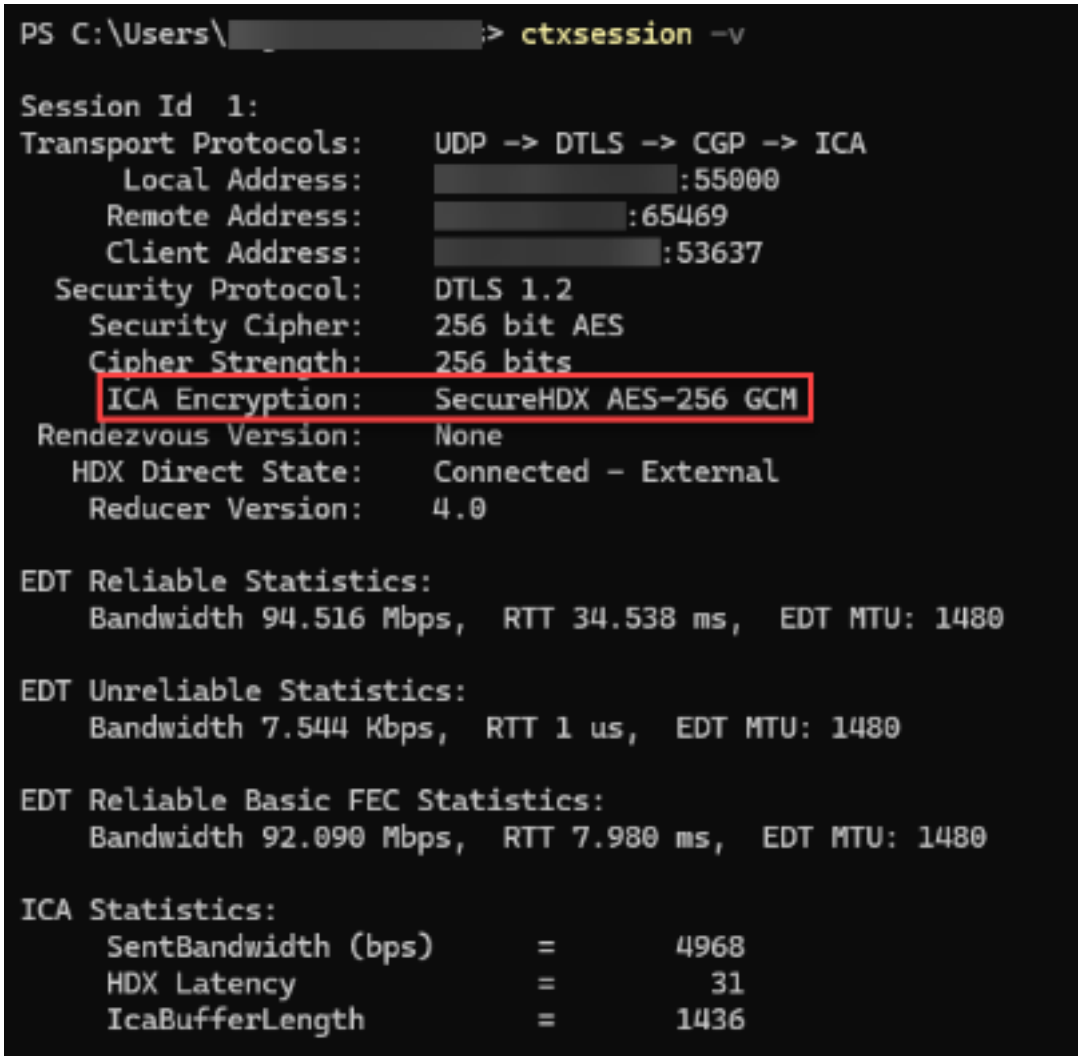
- If a user tries to connect to a session host with Secure HDX enabled using a client that does not support the feature, the connection will be denied.
- Only Service Continuity for connector-less workloads is supported with Secure HDX. If you are using the standard version of Service Continuity, you 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

May 27, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
  - Citrix Workspace
  - 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 NetScaler Gateway	UDP	NetScaler SNIP	1024-65535	VDA network	443
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

September 13, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
```

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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.
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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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`

Troubleshooting

May 5, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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>

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log Name	Id	Source	Level	Description
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> 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>

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log Name	Id	Source	Level	Description
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 VC policy path is not found

Known third-party virtual channels

September 6, 2025

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
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- 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'

© 1997–2026 Citrix Systems, Inc. All rights reserved.

vendors. Alternatively, follow the steps outlined in the Obtaining virtual channel names and processes section.

Virtual Channel Allow List for DVC

September 6, 2025

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:

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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`
- 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

September 6, 2025

HDX™ provides a high-definition user experience on any device, at any location. The articles in the Devices section describe these devices:

- Scanning
- Generic USB device
- Client Drive Mapping
- Mobile and touch screen devices
- Serial devices
- Specialty keyboards
- Webcams

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.

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 http://support.citrix.com/article/CTX123015.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Scanning

September 6, 2025

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.
- **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.).
- **SANE:** scanning protocol is a set of standards and guidelines that allow software applications to communicate with and control image scanners. SANE stands for **S**canner **A**ccess **N**ow **E**asy, and its protocol defines how scanner hardware can be accessed, managed, and controlled by software running on different computer systems.

TWAIN Redirection

September 13, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Introduction

Users can scan documents from applications within Citrix HDX™ sessions using TWAIN compliant scanners connected to the client endpoint. The Citrix scanning module redirects the scan request to the client endpoint to process the request. Upon completion, the scanned information is sent to back to the VDA host.

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
  - 64-bit application

> **Note:**
>
> - To enable scanning functionality for 64-bit applications on the session host, the 64-bit TWAIN Data Source Manager (twaindsm.dll) is necessary. This component is not pre-installed by the operating system.
> - If your 64-bit scanning application does not include this file, please contact the application vendor to acquire the 64-bit twaindsm.dll.
> - Once obtained, administrators must manually copy the file into the **System32** folder on the session host and then restart the machine.

© 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
  - Install TWAIN drivers on the client endpoint

Configuration

TWAIN redirection is enabled by default. The following policy settings are available to configure TWAIN redirection and optimize the scanning experience.

- **Client TWAIN device redirection:** to enable or disable TWAIN redirection.
- **TWAIN compression level:** to set compression levels for images trnasferred from the client to the VDA.

For more details, see TWAIN devices policy settings.

Troubleshooting

TWAIN redirection functionality can be tested with a publicly available test app Twacker, which can be downloaded from this URL.

Follow the steps to validate TWAIN functionality within an HDX session:

1. Install **Twacker** on the VDA host.
2. Launch **Twacker** (32-bit or 64-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:

- Correctly configured to use TWAIN redirection
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WIA devices

September 6, 2025

WIA devices, such as digital cameras and scanners, communicate with server-hosted image processing applications by using the WIA framework.

Prerequisites

- 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.

Configuration

WIA redirection is disabled by default. The following setting can be enabled in Citrix® policy:

- WIA redirection: This setting allows or prohibits users from accessing WIA devices on the user device.

> **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 the Registry Editor can be solved.
> Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

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 VDA that contains Windows Image Acquisition. By default, no applications have access to Windows Image Acquisition.

For 64-bit applications, the following values need to be set:

Append the full path of the scanning application or applications in the AllowProcesses registry value:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Key: HKLM\SOFTWARE\Citrix\WIAAllowedProcesses
- Value name: AllowProcesses
- Value type: REG_MULTISZ
- Value data: <add full path of the scanning application >
- Key:HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\WIAHook<App_Name>

For 32-bit applications, the following values need to be set:

Append the full path of the scanning application or applications in the AllowProcesses registry value:

- Key: HKLM\SOFTWARE\Citrix\WOW6432Node\WIAAllowedProcesses
- Value name: AllowProcesses
- Value type: REG_MULTISZ
- Value data: <add full path of the scanning application >
- Key:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\WIAHook<App_Nam

Reboot the VDA after setting the registry values of WIA redirection to be enabled for WIA based applications.

For information about policy settings, see WIA devices policy settings.

Scanning on non-windows client platforms - SANE Redirection

September 6, 2025

Introduction

Users can scan documents from TWAIN applications inside their Citrix® sessions from ChromeOS endpoints. When a user tries to scan a document from an application, the Citrix scanning module redirects the request to the client endpoint to achieve scanning from the scanner and the files are sent to the VDA once the scan is complete.

Requirements

Citrix Control Plane

- Citrix Virtual Apps and Desktops™ 2411 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix DaaS™

Session Host

- Operating system
  - Windows 10 1809 or later
  - Windows 11
  - Windows Server 2019 or later
- VDA
  - Version 2411 or later

Client Device

- Operating system
  - ChromeOS v129 or later
- Workspace app
  - ChromeOS: version 2409 or later
- Scanner
  - The scanner must be supported by Chrome OS
  - Supported devices: Fujitsu FI-7160, FI-8170

    > **Note:**
    >
    > Scanners other than ones listed above can be used using Native Twain UI if supported by Chrome OS.

  - Must be attached to the client endpoint locally through USB.

Configuration

No additional configuration is required to enable this functionality. This feature is enabled by default.

> **Note:**
>
> To disable this feature, open the Web studio/DaaS console. Set the SANE scanner redirection policy setting to Prohibited.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

Event logs

Administrators can view various scanning related event messages.

Listed below are the event messages that will be logged in the Event viewer on the VDA host for various scan related operations. They can be viewed under the Application section of the Windows Logs with HDX™ Scanner as the event source.

Event ID	Event Text	Explanation
2	AllowScannerSANERedirection policy is disabled. Scanner's not redirected.	Indicates that the SaneRedirection policy is disabled.
3	Scanning details: Pages - '[pages]', Application - '[application]', Scanner - '[scanner]', User - '[user]', Average time per page - '[time]' milliseconds.	Generated when a scan is completed.
101	No page found to scan.	Generated when no document is detected.
102	Scan failure - The device's document feeder is jammed.	Generated when a scan fails due to a paper jam in the scanner's document feeder.
103	Scan failure - '[failure]'. Close and restart the scanner application.	Generated when the scan fails due to errors like unsupported operations, end of file error, access denied errors, etc.
104	Memory failure in application. Restart the application.	Generated when a scan fails due to insufficient memory.
201	Scan operation cancelled by user.	Generated when the scan operation is cancelled by the user.
202	Session disconnected while scanning.	Generated when the HDX session disconnects while scanning.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Event Text	Explanation
203	Unsupported conversion between TWAIN and SANE for '[capability]'. Please check if the scanner/application is supported.	Indicates that the conversion between TWAIN and SANE for the specified capability is not supported.
205	Failed to set the scanner '[scanner]'as active. Please check if the scanner is switched on and connected.	Generated when a connection to a scanner fails to open.
206	Scanner not found. Please check if the scanner is switched on and connected.	Generated when no scanner is detected on the client endpoint.

Known Limitations

1. Network authorized scanners are not supported.
2. Some proprietary scanning applications such as the Fujitsu Paperstream app on the VDA may not list the redirected scanner as supported.
3. Some of the scanner settings such as page width, page height, paper size, brightness and contrast might not be honored due to 3rd party API limitations when using the Native UI.

USB devices

September 6, 2025

Introduction

The generic USB redirection feature allows redirection of USB devices from client machines to HDX™ sessions giving end users the ability to interact with a wide selection of generic USB devices in their HDX session. This is helpful in scenarios where users need to use speciality devices that don't have optimized support or where it is unsuitable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> USB Devices not optimized for virtual channel support will fall back to the Generic USB virtual channel using raw USB redirection.

How does it work?

Generic USB redirection works at a low level and redirects USB request and response messages between client machines and XenDesktop® virtual desktop.

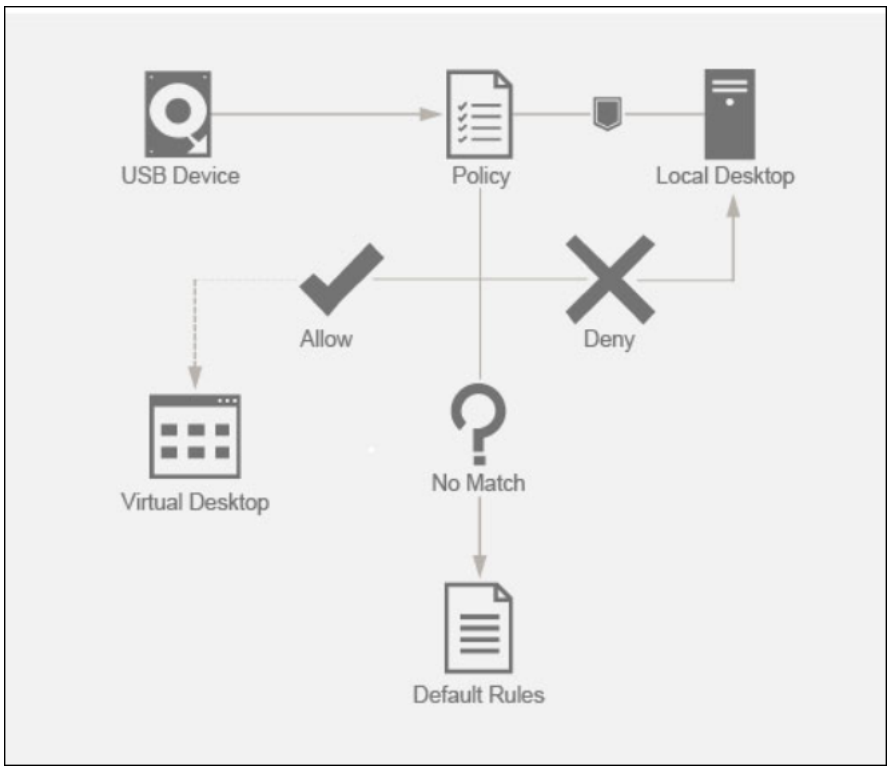
It avoids the requirement for compatible device drivers on the client machine and the driver is expected to be supported on the virtual desktop only. USB redirection policy rules follow a certain order of precedence that allow client side policies and default rules to be honored after DDC policy rules have been evaluated and enforced. This allows Citrix admins to prevent any unauthorized/spoofed devices from being redirected inside a session.

Additionally, event logging of unauthorized devices attempting to access the remote session can be audited and flagged and admins can take additional action to prevent data exfiltration.

When a user plugs in a USB device, the session host checks it against each policy rule consecutively until a match is found. The first match for any device is considered definitive.

- If the first match is an Allow rule, the device is redirected to the virtual desktop.
- If the first match is a Deny rule, the device is not redirected to the session, and only available for use in the local user device. If no match is found, default rules are used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Compatibility with generic USB redirection

These Citrix Workspace™ apps support generic USB redirection:

- Citrix Workspace app for Windows, see Citrix Workspace app for Windows.
- Citrix Workspace app for Mac, see Citrix Workspace app for Mac.
- Citrix Workspace app for Linux, see Citrix Workspace app for Linux.
- Citrix Workspace app for Chrome OS, see Citrix Workspace app for Chrome.

For Citrix Workspace app versions, see the Citrix Workspace app feature matrix.

Configuration

September 6, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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**.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

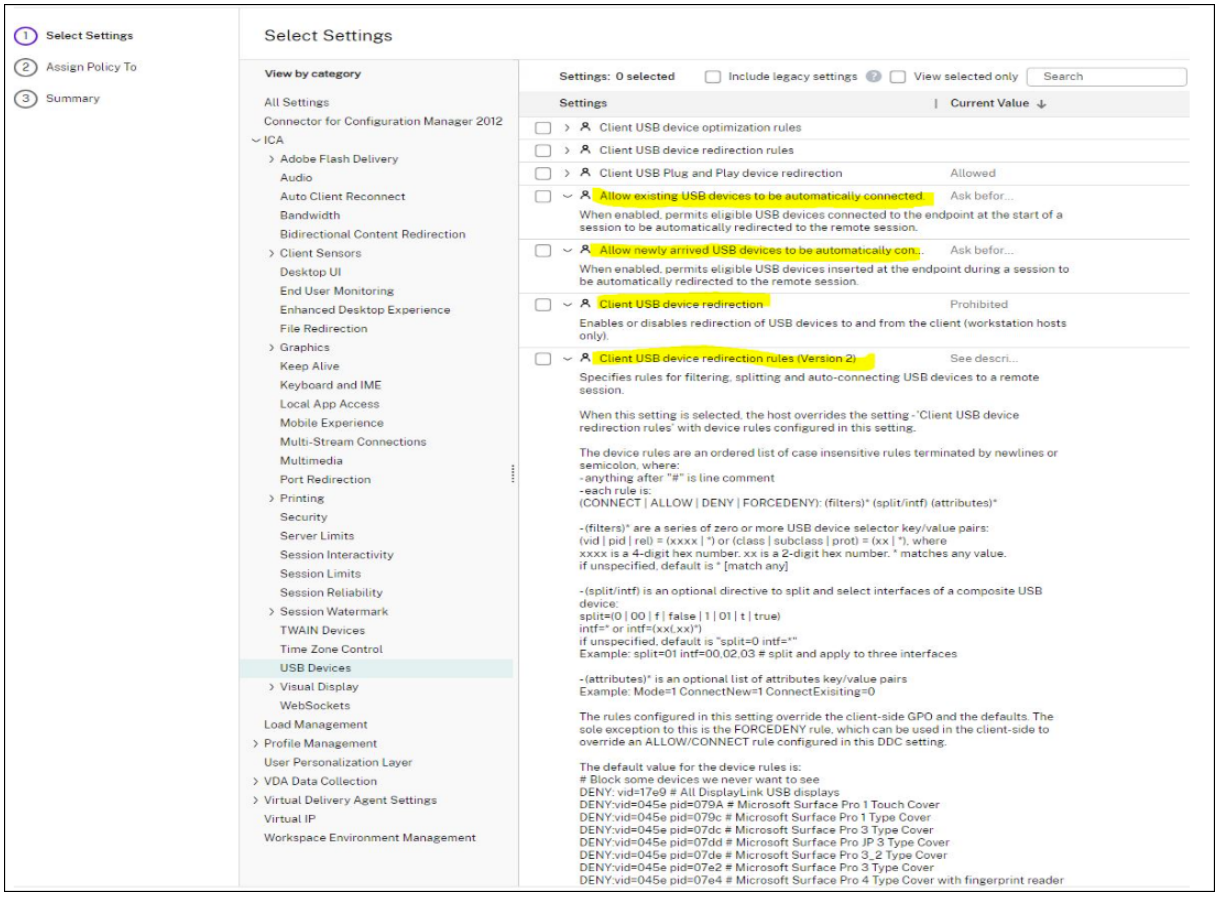
Each rule consists of an action keyword (**Allow, Connect, or Deny**), a colon (:), and zero or more filter parameters that match actual devices at the endpoints USB subsystem. These filter parameters correspond to the USB device descriptor metadata used by every USB device to identify itself.

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 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**.

Understanding USB Device Redirection Rules

When using Citrix Client USB redirection, it's important to understand how different rules are prioritized and applied. Think of it like a set of instructions: the system checks for rules in a specific order, and the first rule it finds for a particular device is the one that sticks. Any other rules for that **same device** found further down the list are then ignored.

Here's the order in which your device rules are evaluated:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Client USB device redirection rules (Version 2)**: Device rules configured by this policy setting are given the highest priority. If a rule for a specific device is found here, that rule is applied, and no other rules for that particular device will be considered.
- **Client USB device redirection rules**: Next in line are rules defined in this legacy setting within Citrix Studio. If no rule for a device was found in the Version 2 policy, the system then checks rules defined in this policy setting. Again, if a rule for a device is found here, it's applied, and the system stops looking for rules for that specific device.

  > **Note:**
  >
  > The above policy setting is only applied if **Client USB device redirection rules (Version 2)** is not set in Studio or if the **Citrix Workspace App for Windows** version is older than 2212.

- **Client-side Group Policy Objects (GPOs)**: If a device still doesn't have an applied rule after checking both Studio policy settings, the system then defers to rules configured via client-side Group Policy Objects.
- **Client-side Registry Settings**: Finally, client-side registry settings are applied as the lowest priority.

This hierarchy ensures that more specific or newer configurations take precedence for a given device, providing a clear and predictable way to manage USB device redirection. It's important to remember that while the hierarchy determines the order of evaluation, a rule found for a device at a higher level will prevent rules for that **same device** from being applied at lower levels.
However, rules set at lower levels are not completely ignored; they are still evaluated for any devices that haven't had a rule applied yet.

This tiered approach also guarantees **backwards compatibility**. When upgrading from older versions of Citrix Virtual Apps and Desktops™ or Citrix Workspace app, existing client-side configurations will be preserved. This gives enterprise admins time to plan the migration path to the more advanced **Version 2 device rules** policy setting in Studio without immediate disruption.

Example:

Let's say you have a specific USB device with Vendor ID (VID) `xxxx` and Product ID (PID) `yyyy`.

- In your **Client USB device redirection rules (Version 2)** policy setting in Citrix Studio, you have a rule set `CONNECT VID=xxxx PID=yyyy`.
- Separately, in a client-side **Group Policy Object (GPO)**, you have a `DENY` rule for the same device `DENY: VID=xxxx PID=yyyy`.

When this device is connected to the client endpoint, the system will first evaluate the rules in the Version 2 Studio policy. It finds the `CONNECT` rule `VID=xxxx PID=yyyy`. Because this rule is at the highest precedence level, it is immediately applied. The system then ignores any further rules for

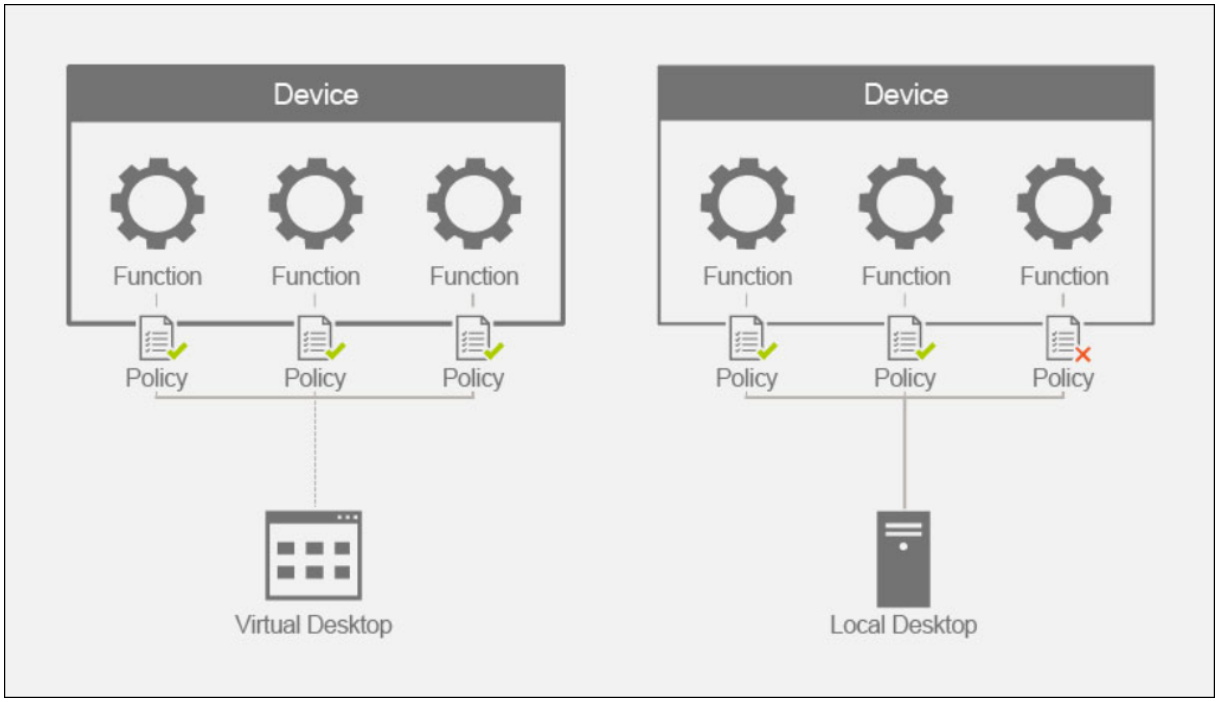
© 1997–2026 Citrix Systems, Inc. All rights reserved.

this specific device. Therefore, even though a DENY rule exists in a client-side GPO, it will be ignored, and the device will successfully redirect.

Composite Devices and Device Splitting

September 6, 2025

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 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
2. Enable the **Client USB device redirection** policy setting in **Citrix Web Studio™**.
3. Edit the **Client USB device redirection rules** (**Version 2**) policy setting.
    a) Set the **VID** and **PID** information for the signature pad that needs to be redirected and click **Save**. For example: **Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB
4. Edit the policy setting **Client USB device optimization rules**.
    a) Set the mode along with other device information. For example: Mode=00000004 VID=06A8 PID=0057 class=03 #Input device operating in capture mode
5. Edit the policy setting **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 setting **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 settings are configured, 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. Enable the **Client USB device redirection** policy setting in **Citrix Web Studio**.
2. Bloomberg 5 keyboards are set by default in the **Client USB device redirection rules (Version 2)** policy setting and no additional admin action is needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Edit the policy 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 policy 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**.

Once these settings are configured, 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. Enable the **Client USB device redirection** policy setting in **Citrix Web Studio**.
2. Edit the **Client USB device redirection rules (Version 2)** policy setting.
    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 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 policy 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once these settings are configured, FIDO2 keyboards will automatically be presented in subsequent HDX sessions and will not require any additional end user action.

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. Enable the **Client USB device redirection** policy setting in **Citrix Web Studio**.
3. Edit the **Client USB device redirection rules** (**Version 2**) policy setting.
    a) Add 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 setting **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 setting **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 setting **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**.

Configuring two or more devices using USB redirection with different device rules

Multiple devices can be redirected inside the HDX session with different device rules. An admin may want to redirect one device automatically while providing an option to the end user to redirect the other device. The following are the steps to configure two devices with different rules.

1. Enable the **Client USB device redirection** policy setting in **Citrix Web Studio**.
2. Edit the **Client USB device redirection rules** (**Version 2**) policy setting.
    a) Add the **VID** and **PID** information of the two devices to be redirected with the appropriate device rule in the session and click **Save**.
    b) **Allow**: VID=0911 PID=0c1c #Phillips speech mic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c) **Connect**: VID=06A8 PID=0043 class=03 # Topaz HSB signature pad

3. Edit the policy 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 policy 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**.

Once these settings are configured, the Topaz HSB signature pad will automatically be presented in subsequent HDX sessions and will not require any additional end user action. The Phillips speech mic on the other hand will require the end user to enable redirection in Connection Center or in the Devices tab of CDViewer.

Troubleshooting

May 5, 2025

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).

   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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

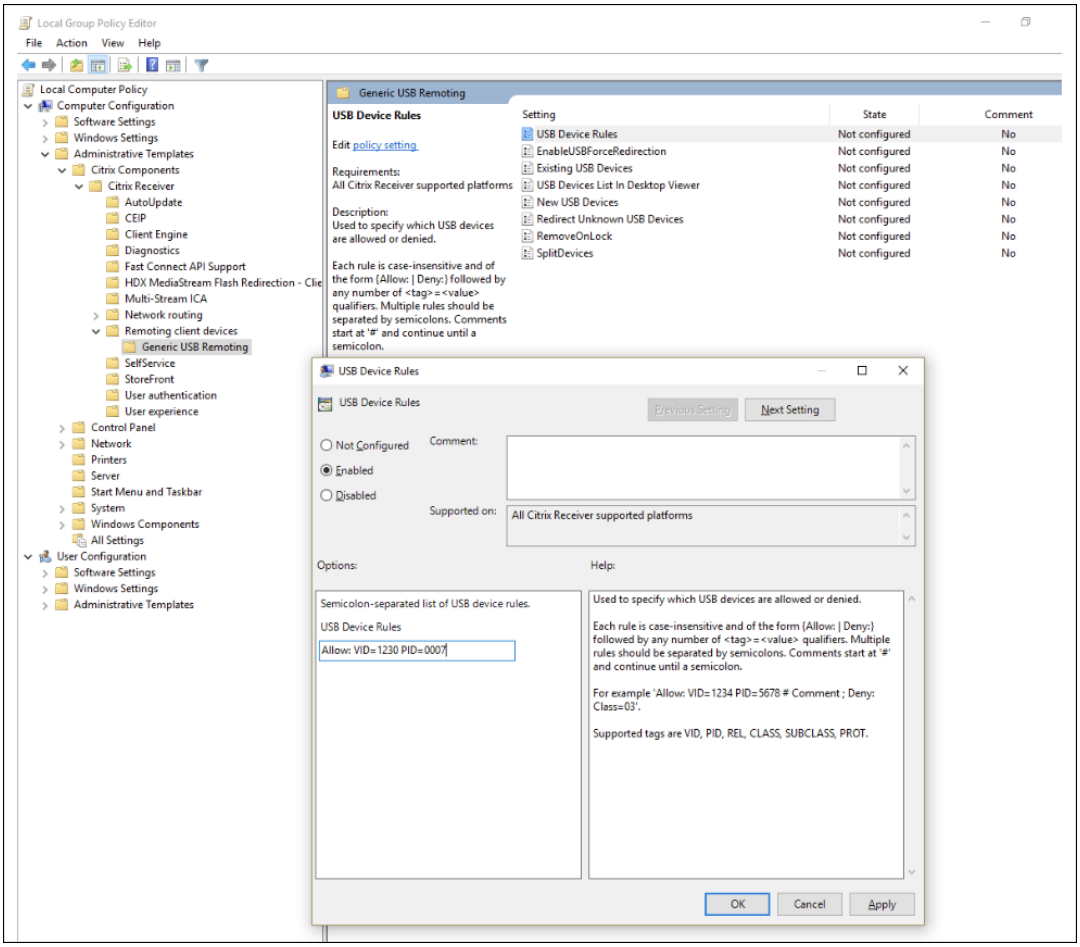
6. Validate USB related rules are set correctly on the client endpoint:

   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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

September 6, 2025

`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.
> - `CtxUsbDiagnostics.exe` is located in `C:\Program Files\Citrix\HDX\bin\`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> `CtxUsbDiagnostics.exe`.
> and is already part of the environment variables. You need not navigate to this path and can directly run this tool on the command prompt with elevated privileges.

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

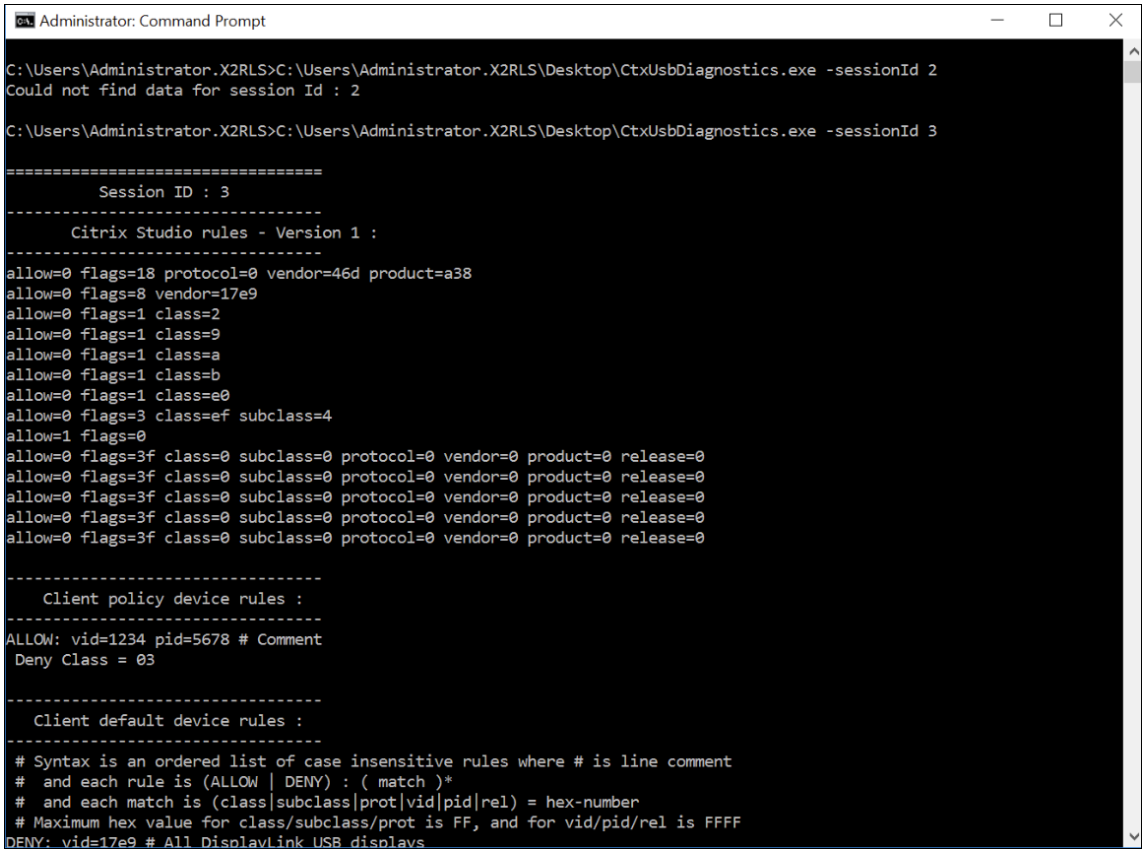
- Operating system
  - Windows 10 1809 or later
- Workspace App
  - Windows: version 2311 or later

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

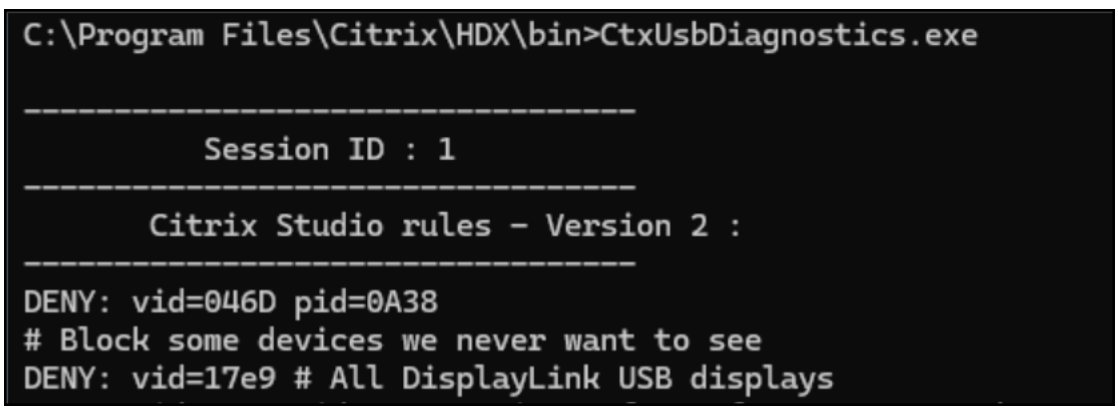
© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note :**
>
> The administrator can see device information for all active sessions.

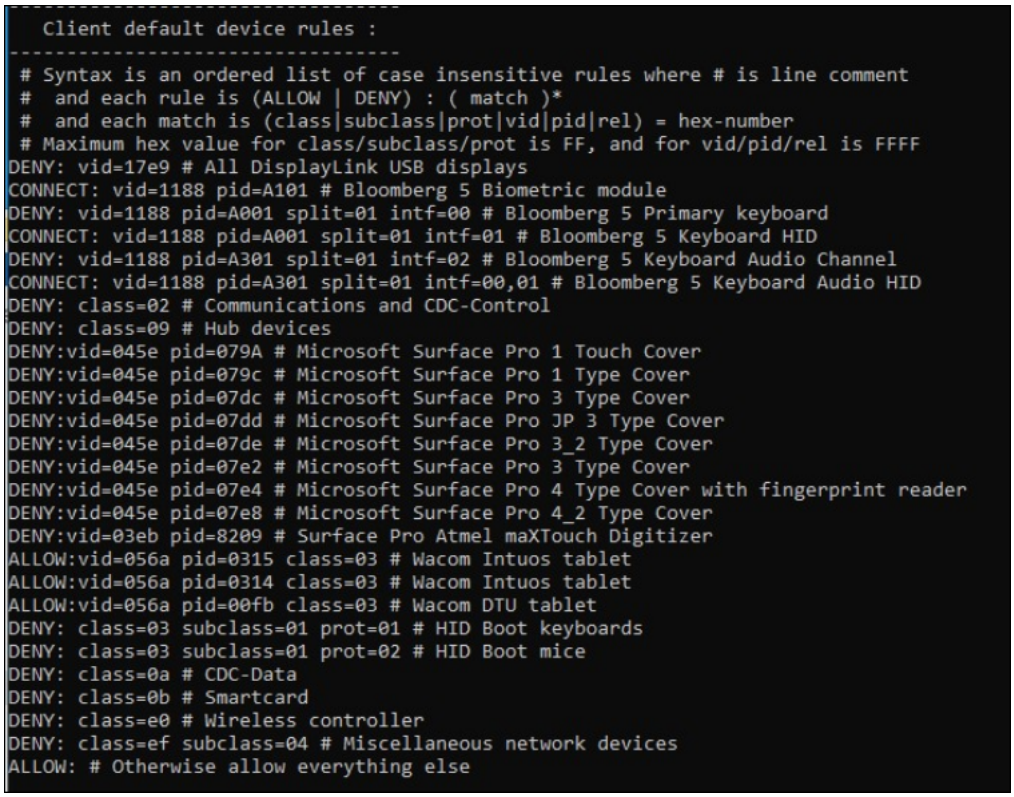
Information Displayed

- **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.



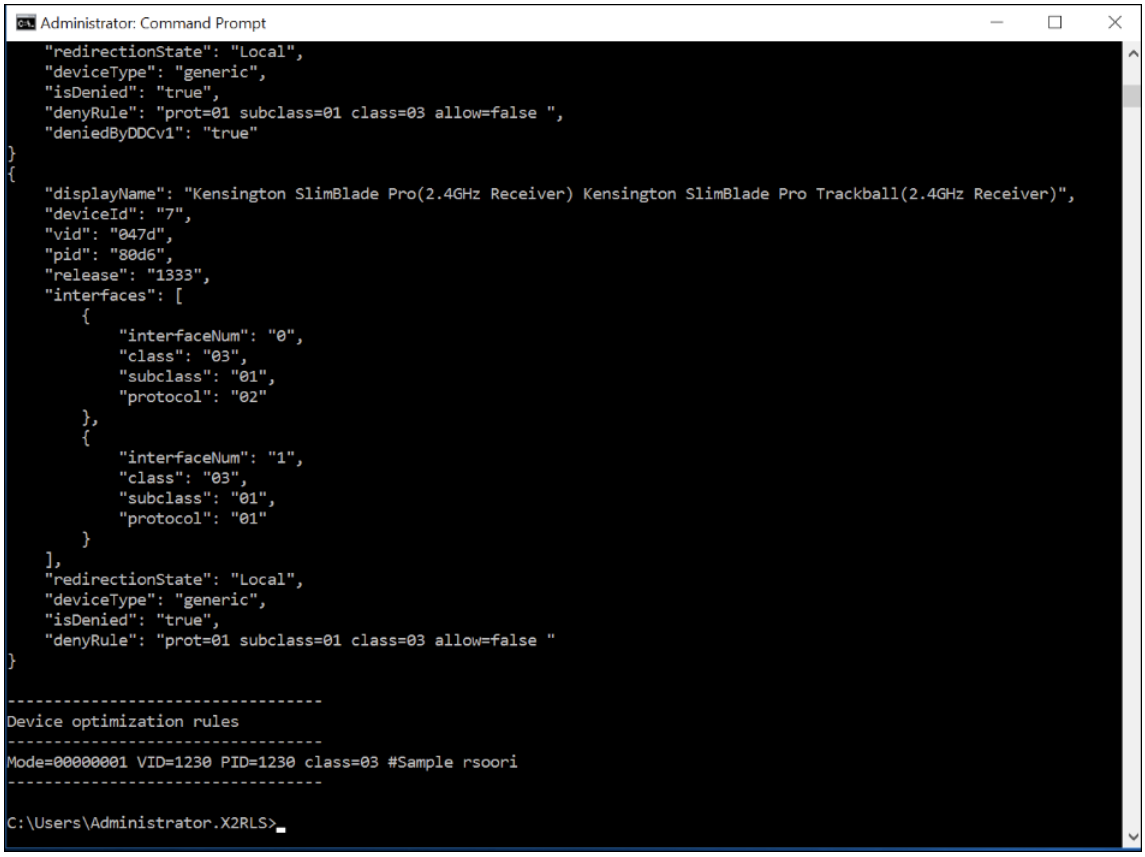
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Client Default Device Rules**
  - This section lists the rules that are set in the registry on the client.



- **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
subclass	Subclass Code

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tag Name	Description
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

September 6, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 setting.
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 appropriate device rules on the Studio console:

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** policy setting.
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`

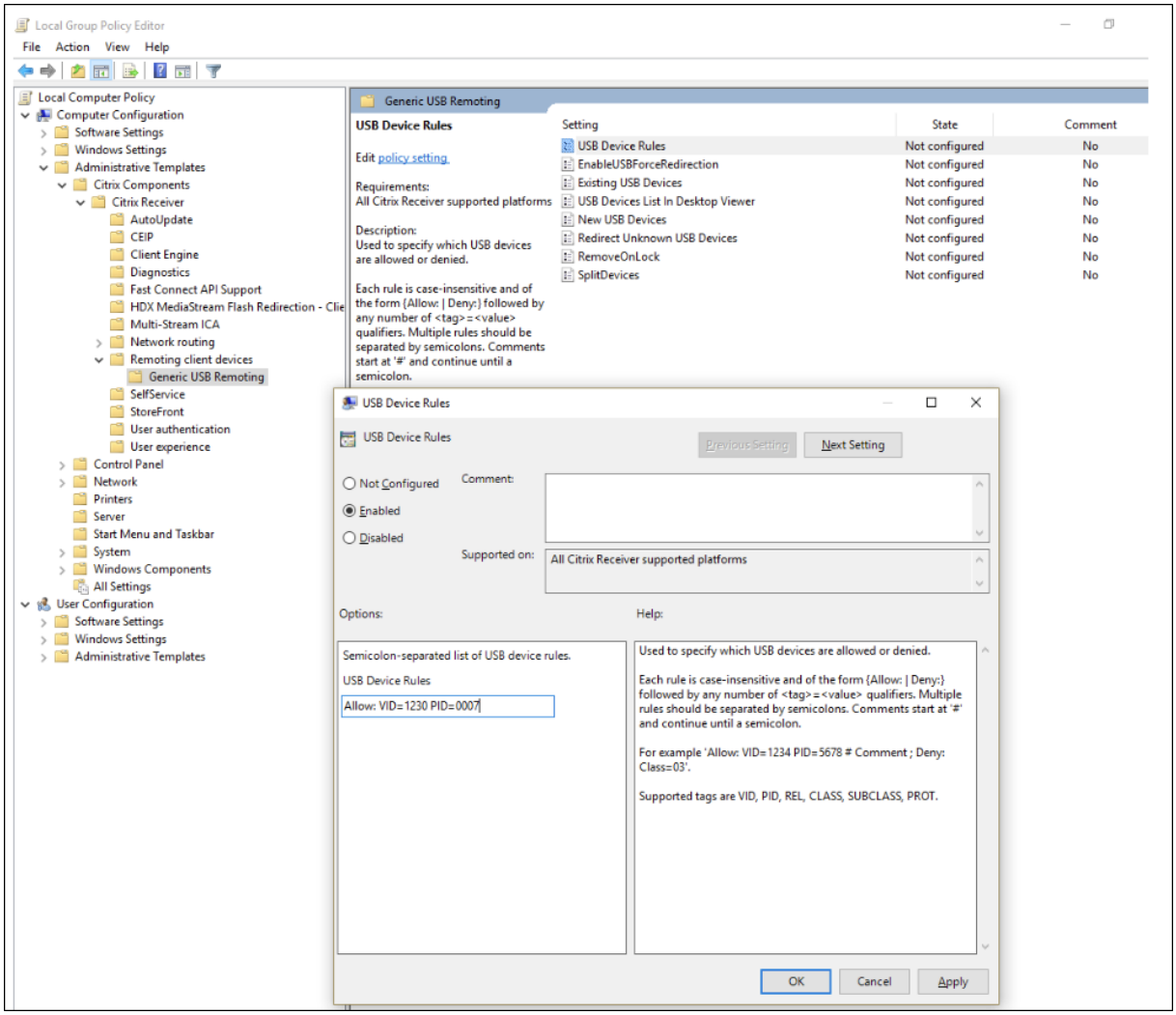
Setting appropriate GPOs on the client:

1. Open the **Local Group Policy Editor** and go to **Administrative Templates > Citrix Components > Citrix Receiver™ > Remoting client devices > Generic USB Remoting**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Open the **USB Device Rules** setting and set it to **Enabled**. 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.

> **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

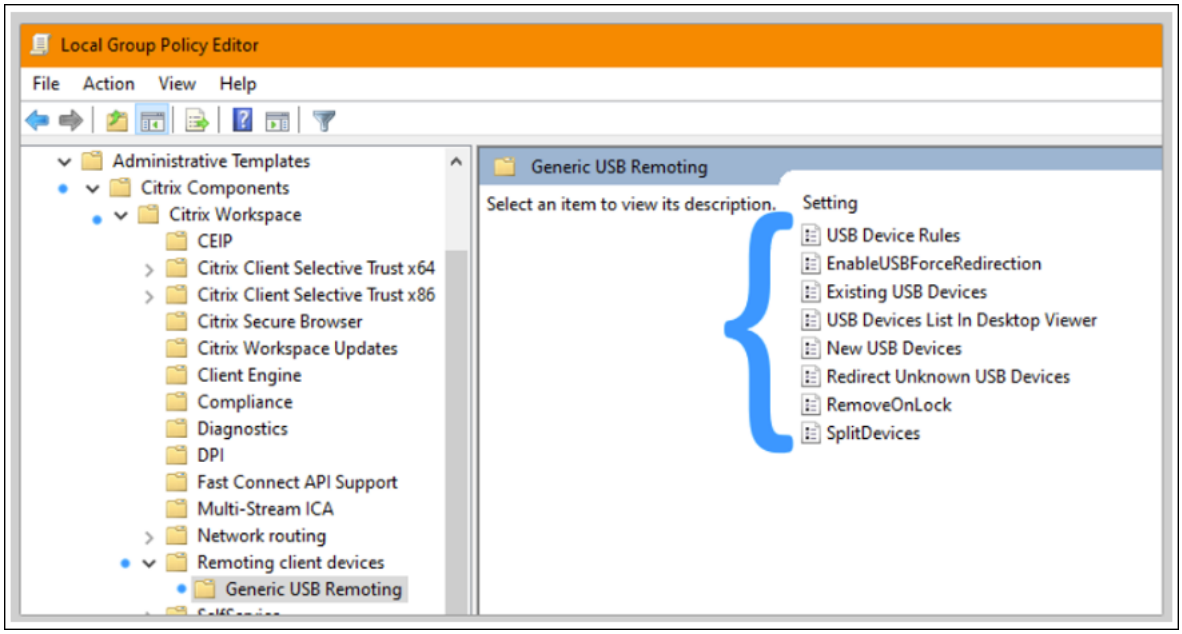
Configure automatic redirection of USB devices

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 automatically redirected. To prevent USB devices from being listed or redirected, use DeviceRules policy setting on the client endpoint.

This policy can be set on the client using a GPO, client side registry, using Citrix Workspace™ Preferences or the Connections tab under CDViewer. All of these methods are described below:

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**.



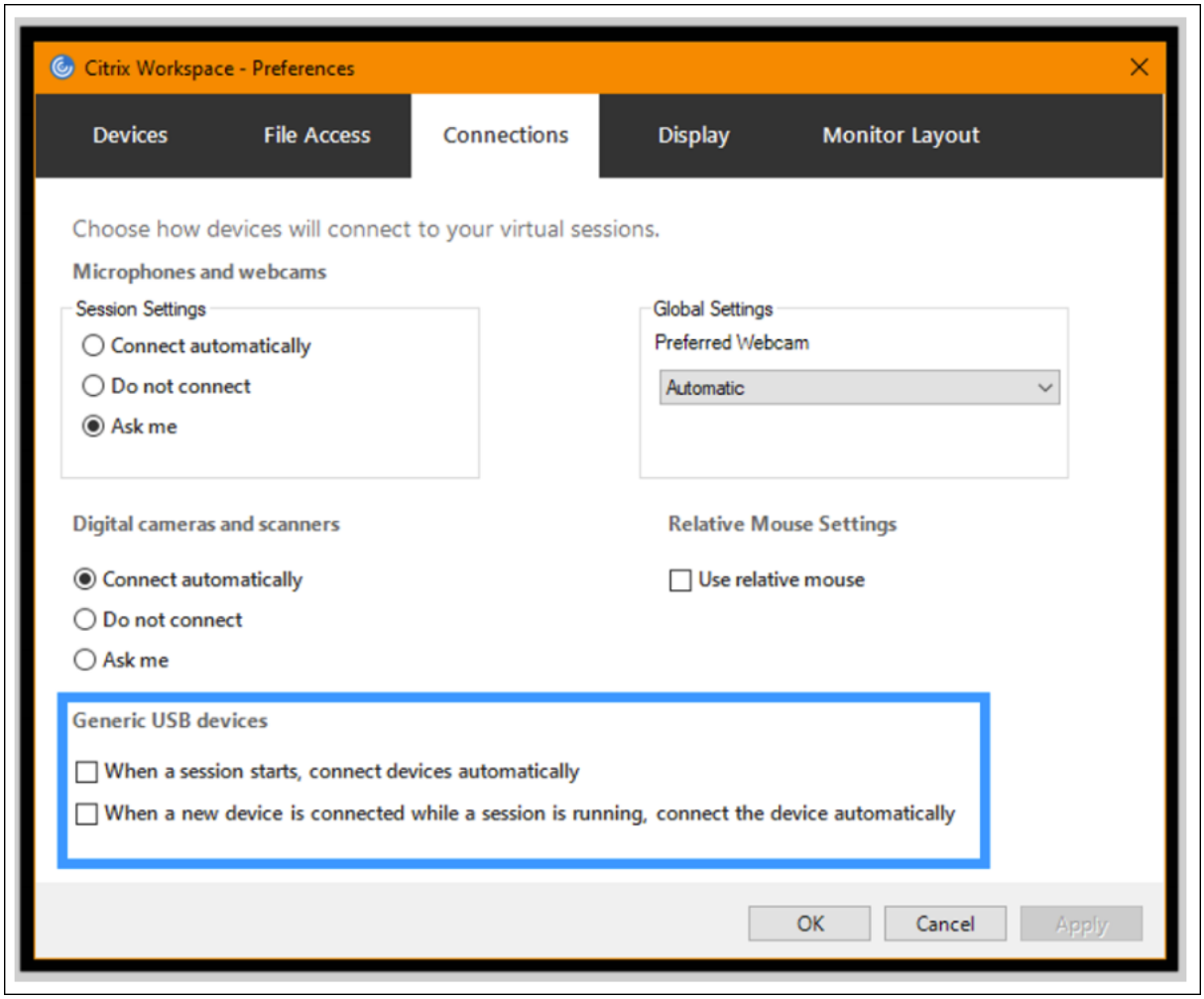
Using Citrix Connection Center:

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



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.

Configuring two or more devices using USB redirection with different device rules

Multiple devices can be redirected inside the HDX™ session with different device rules. An admin may want to redirect one device automatically while providing an option to the end user to redirect the other device. The following are the steps to configure two devices with different rules.

1. Enable the **Client USB device redirection** policy setting in **Citrix Web Studio**.
2. Edit the **USB device rules** setting in client side GPO.
    a) Open the **Local Group Policy Editor** and go to **Administrative Templates > Citrix Components > Citrix Receiver > Remoting client devices > Generic USB Remoting**.
    b) Open the **USB Device Rules setting** and enable the setting. Add the USB Device rule as in this example, The **Allow: VID=0911 PID=0c1c** rule allows the device with **Vendor ID 0911** and **Product ID 0c1c** but it will not be automatically redirected. The **Connect: VID=06A8 PID=0043** rule will automatically redirect the device with **Vendor ID 06A8** and **Product ID 0043** provided the the automatic redirection policies mentioned in step 3 are set.
    c) **Allow**: VID=0911 PID=0c1c #Phillips speech mic.
    d) **Connect**: VID=06A8 PID=0043 class=03 # Topaz HSB signature pad
3. Open **Local Group Policy Editor** and go to **Administrative Templates > Citrix Components > Citrix Receiver > Remoting client devices > Generic USB Remoting**.
4. Open **New USB Devices**, select **Enabled**, and click **OK**.
5. Open **Existing USB Devices**, select **Enabled**, and click **OK**.

Once these settings are configured, the Topaz signature pad will be automatically redirected inside the HDX session and additional end user action will be required (Select Redirect option in Connection center or CD Viewer Devices tab) to redirect the Phillips speech mic in the session.

> **Note:**
>
> The above settings in step 2 and 3 could be applied directly in the client side registry value **DeviceRules** under the GenericUSB key (HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB) but that is not the recommended way.

Generic USB redirection and client drive considerations

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- The USB device only has a Windows driver available. For example, a smart card reader might not have a driver available for the Citrix Workspace™ app for Android.
- The version of the 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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

settings. For more information, see Bandwidth policy settings for Client USB device redirection, and Multi-stream connection policy settings.

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, see Communication between client and VDA.
>
> 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.

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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> USB redirection is supported over lower bandwidth connections, for example 50 Kbps. However, copying large files doesn't work.

Client Drive Mapping (CDM)

September 13, 2025

Client Drive Mapping makes storage drives on the client endpoint available inside a Citrix HDX™ session to allow files and folders to be transferred from the client to the session host, and vice versa. This feature is enabled by default with both read and write privileges. To prevent users from adding or changing files and folders on mapped client-devices, enable the **Read-only client drive access** policy setting. When adding this setting to a policy, ensure that the **Client drive redirection** setting is set to **Allowed** and is also added to the policy.

As a security precaution, endpoint drives are mapped without the run permission by default. To allow users to run executables directly from the mapped client drives, edit the **ExecuteFromMappedDrive** registry value in the session host. For details, see Mapped client drives in the **HDX features managed through the registry** section.

Requirements

The following are the requirements for using CDM:

Citrix Control plane

- Citrix Virtual Apps and Desktops™ 1912 or later
- Citrix DaaS™

Session host

- Operating system
  - Windows 10 1809 or later
  - Windows Server 2016 or later
  - Linux: Please refer to the Linux VDA system requirements
- VDA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows: Citrix Virtual Apps and Desktops 1912 or later
- Linux: Please refer to the Linux VDA documentation

Client device

- Operating system
  - Windows 10 1809 or later
  - Linux: Please refer to the Workspace app for Linux system requirements

Related Policies

Please refer to Policy settings reference section for CDM settings.

Double-hop scenarios

CDM is supported in double-hop scenarios. By default, the client endpoint's drive is mapped to the second hop session and the first hop's drives are not available. However, this can be set so that the first hop's drives are mapped in the second hop's session instead of the client endpoint's drives.

To configure this functionality, edit the following registry value:

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced
- Value name: NativeDriveMapping
- Value type: REG_SZ
- Value data:
  - True - Maps the drives of the first hop session in the second hop session
  - False - Maps the drives of the client endpoint in the second hop session

> **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 the Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Support for mobile and touch screen client devices

September 13, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 1912 or later
- Citrix DaaS™

Session host

- Operating system
  - Windows 10 1903 or later
  - Windows 11 21H2 or later
- VDA
  - Windows: Citrix Virtual Apps and Desktops version 7.15 or later

Client device

- Operating system
  - Windows 10 1809 or later
  - Windows 11 21H2 or later
- Citrix Workspace™ app for Windows version 1808 or later

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

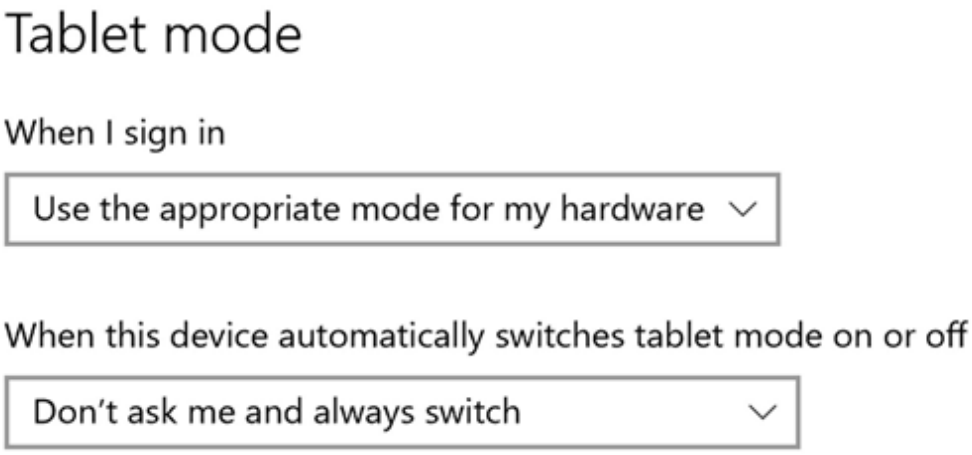
XenServer (formerly Citrix Hypervisor™)

- 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
  - Windows 11 21H2 or later
- 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Slightly larger buttons.
- The Start screen and any apps you start open in a full screen.
- 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 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:

Citrix control plane

- Citrix Virtual Apps and Desktops 1903 or later
- Citrix DaaS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session host

- Operating system
  - Windows 10 1809 or later
  - Windows 11 21H2 or later
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1903 or later

Client device

- Operating system
  - Windows 10 1809 or later
  - Windows 11 21H2 or later
- Citrix Workspace app for Windows version 1902 or later

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Due to OS limitations in Windows server 2k22, users will not be able to set pen shortcuts or make adjustmentes to pen/ink settings in 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.

Serial ports

September 6, 2025

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.

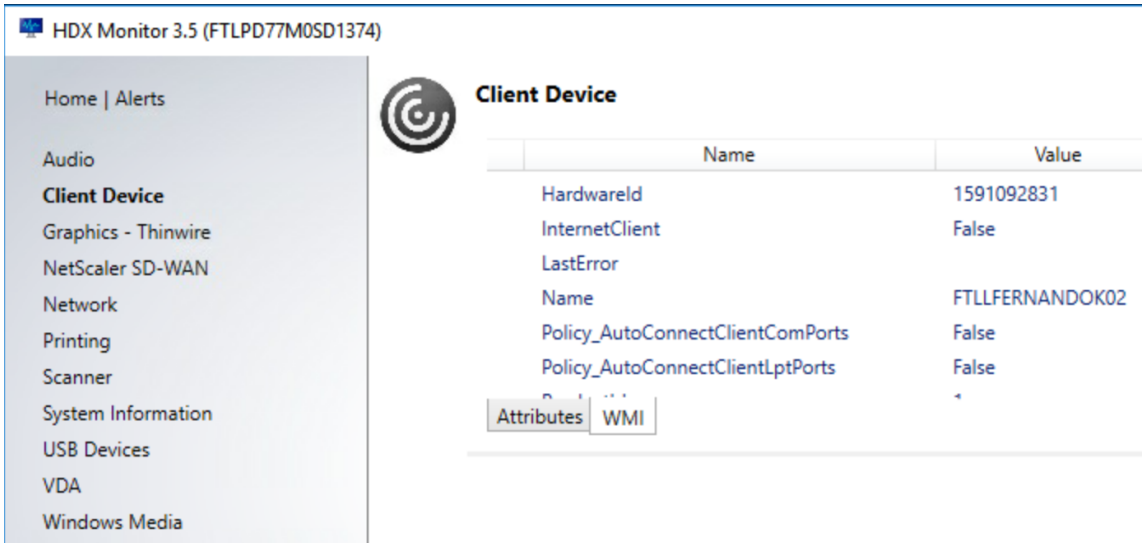
Map a client COM port to a server COM port

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



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.

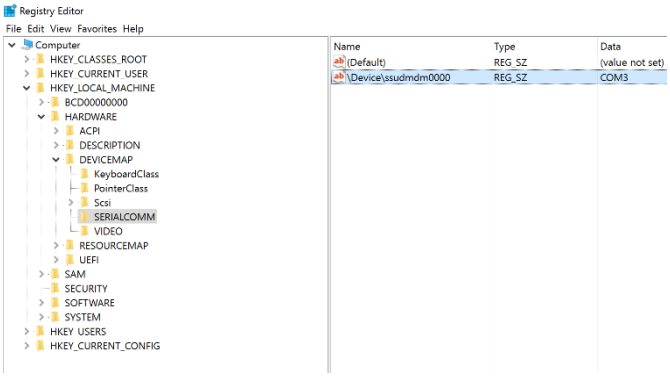
3. To use this COM port in a virtual desktop or application, install your user device application and point it to the mapped COM port name. For example, if you map COM1 on the client to COM3 on the server, install your COM port device application in the VDA and point it to COM3 during the session. Use 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.

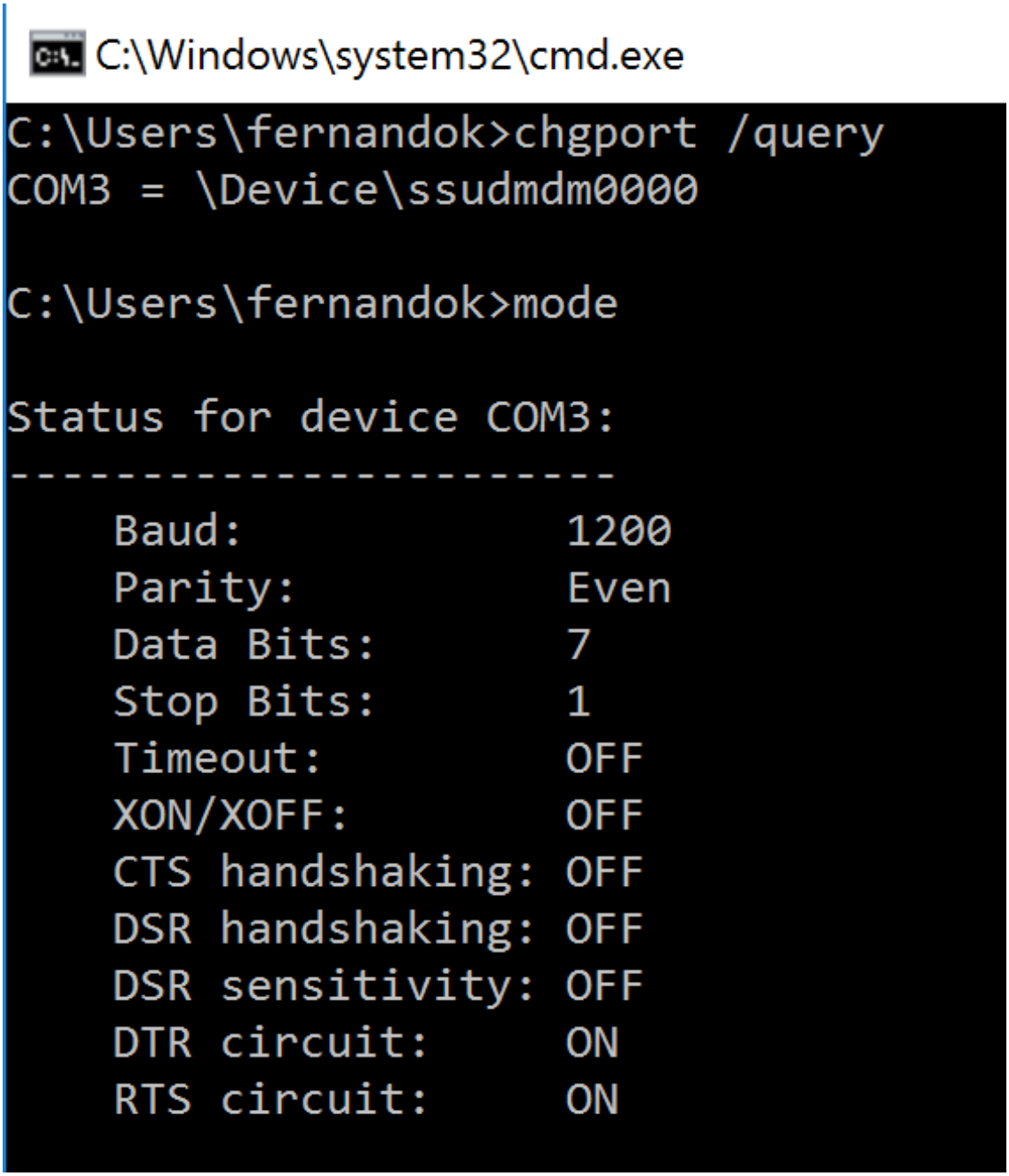
Troubleshoot

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:



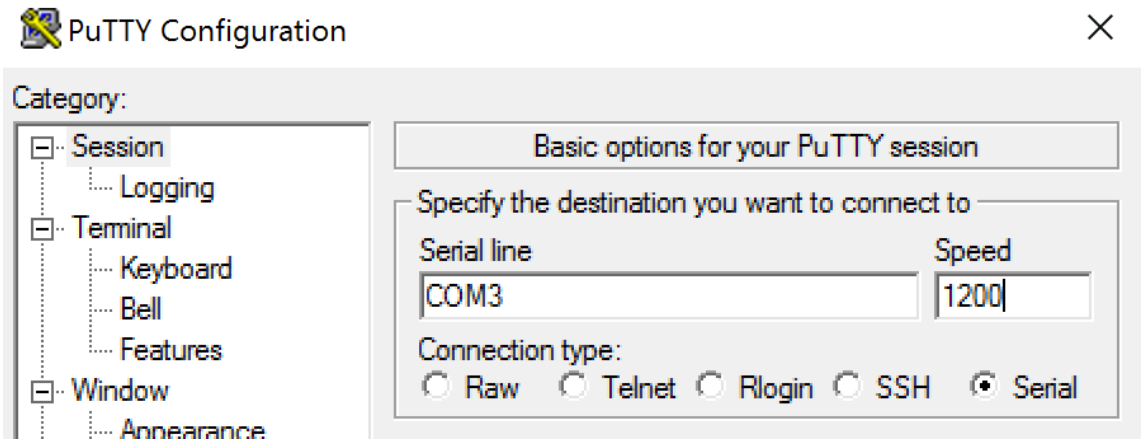
   You can also find this information from the command prompt by running **chgport /query**.

© 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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\>`
- 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

September 6, 2025

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™ supports the Bloomberg model 5, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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).

The Bloomberg keyboard is a USB composite device comprising multiple 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 2207 for Linux to support Bloomberg keyboard model 5.
- Minimum of Citrix Workspace app 2109 for Windows to support Bloomberg keyboard model 5.
- 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:

For Bloomberg 5 keyboard:

- Bloomberg LP Bloomberg Biometric Module
- Bloomberg LP Keyboard (Composite device with two interfaces)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Bloomberg LP Keyboard Audio (Composite device with three interfaces)

For Bloomberg 3 and 4 keyboards:

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

Seamless Application only scenario:

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.

Support key event sequence processing in Windows VDA for double hop

September 6, 2025

This feature ensures that the key events are sent sequentially in the Windows Virtual Desktop Agent (VDA) when the client device is non-Windows and operates in Unicode mode. It addresses specific input-related issues, including

1. Double-hop scenarios with RDP as the second hop.
    - When using a German keyboard layout, holding the **AltGr** key and pressing **q** should produce **@** as the output. However, without this feature, the actual output is **q**.
2. Key shortcut functionality
    - The **Alt+Tab** shortcut may not function consistently in Windows VDA when using Citrix Workspace™ App (CWA) for Android.

By enabling this feature, these input inconsistencies are resolved. This ensures accurate key event handling and improved usability.

The feature is disbled by default. The toggle of this feature is `EnableSendUnicodeKeyQueue` in registry setting.

A new registry `HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd\EnableSendUnicodeKeyQueue` DWORD = 0/1 is used to to switch to the new implementation if the value is 1.

By default, the value is 0.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Set the above registry key in the 1st hop Windows VDA for double hop use scenarios.

Windows - Keyboard & IME Supportability Tool

September 6, 2025

This is a self-service command line tool which can diagnose relevant problems to the keyboard and Input Method Editor.

In order to meet a variety of user requirements, provide platform versatility, and provide users with personalized needs, the functions of the keyboard and Input Method Editor (IME) rely on different configurations and capabilities in VDAs and Citrix Workspace™ apps.

An incorrect setting in VDA or client side might result in unexpected input behaviors.

However, Citrix® provides the recommended settings for some common usage scenarios, and these recommendations are also included in the diagnose results.

With this tool, below categories of issues can be identified:

- **Keyboard type inconsistency:** will check VDA keyboard type and client keyboard type to confirm if there is inconsistency. For example, VDA is using 101 English keyboards, but the client is using a Japanese 106 keyboard. This diagnostic is targeted for JP 106/109 keyboard, and KO 103/106 keyboard use cases.
- **Keyboard layout sync mode inconsistency:** will check the keyboard layout sync settings, registry settings, group policies, and sort out problems in sync mode configurations in a given environment.
- **Client keyboard layout and VDA keyboard layout inconsistency:** will check if the client keyboard layout is the same as VDA keyboard layout
- **Remote Language Bar is now showing for application sessions:** will check if the remote language bar is showing when end users launch an application session and are using more than 1 keyboard layout.

This command line tool is hosted in Windows VDA - `CtxKbImeDiagnostics.exe`.
The command line interfaces are as below:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Interface	Description	Note
`CtxKbimeDiagnostics`	show diagnostic result only for current ICA® session	If the user has admin privilege, it shows diagnostic for all active ICA sessions. If the user has no admin privilege, it shows diagnostic for current users'ICA sessions
`CtxKbimeDiagnostics [-v]`	show setting information and diagnostic result for the current session	If the user has admin privilege, it shows diagnostic for all active ICA sessions
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	show setting information and diagnostic result for this session	
`CtxKbimeDiagnostics [-s Session_Id]`	specific a session and show the respective diagnostic result for this session	Admin Privilege can query other ICA sessions/Normal user can only query their own ICA sessions
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	specific a session and show all setting information and diagnostic result for this session	Admin Privilege can query other ICA sessions. Normal user can only query their own ICA sessions
`CtxKbimeDiagnostics [-h]`	show supported args/parameters and example	"help"interface
`CtxKbimeDiagnostics [-V]`	show current tool version	

> **Note:**
>
> In this version, only CWA Windows as a client is supported.

Webcams

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Graphics

September 13, 2025

Citrix HDX graphics include an extensive set of graphics acceleration and encoding technologies that optimizes the delivery of rich graphics applications from Citrix Virtual Apps and Desktops. 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 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. Graphics are generated as a result of user input, for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

example, keystrokes or mouse actions.

HDX 3D Pro

The HDX 3D Pro capabilities in 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.

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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the entire session screen without changing the content of the original document. Text-based session watermarks require VDA support.

Adaptive Refresh Rate

With the new scalability improvements, HDX matches the refresh rate of virtual monitors to match the target FPS policy set. Adaptive Refresh Rate (ARR) is available for both single and multisession VDAs, and works for both GPU-accelerated and non-GPU scenarios.

loss tolerant mode

The loss tolerant mode is thoroughly reworked to ensure the session remains interactive when packet loss is detected.

Related information

- HDX 3D Pro
- GPU acceleration for Windows Single-session OS
- GPU acceleration for Windows Multi-session OS
- Framehawk
- Thinwire
- Text-based session watermark

An introduction to Thinwire

September 6, 2025

HDX™ Graphics, powered by Thinwire, is Citrix's advanced display technology that delivers high-performance, adaptive, and efficient remote desktop and application experiences.

Thinwire ensures optimal performance across diverse network conditions and endpoint devices by intelligently analyzing, caching and compressing graphical data.

HDX™ 3D Pro

September 13, 2025

HDX 3D Pro, now known as HDX Graphics, delivers a high-performance user experience for demanding graphical workloads. By default, it leverages GPUs to provide hardware acceleration for both DirectX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

and OpenGL applications. This functionality, previously associated with HDX 3D Pro, is now available out of the box for all users without requiring any additional policies or configuration.

Using hardware acceleration, you can provide users with a seamless and responsive experience for even the most graphically intensive applications, including those used in fields like design, engineering, and multimedia production.

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.

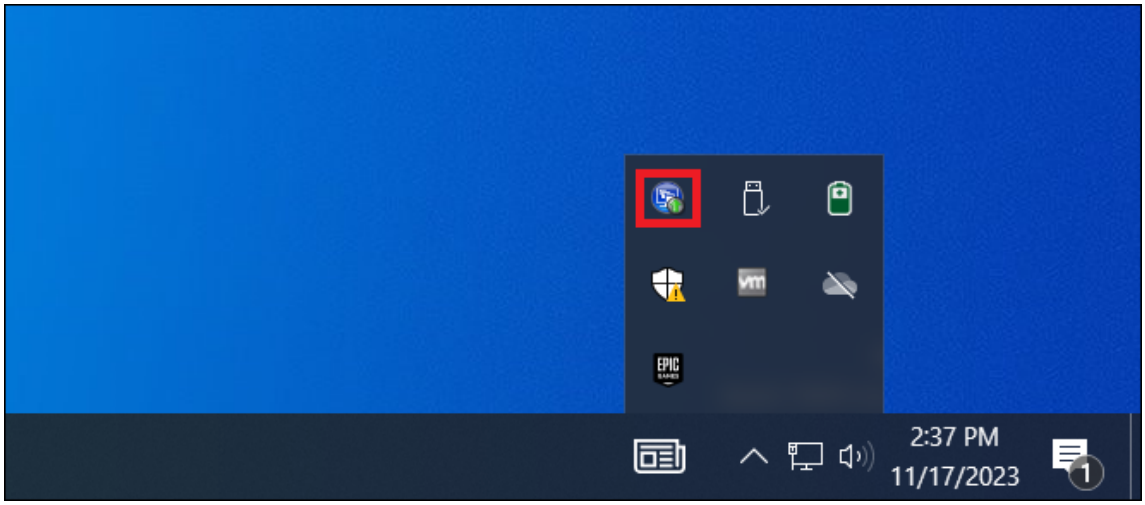
Lossless compression option for specialized use cases

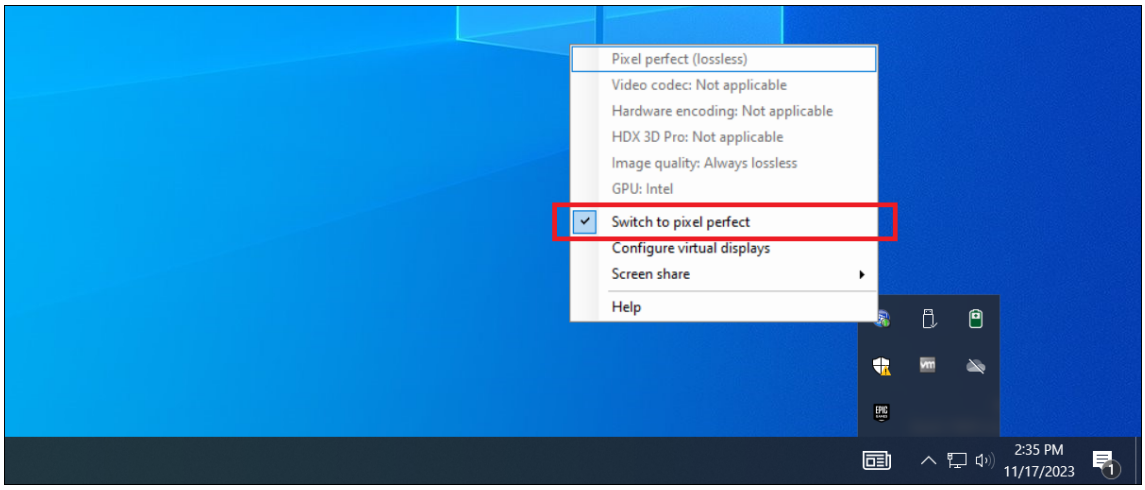
HDX 3D Pro also offers a CPU-based lossless codec to support applications where pixel-perfect graphics are required, such as medical imaging. True lossless compression is recommended only for specialized use cases because it consumes more network and processing resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When using lossless compression:

- The lossless indicator in the Graphic Status 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 the **Always Lossless** mode anytime within the session. To select or clear **Lossless** 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure a new registry setting at `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`.

- Name: HKEY_LOCAL_MACHINE_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
  For Ctrl + Shift + F5, set A=1, S=1, K=0x74

Optimize the HDX 3D Pro user experience

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 throughout 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.

Use the HDX Monitor tool to validate the operation and configuration of HDX visualization technologies and to diagnose and troubleshoot HDX issues. The tool is available in the **Support** folder on the Citrix Virtual Apps and Desktops installation media.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GPU Acceleration

September 6, 2025

HDX™ Graphics seamlessly leverages GPU hardware on both the Virtual Delivery Agent (VDA) and endpoint devices.

This out-of-the-box hardware acceleration, previously known as HDX 3D Pro, is enabled by default and significantly boosts performance for graphically demanding DirectX and OpenGL applications, both in single and multi-session operating systems.

Citrix Virtual Apps and Desktops™ support 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, the server's CPU can be used more efficiently.

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 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.

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.
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

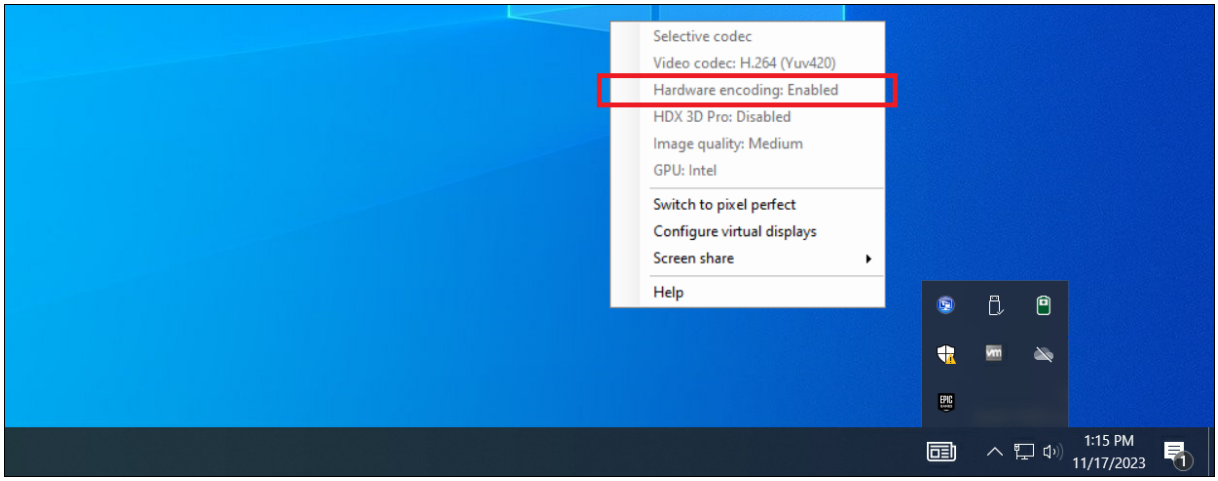
Scalability using GPU Sharing depends on several factors:

- 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.

- 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 falls back to CPU-based encoding using the software video codec. For more information, see Graphics policy settings.

To confirm that GPU acceleration is occurring, the Graphics Status Indicator can be used:



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.

- On Windows Server 2016 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 2016 and later, enable the **Use the hardware default graphics adapter for all Remote Desktop Services sessions** setting in the group policy **Local Computer**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 features, enable the registry settings. For information, see GPU acceleration for CUDA or OpenCL applications in the list of features managed through the registry.

10-Bit High Dynamic Range (HDR)

September 6, 2025

With 10-bit High Dynamic Range (HDR) virtual desktop sessions, you can use enhanced encoding and decoding capabilities to render high-quality images and videos with an extended range of colors, and greater contrast and brightness.

System requirements

Endpoint:

- Citrix Workspace™ app for Windows 2209 or later for NVIDIA GPUs
- NVIDIA GPUs with 10-bit HEVC (H.265) 444 decoding support on the endpoint
- 10-bit HDR-supported monitors, 10-bit HDR must be enabled on all monitors using display settings.

Server:

- Windows single-session OS VDA 2209 or later for NVIDIA GPUs, and VDA 2308 or later for Intel GPUs
- NVIDIA GPUs with 10-bit HEVC 444 encoding support on the VDA

Required policies

Endpoint:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enable H.265 decoding for graphics

Server:

- Optimize for 3D Graphics workload
- Graphics Status Indicator (optional)

Server configurations

Launching a Citrix® session on a 10-bit HDR-enabled endpoint monitor enables the HDR session by default. In multi-monitor HDR sessions, all endpoint monitors must have 10-bit HDR enabled. HDR sessions are supported in both windowed and full-screen modes.

Reference White Level

This setting defines the white luminance level by nit value. It controls the relative HDR screen brightness within the session. The default value is 80 nits. Set the following registry key to define a different nit value:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Type: REG_DWORD
- Name: RefWhiteLevel

To activate the setting, you must either resize your session or disconnect and relaunch the session.

EDID override

You can configure the VDA to use the endpoint monitor EDID for your HDR sessions. This allows you to fully utilize the monitor's display capabilities by matching the color gamut and luminance range. By default, HDR sessions assume an HDR1000-capable display.
You can export endpoint monitor EDID using NVIDIA or other tools. Apply it to the VDA using the following registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Type: REG_BINARY
- Name: EDIDOverride

When you store the EDID in the registry, it must not have commas, spaces, or special characters. To activate the override EDID, sign out and launch a new session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Visual lossless experience

Enable the following policies for a visually lossless experience:

- Allow Visual Lossless Compression
- Visual Quality: Always Lossless or Build to Lossless

After the policies are set, you can control the HDR session quality using the Graphics Status Indicator by using the Image Quality Slider, or by switching to pixel-perfect mode.

Allow Windows screen lock

You can use this policy to allow all Windows display timeouts, including screen lock, to apply to a Citrix Virtual Desktop session on Workstation OS. This setting can be set using a Citrix Group Policy Object in Citrix Studio.

By default, when this setting is not enabled, a Citrix Virtual Desktop does not respond to timeouts for session lock, screensaver, or display off, during an active session.

When a password-protected screensaver is configured on a Workstation VDA, this setting must be enabled to allow the Citrix Virtual Desktop session to be automatically locked when the screen saver timeout is reached.

Enabling this setting when a display-off timeout is configured on the VDA causes the expiration of that timeout to result in a session that does not update until the user resumes interaction with the session. For instance, any time displayed is not updated, and new notifications are not displayed.

Other considerations

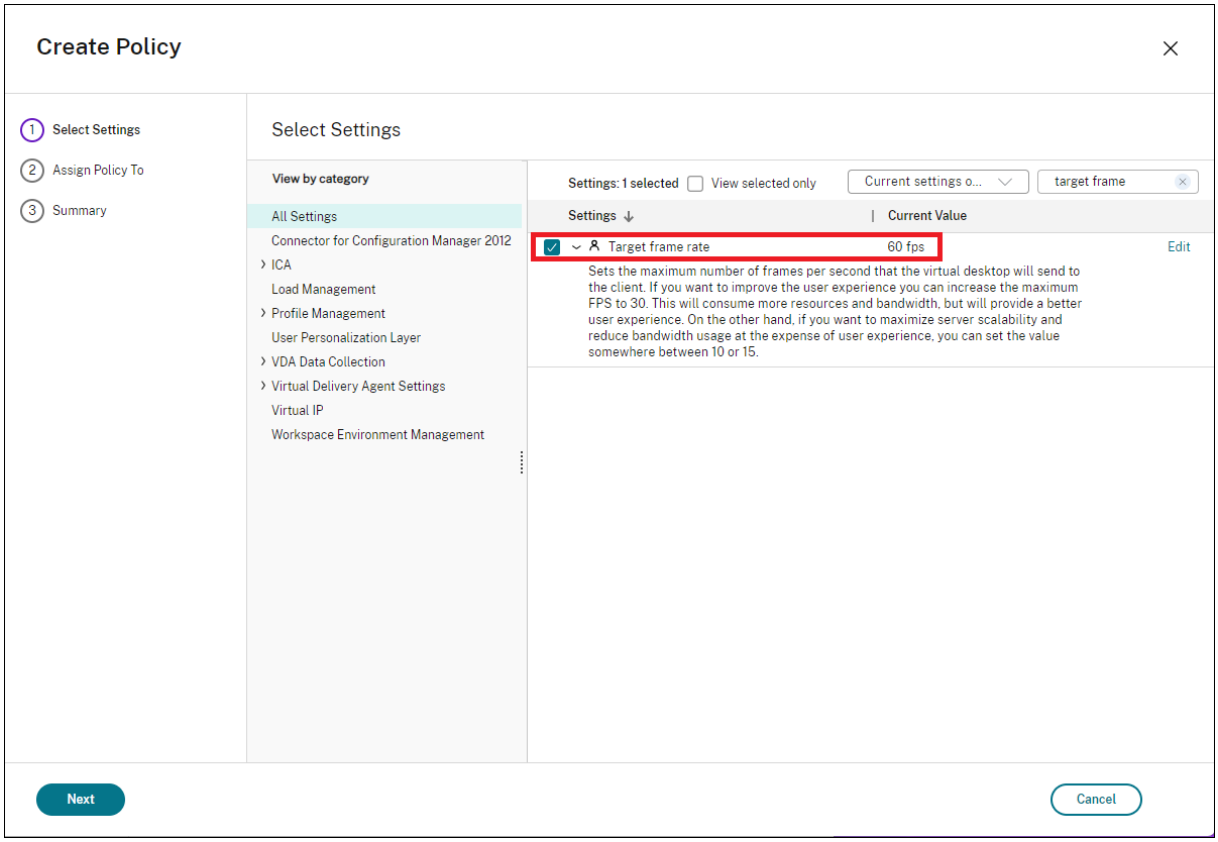
- You can launch 10-bit HDR sessions on up to four monitors on virtual GPUs.
- The Citrix session reverts to an 8-bit, non-HDR mode in the following instances:
    - If any endpoint monitors do not have 10-bit HDR enabled
    - Enabling screen sharing.
    - Setting a virtual display layout on the VDA.
    - Switching to pixel-perfect mode without setting the **Allow Visually Lossless Compression** policy.

Adaptive Refresh Rate

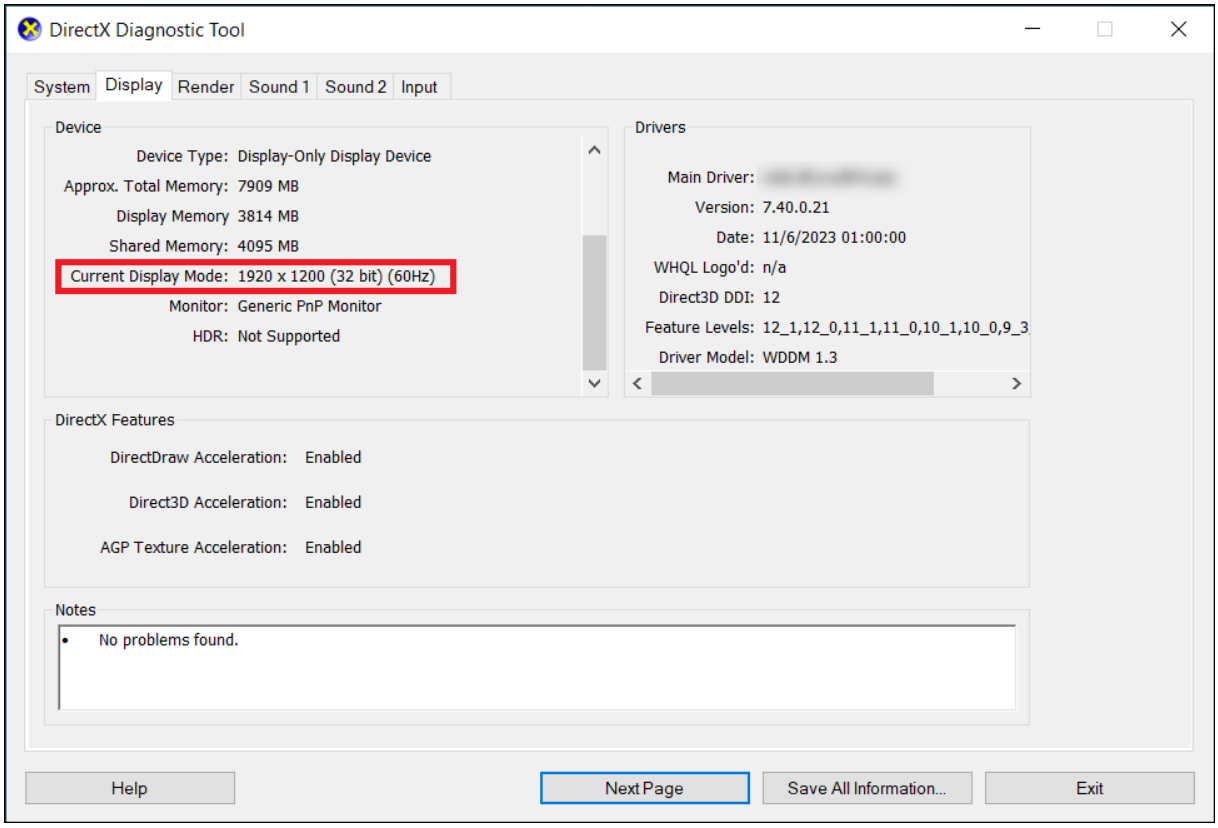
September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With Adaptive Refresh Rate, HDX™ matches the refresh rate of virtual monitors to match the target FPS policy set. Adaptive Refresh rate provides better performance and scalability for both single and multi-session VDAs.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note**
>
> Adaptive Refresh Rate is only available when Citrix Indirect Display or IDD is used (as per Citrix Virtual Apps and Desktops™ default) and is not available when using Vendor supplied Display Adapters.

Loss tolerant mode for graphics

September 6, 2025

Loss tolerant mode ensures the best performance and interactivity over unreliable networks.

When network conditions degrade beyond pre-defined bandwidth, latency, and packet loss thresholds, the Citrix® graphics encoder automatically switches into a more aggressive mode of packet delivery to overcome the effect of packet loss.

The loss tolerant mode for graphics is thoroughly reworked to ensure the session remains interactive when packet loss is detected. When network conditions degrade beyond pre-defined bandwidth, latency, and packet loss thresholds, the Citrix graphics encoder automatically switches into a more aggressive mode of packet delivery to overcome the effect of packet loss. As a result, bandwidth usage increases by an amount proportional to the amount of packet loss. If conditions later improve,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the Citrix graphics encoder seamlessly switches back. The thresholds can be configured via policy, with the defaults being 300 ms latency and 5% packet loss.

Citrix Workspace™ app for Windows 2311 is currently supported. Support for other platforms will be added in later Citrix Workspace app releases. As with previous versions of this feature, HDX™ Adaptive Transport (EDT) must be enabled for this feature to work. In addition, if connecting via the Citrix Gateway Service, loss tolerant mode for graphics must also be enabled on the Gateway.

HDX™ Screen sharing

September 6, 2025

HDX Screen Sharing is our native, high performance and low latency screen sharing technology. Screen sharing allows a user to share a Citrix Virtual Desktop session with others including screen contents, keyboard, and mouse controls.

System requirements

- Windows: Single-session or multi-session OS VDA
- Linux: See the Linux VDA documentation for more information on sharing Linux sessions.
- Only desktop sessions can be shared.
- There must be network connectivity between the VDA hosting the session and the machines connecting to the shared sessions. Network port requirements are based on ICA ports in use (TCP/UDP 1494 or 2598) and the Screen sharing policy configuration (TCP 52525 to 52625 by default).

Configuration

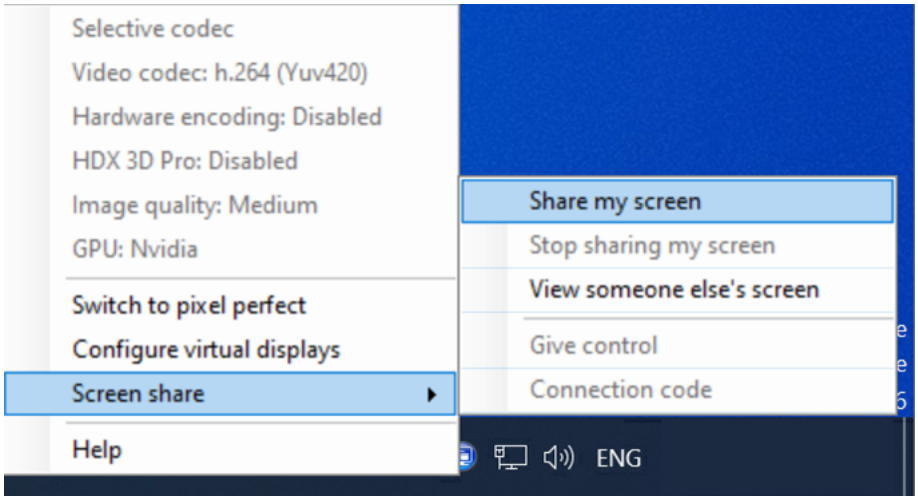
Screen sharing must be enabled using Citrix policies. Screen sharing is disabled by default. Configure the screen sharing policy to enable or disable the function and assign the usable network port range.

Enable the graphics status indicator policy to display the user interface that includes controls for sharing and connecting to sessions.

Sharing a session

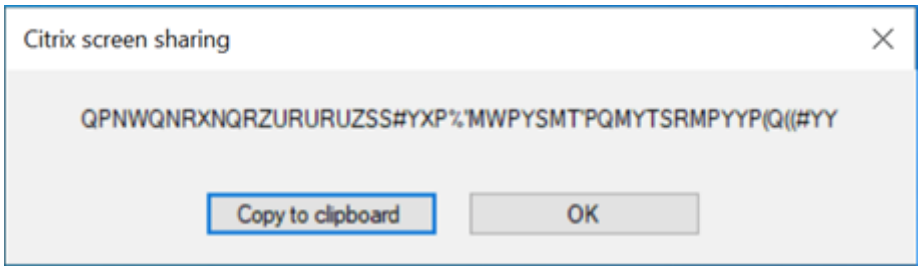
To share a session, look for the HDX graphics status indicator icon on the Windows notification area. Right-click on it to display the menu and select **Screen share > Share my screen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Copy to clipboard** or manually select and copy the entire string shown in the dialog box. The string can then be pasted into the application of choice, such as an email or IM client, to be distributed to other users.

Click **OK** or the **x** to close the dialog box. The connection code can be retrieved from the **Screen share > Connection code** menu option at any time while the session is shared.

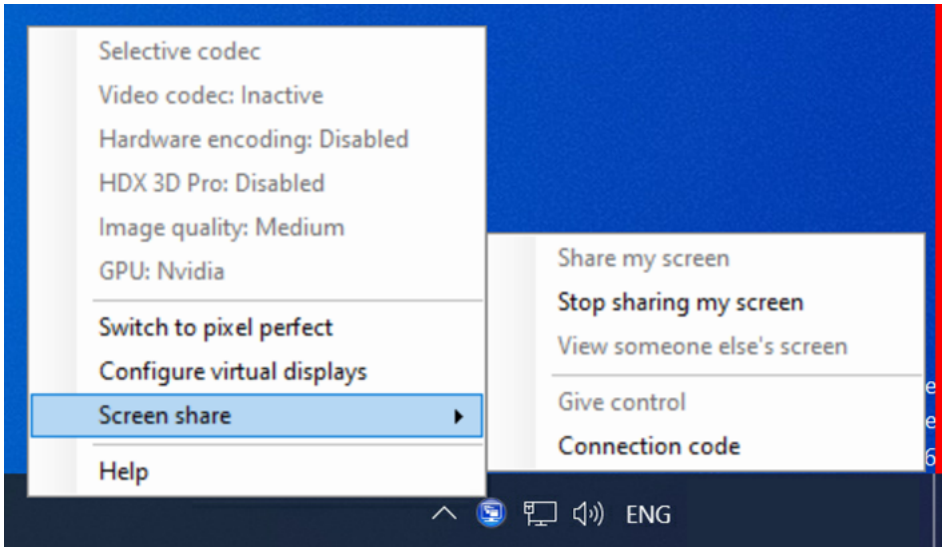


A red outline appears around the screen as an indicator that the session is now being shared and is visible by others.

Keyboard and mouse controls can also be shared with other users using the **Screen share > Give control** menu option.

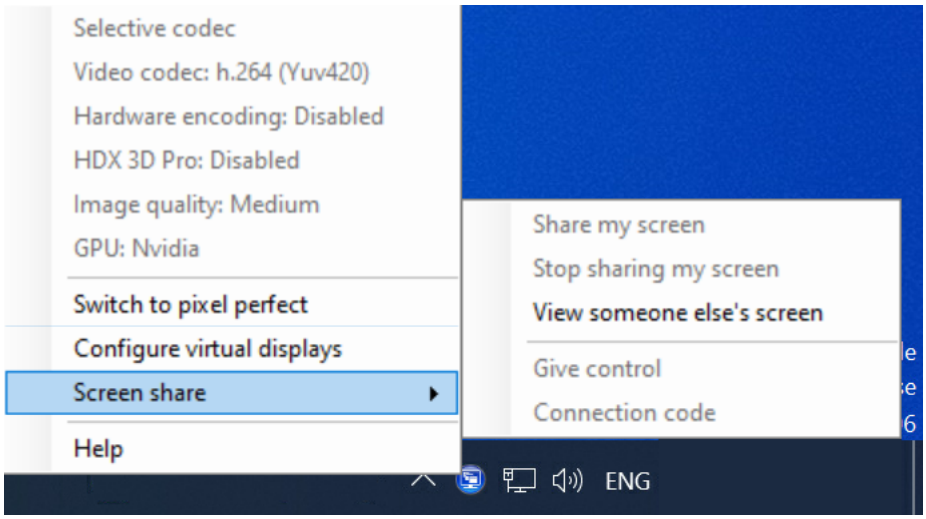
Use the **Screen share > Stop sharing my screen** menu option to stop sharing the session and disconnect all users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



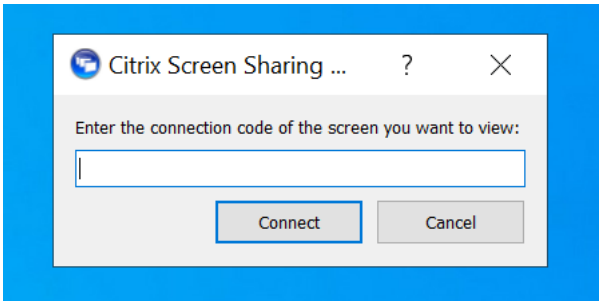
Connecting to a shared session

To connect to someone else's sessions, look for the HDX graphics status indicator icon on the Windows notification area. Right-click on it to display the menu and select **Screen share > View someone else's screen**.



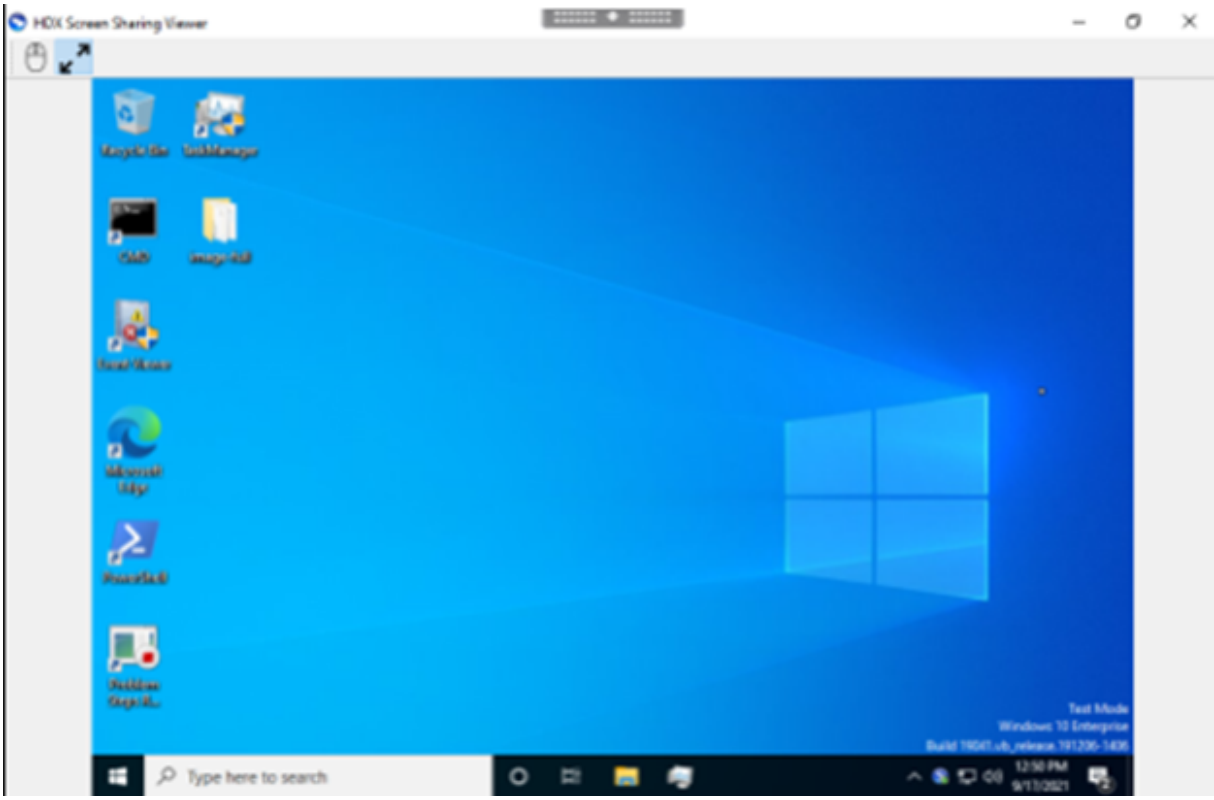
Enter or paste the connection string that was provided by the user sharing the session into the text box. Click **Connect** to establish the connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can request keyboard and mouse controls by clicking the mouse icon on the top left corner of the **HDX Screen Sharing Viewer** window.

Close the **HDX Screen sharing Viewer** window to disconnect from the shared session at any time.



Other considerations

- The screen sharing viewer application is included with the VDA in *C:\Program Files\Citrix\HDX\bin\TwPlayer.ex* and might be deployed as a published application using a Virtual Apps Server. This alternative deployment model allows collaboration with users that don't have access to a virtual desktop.
- The number of users allowed to connect to a shared session can be limited using the network port range in the screen sharing policy. One port is required per user. The default range allows 100 users at most.
- All monitors connected to the session are shared. You cannot select individual monitors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The H.265 video codec isn't supported.

Virtual display layout

September 6, 2025

The virtual display configuration lets you define a virtual display layout per session monitor on the VDA, inside a live session. This feature allows you to split each session monitor independently into multiple virtual monitors.

The virtual display configuration UI lets you define a virtual display layout per session monitor on the VDA, inside a live session. This feature allows you to split each session monitor independently into multiple virtual monitors. You can split into a total of 8 virtual monitors on the remote desktop. Also, you can update the session primary monitor and DPI settings for the displays.

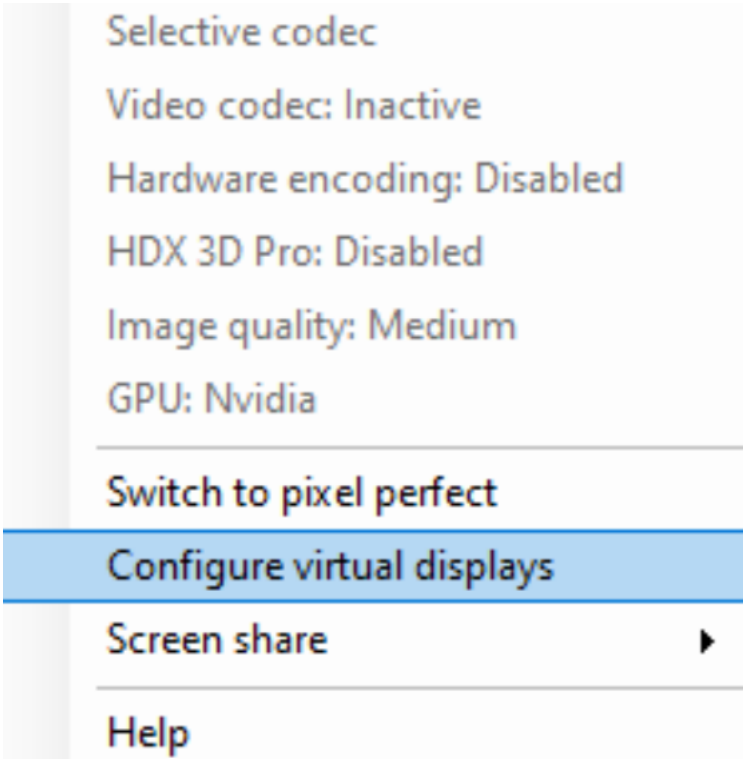
System requirements

- Windows: Single-session or multi-session OS VDA
- Graphics status indicator policy must be enabled
- Only desktop sessions can be configured.

Configuration

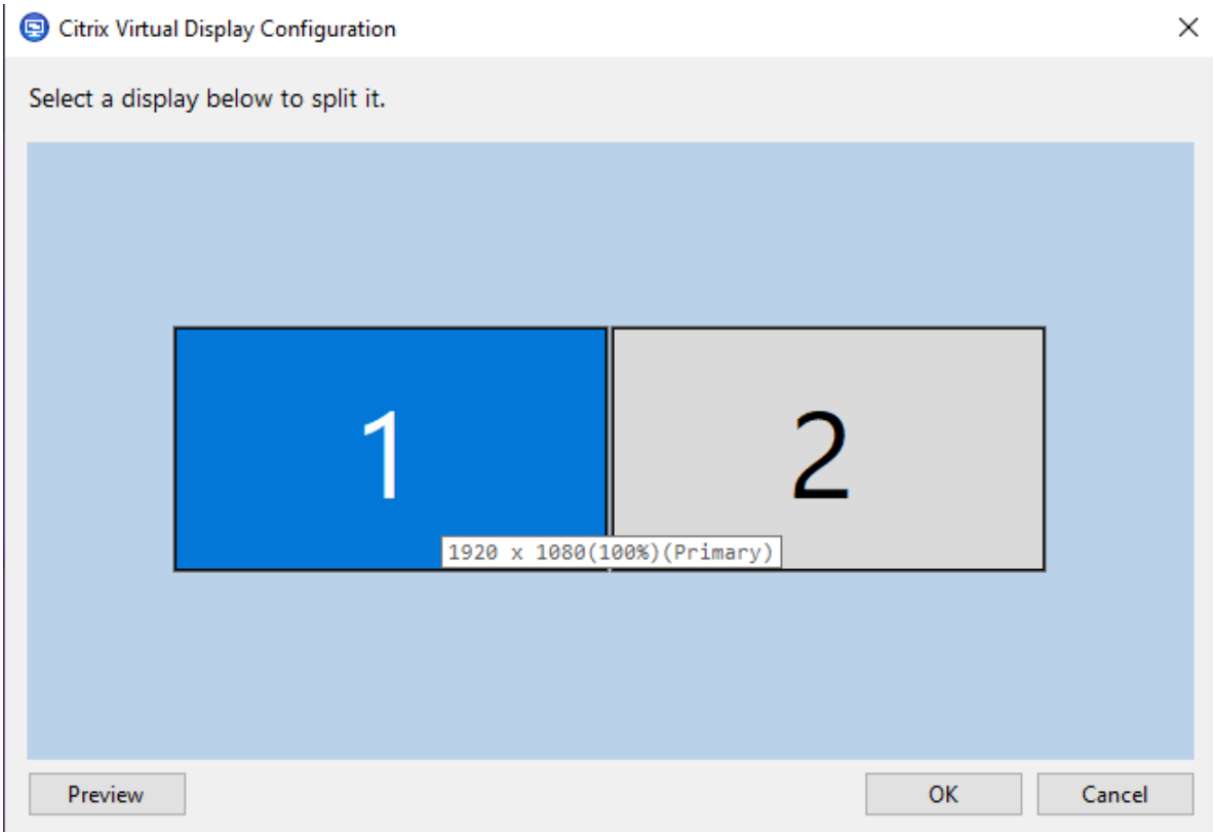
To configure the virtual display layout, right-click the graphics status indicator icon and select the Configure virtual displays option. The virtual display configuration UI is launched.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

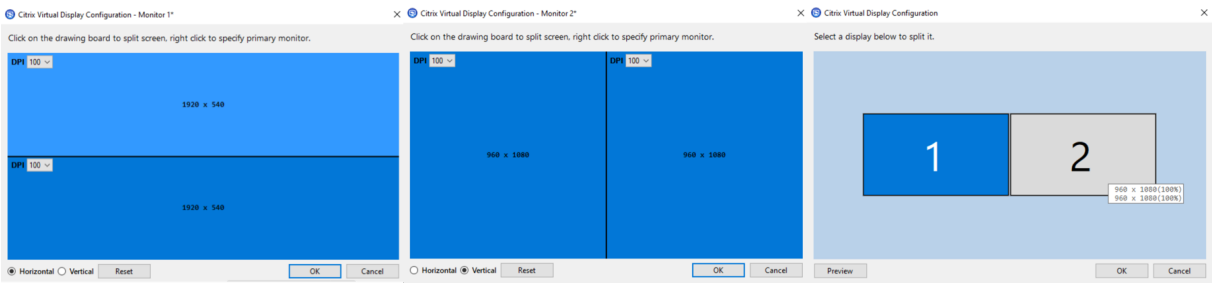


The UI shows the current session display layout, with blue denoting the session's primary monitor. You can see the Display settings tooltip when you hover on a display. The tooltip provides information about the current virtual display layout defined on a given session monitor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

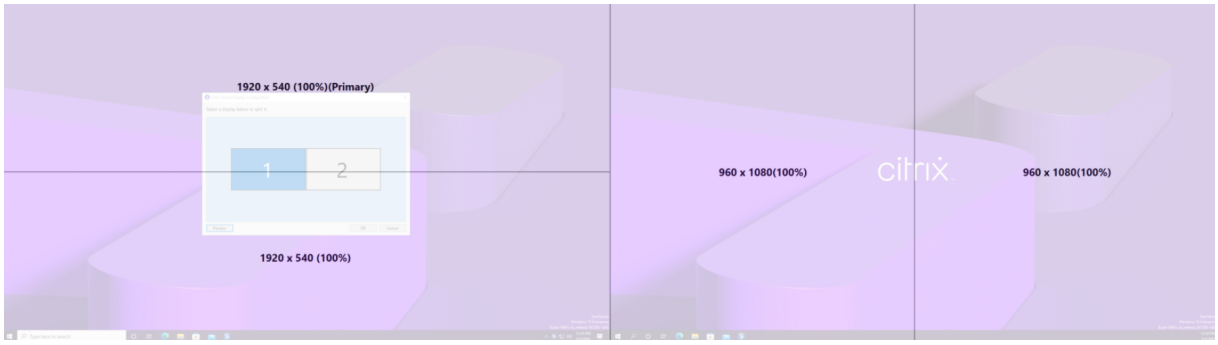


Select a display to transition to an interactive UI, which allows you to configure virtual displays for the selected session monitor. You can draw horizontal or vertical lines to separate the screen into virtual monitors. The screen is split according to specified percentages of the session monitor resolutions. Right-click on a virtual display to mark it as the primary monitor and use the DPI drop-down list to set a preferred scaling factor for the virtual display. After defining a virtual display layout, click **OK** to temporarily save the layout or **Cancel** to discard any changes. You can use **Reset** to undo the configuration and restore the original layout for the session monitor.

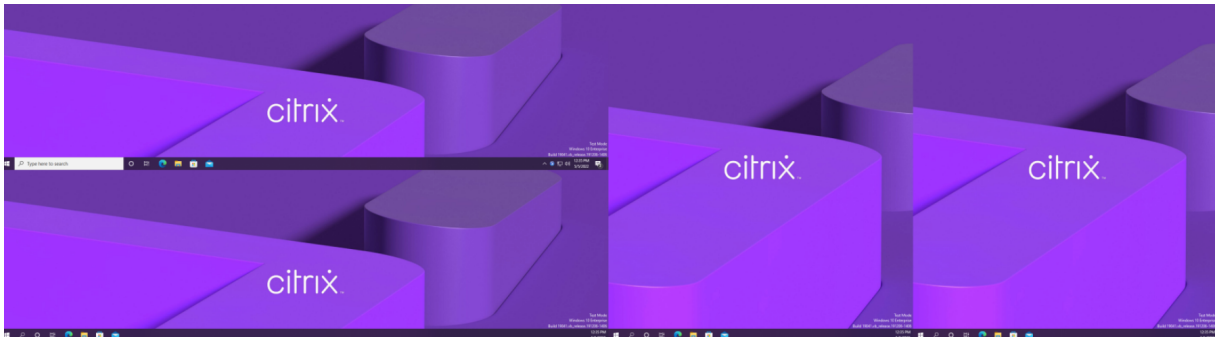


To preview the current configured virtual display layout, click the **Preview** button. A window appears to highlight the expected position and resolution of the virtual displays in the session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **OK** to immediately apply and save the virtual display layout. Click **Cancel** to close the UI and discard all changes.



Other considerations

- The minimum virtual display resolution required is 640 x 480.
- Virtual display DPI defined through the UI depends on OS scaling support for the given display resolution.
- Do not use this feature simultaneously with the existing virtual display feature in Citrix Workspace™ app.
- Preview functionality isn't supported on Server 2016.

Text-based watermark

September 6, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

  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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

Thinwire

September 6, 2025

Thinwire is the core display remoting technology within Citrix HDX, responsible for delivering smooth and interactive visual experiences in Citrix Virtual Apps and Desktops™ environments.

Thinwire analyzes screen content, identifies changes, and encodes the on-screen graphical data for efficient transmission over the network from the VDA to the user's endpoint device.. This ensures that the information is sent as efficiently as possible, minimizing bandwidth consumption and optimizing performance, especially in challenging network conditions.

HDX™ Graphics, powered by Thinwire, is Citrix's advanced display technology designed to deliver high-performance, adaptive, and efficient remote desktop and application experiences. By intelligently analyzing and compressing graphical data, Thinwire ensures optimal performance across diverse network conditions and endpoint devices.

Key Features of HDX Graphics and Thinwire

- **Adaptive Display Compression:** Thinwire dynamically adjusts compression algorithms based on the content type and network conditions, ensuring a balance between image quality and bandwidth efficiency. This adaptability allows for smooth performance even in bandwidth-constrained environments.
- **Graphics Processing Units:** HDX Graphics will automatically leverage the GPUs capabilities when available on the VDA for hardware encoding
- **Efficient Multimedia Redirection:** By redirecting multimedia content directly to the endpoint for local rendering, Thinwire reduces server-side processing and network load, resulting in a seamless multimedia experience for the user.
- **Optimized Text and Image Rendering:** Utilizing techniques like lossless text compression and intelligent image caching, Thinwire delivers crisp text and sharp images, enhancing readability and visual clarity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Support for High-Resolution Displays:** Thinwire efficiently handles high-resolution and multi-monitor setups up to 8 monitors, providing users with a consistent and high-quality visual experience across various display configurations.
- **High Frame Rate Support:** HDX supports frame rates of up to 120 frames per second (fps), ensuring smooth and responsive performance for high-motion applications and scenarios. This capability enhances user experience, particularly in gaming, video editing, and other graphically demanding workloads.
- **10-bit High Dynamic Range:** With 10-bit High Dynamic Range (HDR) virtual desktop sessions, you can use enhanced encoding and decoding capabilities to render high-quality images and videos with an extended range of colors, and greater contrast and brightness.

In comparison to other industry solutions, such as Microsoft's Remote Desktop Protocol (RDP), VMware's Blast Extreme, and Amazon's NICE DCV, Citrix's HDX Graphics with Thinwire stands out by offering a comprehensive set of features tailored to meet the demands of modern remote work environments. Its ability to adapt to varying network conditions, combined with efficient resource utilization and superior image quality, positions it as a leading choice for organizations seeking a robust and flexible remote display solution.

HDX Graphics supports server side graphics processing units (GPU) on the VDA for hardware acceleration of encoding and rendering. HDX Graphics will automatically detect if a GPU is present and will automatically use the GPUs capabilities.

Adding a GPU to the VDA can also help to accelerate graphically intensive applications in use cases like graphics design, video rendering, 3D CAD, and data processing and visualization applications.

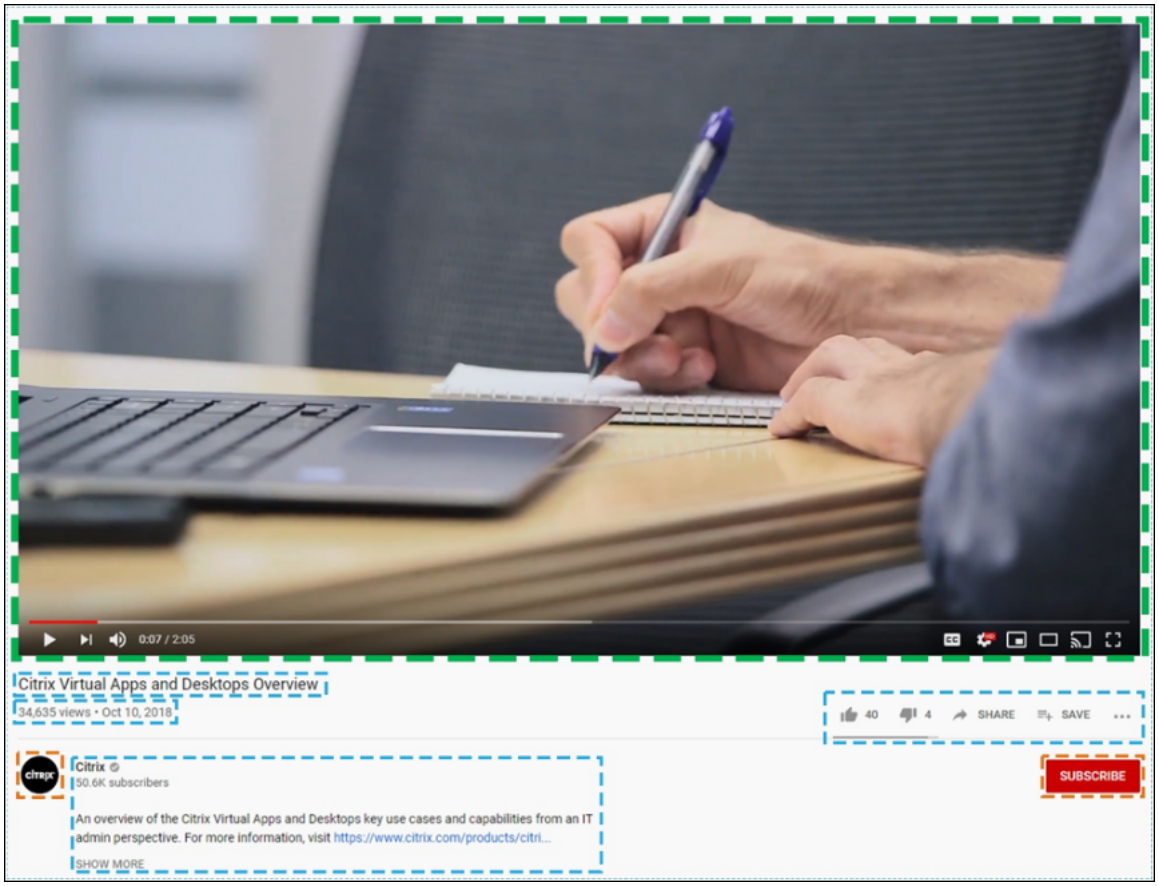
Thinwire Analysis

September 6, 2025

Thinwire analyzes the content on screen in real-time and dynamically categorizes the display data into three types:

- Text, Simple Images and Solid Colors
- Static Image Content
- Moving (or Fluid) Images

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this example shown above, text or simple graphics are highlighted in blue, static images in orange and moving (or fluid) images in green.

After screen analysis, Twinwire will take different approaches to compress and encode each category of display data as efficiently as possible based on the VDAs capabilities and the Thinwire configuration policies set.

Thinwire Configuration

September 6, 2025

Thinwire can operate in different graphics encoding modes depending on its configuration.The main configuration policy for Thinwire is the ‘Use Video Codec for Compression’policy.

- Use when preferred (default)
- For actively changing regions
- For the Entire screen
- Do not use a video codec

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The sections below will describe each mode in more detail.

Use a video codec for compression setting	Text	Images	Moving images and videos	Use cases
Use when preferred (GPU)	Lossless	JPEG	Intelligent Build to Lossless / Video Codec*	Default for most most workloads, including graphically intensive applications
Use when preferred (no GPU)	Lossless	JPEG	Video Codec	Default for most workloads
For actively changing regions	Lossless	JPEG	Video Codec	
For the entire screen	Video Codec	Video Codec	Video Codec	Graphically intensive applications like gaming, when Build to Lossless is not preferred
Do not use a video codec	Lossless	JPEG	Adaptive JPEG	When image quality is preferred over session interactivity. Best scalability due to minimized GPU utilization

*Intelligent Build to Lossless is used only when certain conditions are met.

For most use cases, leaving the Thinwire configuration as default will result in the best performance and display quality.

For more information about the different use cases, refer to our Techzone documentation, HDX Graphics Design decisions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Thinwire Full Screen Encoder

September 6, 2025

Overview

With the release of Citrix Virtual Apps and Desktops™ 2503 and onward, the ‘Optimize for 3D Graphics workload’policy has been deprecated and removed.

This policy has been replaced by the Full Screen Encoder, which provides enhanced functionality and improved user experience for certain graphically intense workloads.

The Full Screen Encoder can be configured using the ‘Use video codec for compression’policy, set to ‘For the entire screen’.

The Full Screen Encoder simplifies configuration while offering robust performance for graphics-intensive workloads. It ensures the entire screen is encoded using a video codec, foregoing any screen analysis or bandwidth optimization to maximize frame rate and interactivity.

This mode is particularly suited for 3D applications and workloads where consistent graphical fidelity is paramount.

The primary benefit of the Full Screen Encoder is that it is able to leverage the YUV444 color space. Moreover, full Screen encoding can provide the highest frame rate possible, up to 120 Frames per second (FPS) compared to the Selective encoder, but uses more bandwidth and resources as a result.

When to Use the Full Screen Encoder?

September 6, 2025

For graphically intensive applications, Build to Lossless should be considered before trying the Full Screen Encoder. Build to Lossless can be set by setting the Visual Quality policy to “Build to Lossless”and leaving the “Use Video Codec for Compression”policy at its default setting “Use when preferred.”

The Full Screen Encoder is only recommended if higher moving image quality is required as it supports the YUV444 color space (see “Allow Visually Lossless”policy). Video Editing is a good example of where this extra fidelity might be required, however, this will come at a considerably higher bandwidth cost.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

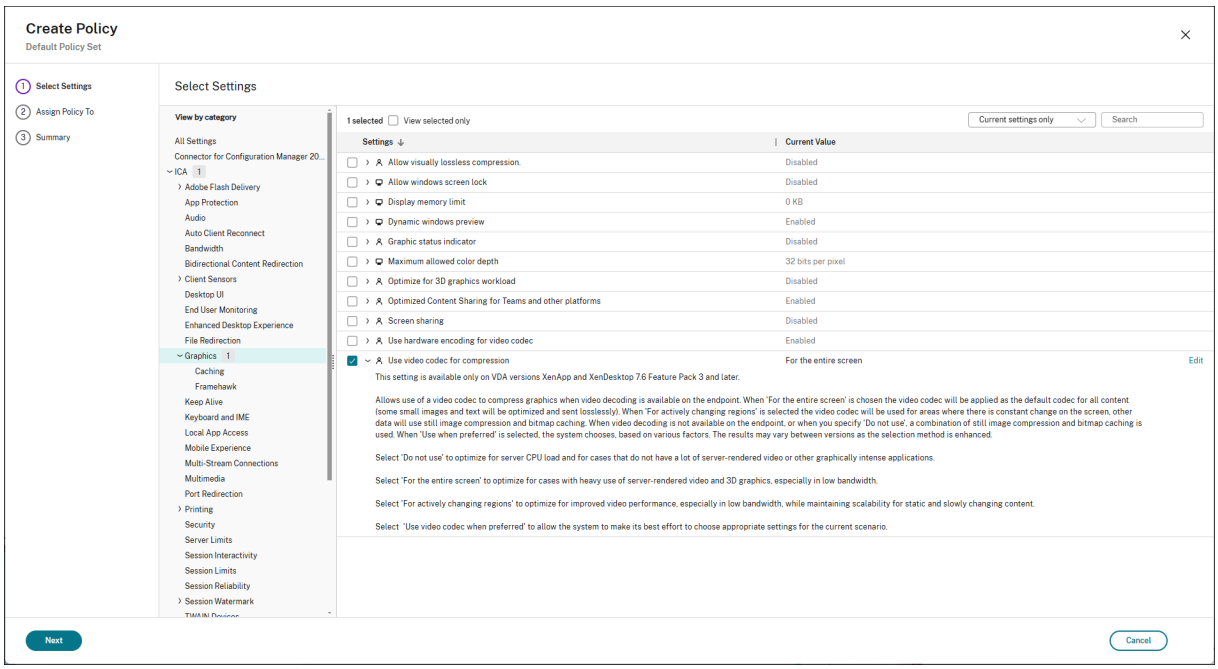
Configuration

September 6, 2025

To enable the Full Screen Encoder:

1. Navigate to the graphics policy settings in Citrix Studio.
2. Locate the ‘Use video codec for compression’policy.
3. Set the policy to ‘For the entire screen’.
4. Apply and propagate the policy changes to your delivery groups.

For additional details on codec behavior and configuration, refer to the Automatic Video Codec Configuration documentation.



Monitoring

September 6, 2025

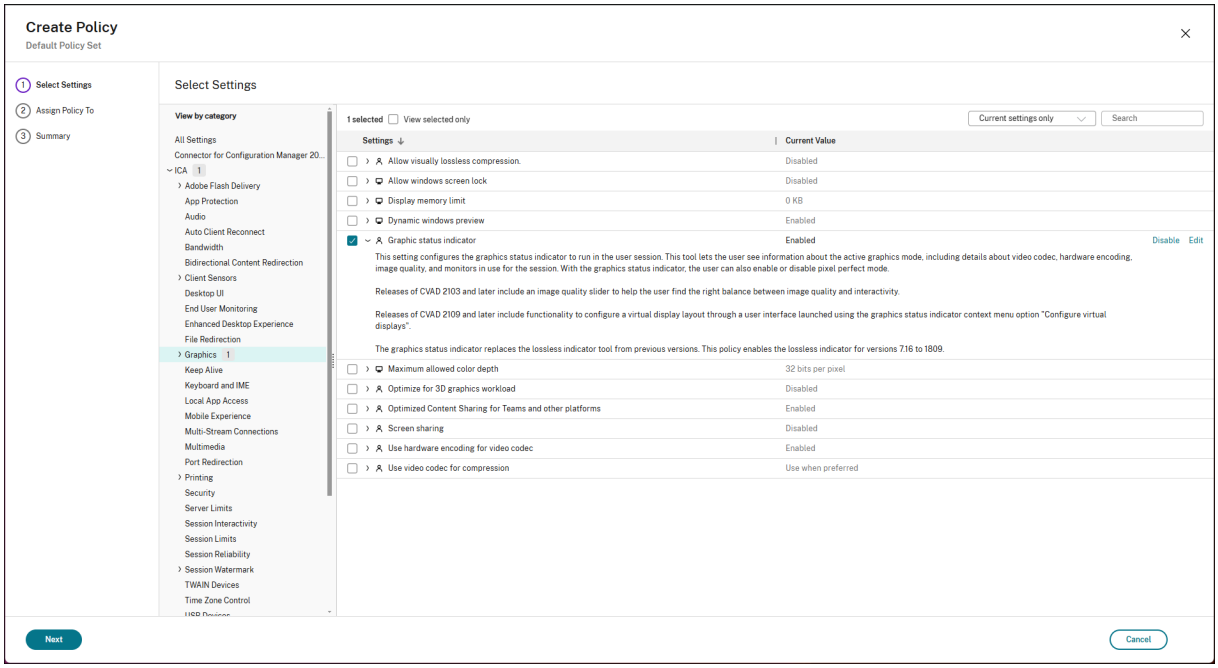
For monitoring the full screen encoder, the Graphics Status Indicator can be used in-session. Currently the Graphics Status Indicator is not enabled by default.

To enable the Graphics Status Indicator:

1. Navigate to the graphics policy settings in Citrix Studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

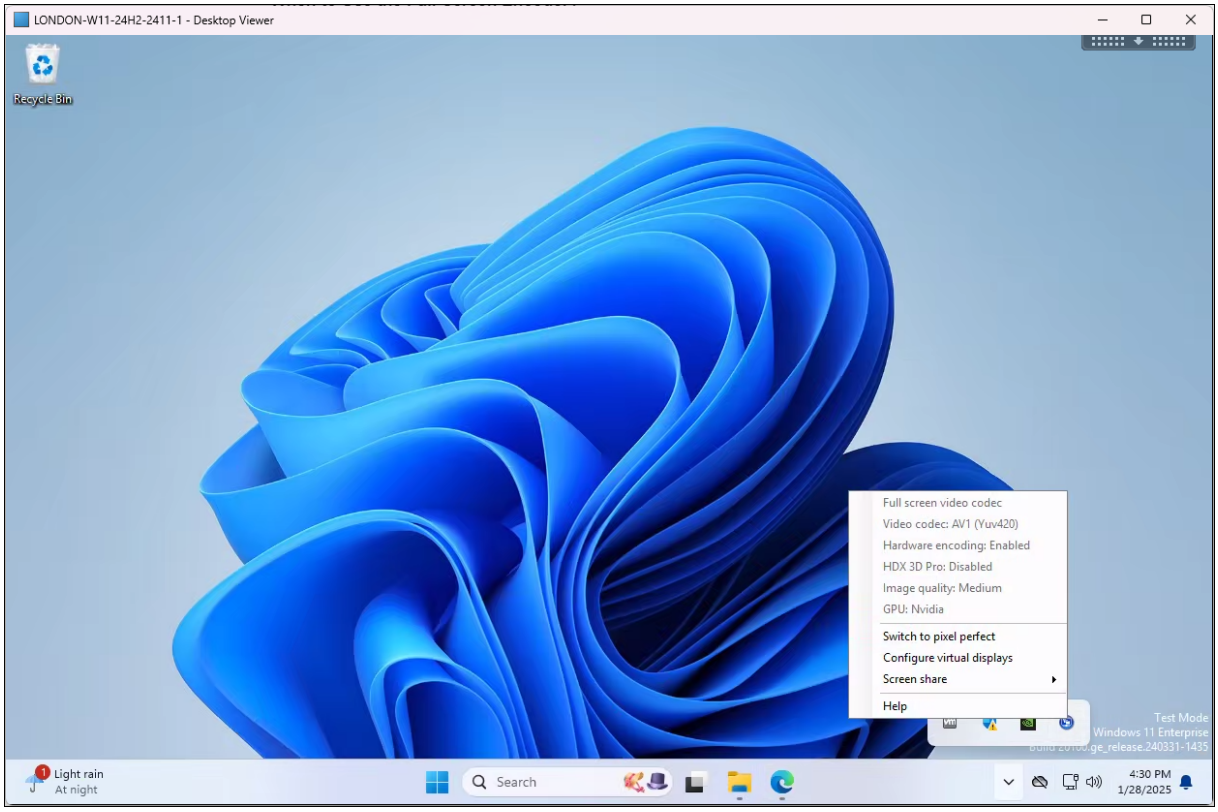
2. Locate the ‘Graphics Status Indicator’policy.
3. Set the policy to ‘Enabled’.
4. Apply and propagate the policy changes to your delivery groups.



The Graphics Status Indicator will be available in the tasktray in the remote session.

When using the full screen encoder the Graphics Status Indicator will show:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Deprecated Policy - Optimize for 3D Graphics Workload

September 6, 2025

Previously, the ‘Optimize for 3D Graphics workload’policy provided functionality similar to the Full Screen Encoder. However, this policy lacked the advanced capabilities.

The removal of this policy streamlines configuration and ensures consistency in performance across varying workloads and environments.

Additional Notes

September 6, 2025

For environments utilizing high-performance GPUs, the Full Screen Encoder maximizes their potential, ensuring smooth delivery of complex visual applications.

Note that YUV444 offers higher color fidelity at the cost of increased bandwidth usage compared to the default YUV420. For more information, see the colour space section

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overview

September 6, 2025

Selective encoding is the default mode of operations for Thinwire. In this mode Thinwire will analyze the screen contents in real-time and select the best method to encode each part of the screen for optimal visual quality, session fidelity and bandwidth usage.

Selective encoding will use:

- Text: Lossless encoding
- Simple Images & Solid Colors: Lossless encoding
- Complex/ Photographic Images: JPEG encoding
- Transient content and moving images: video codec, H.264 / H.265 / AV1 in YUV 4:2:0 colour mode.

Selective encoding has the following characteristics:

- Adaptive Display: The adaptive display technology in Thinwire identifies moving images (video, 3D in motion) and uses a video codec in the parts of the screen where the image is moving.
- Intelligent Build to Lossless: when a GPU is present, Intelligent Build to Lossless can be used to provide the best session interactivity when movement is detected and a guaranteed pixel perfect image once movement has stopped. Thinwire automatically enables Intelligent Build to Lossless on a per-monitor basis based on several factors, including response time monitoring and screen activity.
- Hardware Acceleration: If a GPU is present on the Virtual Delivery Agent (VDA), the Full Screen Encoder leverages the GPU for hardware-accelerated encoding, reducing CPU usage and enhancing performance.
- Automatic Video Codec Selection: The video codec used is dynamically selected based on the capabilities of the VDA and the client. Supported codecs include:
  - AV1: Preferred for its efficiency and high-quality compression.
  - H.265 (HEVC): Used as a fallback for systems that do not support AV1.
  - H.264 (AVC): Utilized in legacy or low-capability scenarios or when no GPU is present on the VDA

When to use Thinwire Selective Encoding

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This mode is recommended for most use cases and will automatically adapt the visual quality based on the available bandwidth. These use cases include (but are not limited to):

- Office workers and developers. Office workers and Developers benefit from the high image quality and sharp text quality provided by the selective encoder
- Financial Traders: Financial traders typically use multiple high resolution monitors.
- 2D CAD: For 2D CAD use cases, sharp lines and high resolutions are important. Intelligent Build to Lossless, which is part of the Thinwire Selective Encoder, will ensure fast response times as well as a pixel perfect image when movement ceases.
- Medical Imaging: Selective encoding can be combined with lossless image quality to provide a pixel perfect image for medical use cases. (Pending FDA approval)

Configuration

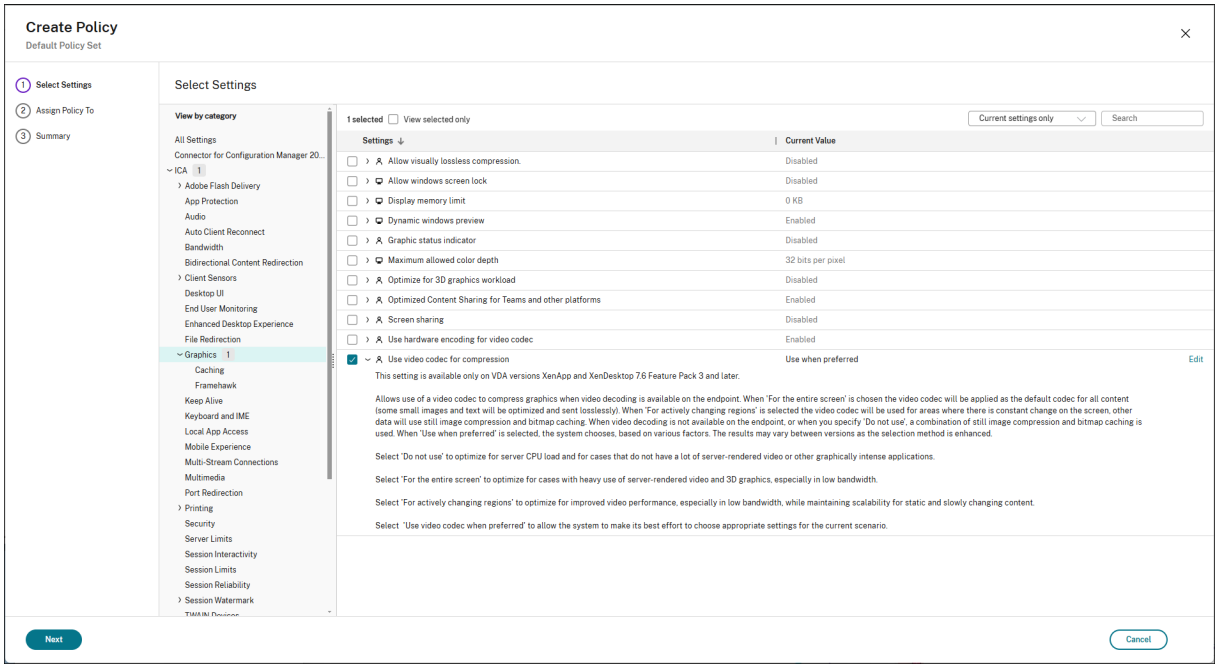
September 6, 2025

Selective encoding is the default mode of operation and therefore no additional configuration is necessary. By default, selective encoding will use Intelligent Build to Lossless when a Server side GPU is available.

To explicitly set selective encoding:

1. Navigate to the graphics policy settings in Citrix Studio.
2. Locate the 'Use video codec for compression' policy.
3. Set the policy to 'Use When Preferred'.
4. Apply and propagate the policy changes to your delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

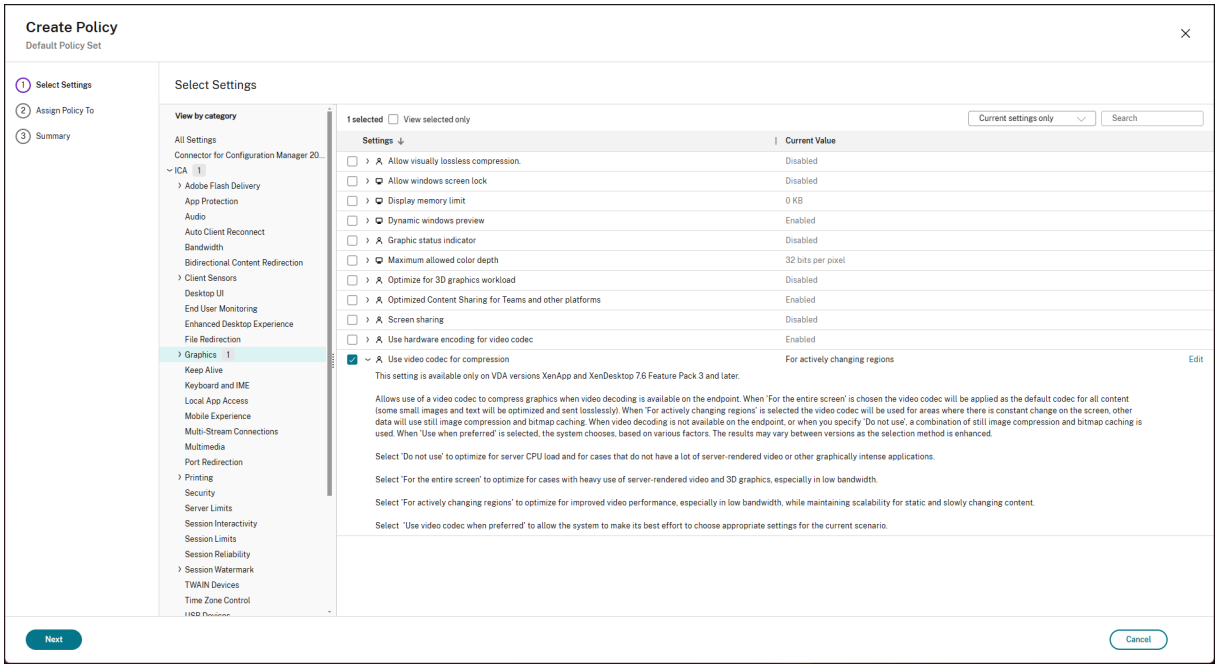


Intelligent Build to Lossless was introduced with Citrix Virtual Apps and Desktops™ version 2503. For CVAD versions prior to 2503, selective encoding will work without Intelligent Build to lossless.

To use selective encoding without Intelligent Build to lossless for VDAs with a GPU (to set the legacy behaviour of versions prior to 2503):

1. Navigate to the graphics policy settings in Citrix Studio.
2. Locate the 'Use video codec for compression' policy.
3. Set the policy to 'For actively changing regions'.
4. Apply and propagate the policy changes to your delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Note for versions prior to 2503, use when preferred and for actively changing regions were identical. In 2503, the default setting of use when preferred includes Intelligent Build to lossless when a GPU is available. In cases where there is no GPU, use when preferred is identical to for actively changing regions.

Build to Lossless

September 6, 2025

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 is designed to be as lightweight as possible, and will disable most of the Thinwire image analysis performed in regular selective encoding. It employs a "fuzzy-first"approach, assuming a lossy codec will give better performance for moving images and when movement has stopped will gradually build up to a guaranteed lossless image.

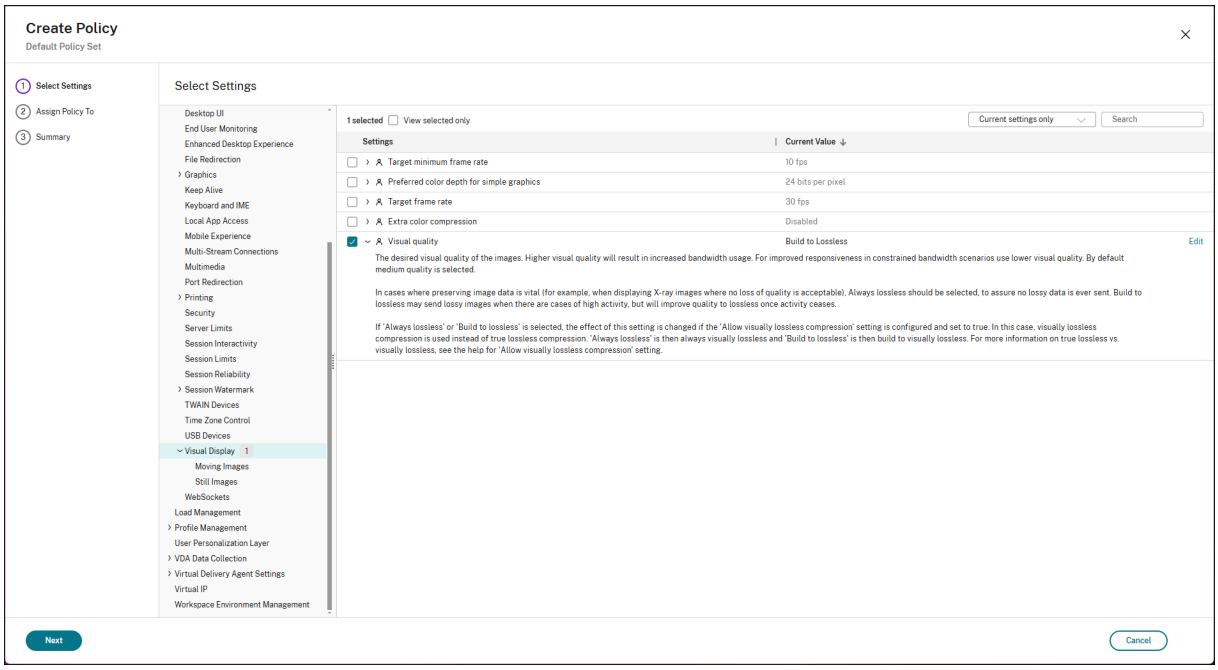
Build to Lossless compresses the screen using the selected video codec (AV1, H.265 or H.264) during screen activity and sharpens to pixel perfect (lossless) when activity stops. The lossy image quality adapts to available resources to maintain the best possible frame rate. The sharpening step is performed gradually, radiating outwards from the mouse cursor. This allows for an immediate response if the user begins screen activity shortly after sharpening starts. For example, selecting a model and rotating it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With regular Build to Lossless, all monitors will operate in Build to Lossless mode when enabled. If you are looking for the ability to run Build to Lossless on select monitors, please refer to our new Intelligent Build to Lossless feature below. [insert link to Intelligent Build to Lossless]

Build to lossless can be enabled by using the Visual Quality policy setting.

1. Navigate to the graphics policy settings in Citrix Studio.
2. Locate the 'Visual Quality'policy.
3. Set the policy to 'Build to lossless'.
4. Apply and propagate the policy changes to your delivery groups.



When to Use the Regular Build to Lossless?

September 6, 2025

The Regular Build to lossless is designed for following use cases

- Full screen 3D CAD
- Full screen 2D CAD
- Certain modalities for medical imaging
- Financial / Trader

For all of these use cases, please consider using Intelligent Build to Lossless over regular build to lossless when using multiple monitors within the Citrix® session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Intelligent Build to Lossless

September 6, 2025

This article describes the Intelligent Build to Lossless graphics mode for Citrix HDX. It explains how the feature works, how to configure it, and how to verify and monitor its operation. It also compares this mode to the existing Build to Lossless and Always Lossless Visual Quality settings.

Designed for mixed workloads in mind, Intelligent Build to Lossless is an evolution of Thinwire Selective Encoding and is the new default graphics mode. Similar to the existing Build to Lossless setting, Intelligent Build to Lossless uses a video codec on large, actively changing screen regions to maintain smooth session graphics. When the screen activity ceases, it progressively refines the image until it is pixel perfect. Where Intelligent Build to Lossless differs from the existing Build to Lossless setting is how the mode is toggled: the choice of whether to engage Build to Lossless or not is no longer just a policy decision, but instead based on screen activity and other factors. Moreover, this decision is made on a per-monitor basis, allowing - for the first time - a mix of Thinwire Selective Encoding and Build to Lossless all within the same session.

Intelligent Build to Lossless is enabled by default for Citrix Virtual Apps and Desktops™ version 2503 and later when a GPU is present on the VDA. When no GPU is present on the VDA, Selective Encoding without Intelligent Build to Lossless is used, which is essentially the same as how Selective Encoding worked prior to version 2503.

No Citrix Workspace™ app upgrades are required to take advantage of Intelligent Build to Lossless.

Comparing Graphics Modes - Intelligent BTL vs. BTL vs. Always Lossless

September 6, 2025

The following table highlights the key differences between Intelligent BTL, BTL and Always Lossless:

Feature	Intelligent Build to Lossless (Recommended)	Build to Lossless	Always Lossless
Configuration	Enabled by default, controlled via the Use video codec for compression policy on GPU-enabled VDAs	Visual Quality policy set to Build to Lossless	Visual Quality policy set to Always Lossless

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Intelligent Build to Lossless (Recommended)	Build to Lossless	Always Lossless
Activation	Dynamic. Thinwire intelligently activates and deactivates based on screen content.	Always on for the entire session duration.	Always on for the entire session duration.
Scope	Per-monitor. Activates and deactivates in real time only on the monitor(s) where Build to Lossless is required.	Affects all monitors connected to the session, which may result in productivity apps e.g., e-mail being rendered in two passes.	Affects all monitors connected to the session.
Bandwidth consumption	Moderate to Low, depending on screen activity.	Moderate, depending on screen activity.	High.
Use cases	The default mode for all use cases on GPU-enabled VDAs. For VDAs without a GPU, Selective Encoding will be used, similar to VDAs before 2503.	Superseded by Intelligent Build to Lossless. Not recommended for new deployments with GPU-enabled VDAs.	Use cases where every single frame, including during motion, must be lossless.

Prerequisites

September 6, 2025

Intelligent Build to Lossless is the new default mode for all use cases on GPU-enabled VDAs.

VDA

Intelligent Build to Lossless is available for Windows, Linux and Mac VDAs.

It is important to note that the CVAD version requirements vary by operating system.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Windows VDA:** CVAD 2503 or later
- **Linux VDA:** CVAD 2503 or later
- **MacOS VDA:** 2507 or later

VDA Hardware: A server-side GPU is required (NVIDIA, AMD, or Intel).

More information see, Intelligent Build to Lossless for Linux VDA.

> **Note**:
>
> Intelligent Build to Lossless is not available on VDAs without a GPU.

Citrix Workspace™ App

Citrix Workspace app: all currently supported versions.

Intelligent Build to Lossless is independent of the client's hardware and will work with all clients, whether or not they have a client-side GPU.

When to Use the Intelligent Build to Lossless?

September 6, 2025

Intelligent Build to Lossless is suitable for all workloads and networking scenarios. It is particularly well suited for mixed workloads and use cases where end users are using multiple monitors and high-resolution displays, like high-end financial traders, for example.

Intelligent Build to Lossless is enabled and on by default for VDAs running Citrix Virtual Apps and Desktops™ version 2503 or later and are equipped with a server-side GPU.

There are no additional endpoint requirements; however, Citrix® always recommends using the most recent available CWA client version.

VDA Version	Serverside GPU	Intelligent Build to Lossless
VDA version prior to 2503	yes	no
VDA version prior to 2503	no	no
VDA 2503 or later	**yes**	**yes**
VDA2503 or later	no	no

Citrix recommends using Intelligent Build to Lossless for the following scenarios:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Medical Imaging:

For viewing diagnostic images, such as X-rays, MRIs, or CT scans, where compression artefacts could obscure details and compromise clinical accuracy.

3D CAD/CAM & Engineering:

When working with intricate and complex models and blueprints, precise line clarity is essential for both design and manufacturing.

Pre-press and Graphic Design:

For reviewing color proofs, high-resolution images, or text layouts, where seeing the actual, high-quality source material is required for quality control.

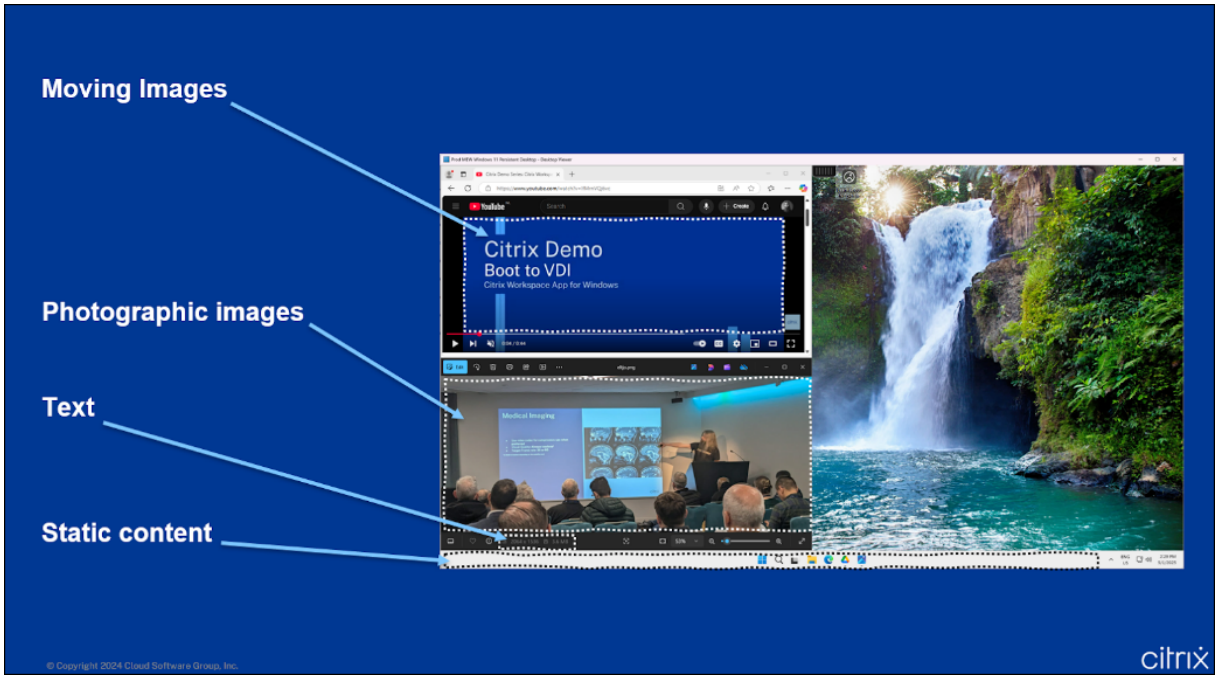
Financial Services:

For displaying dense, real-time data on trading floors, where absolute clarity of static charts and figures is necessary for analysis when using multiple high-resolution monitors

How it works?

September 6, 2025

The feature operates as part of the HDX™ Thinwire display protocol.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Once Thinwire detects a screen region with moving images, it encodes the region using the configured video codec, H.264, H.265, or AV1, depending on the VDA and client's capabilities. This prioritises frame rate and responsiveness.
2. When the region of the screen becomes static, i.e., no movement is detected, Thinwire will gradually build up the area to a lossless state through a series of refinement updates for the static region.

Configuration

September 6, 2025

In Citrix Virtual Apps and Desktops™ release 2503 and later, Intelligent Build to Lossless is enabled by default on VDAs with a supported GPU. You do not need to create any policies to enable it. The behavior is controlled by the state of the "Use video codec for compression"policy:

To enable Intelligent Build to Lossless (Default Behaviour)

Leave the Use video codec for compression policy as *Not Configured*. Alternatively, you can explicitly set the *Use video codec for compression policy* to *Use when preferred*.

To disable Intelligent Build to Lossless (not recommended)

Explicitly set the "Use video codec for compression"policy to "For actively changing regions".

Selecting "for actively changing regions"will result in Thinwire using Selective Encoding like in pre-2503 VDAs with a server-side GPU.

Step-by-Step Instructions

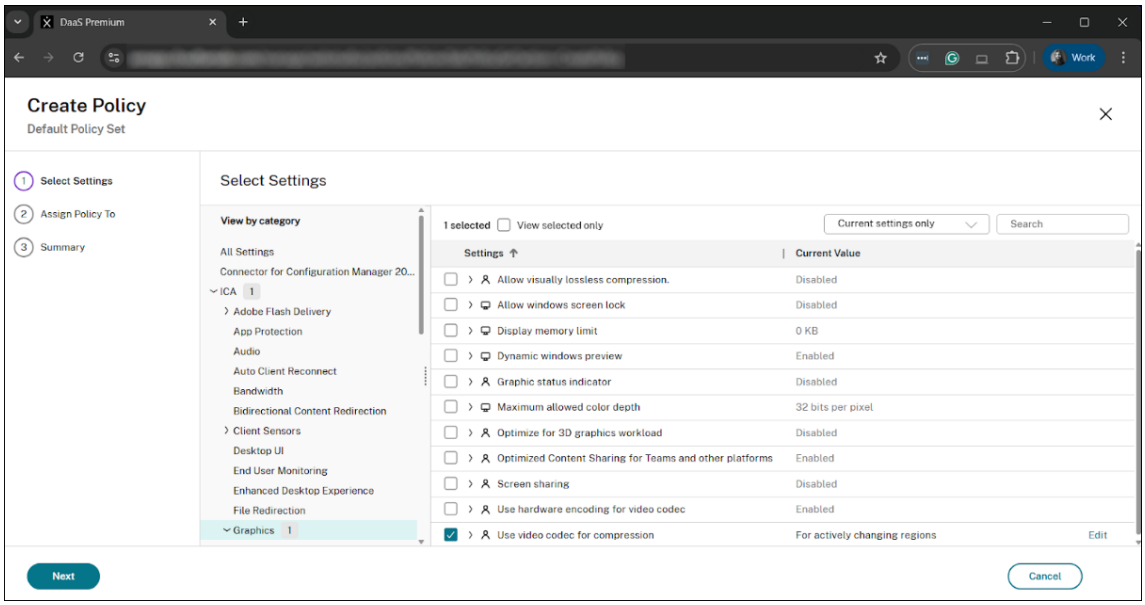
To explicitly disable the Intelligent Build to Lossless policy using Citrix Studio, follow the instructions below.

Citrix Studio (GUI)

1. **Open** the Citrix Studio.
2. In the left-hand pane, navigate to **Policies**.
3. Click **Create Policy** or edit an existing policy that applies to the target users or delivery group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. In the policy configuration window, use the search bar to find the **Use video codec for compression** policy, which is located under the **ICA®** > **Graphics** category.
5. **Select** the policy and click **Edit**.
6. By default, this policy is set to **Use when preferred**. Uncheck the **Use default value** option.
7. Change the value to for actively changing regions.
8. Click **OK** to save the policy setting.
9. Ensure the policy is enabled, prioritized correctly, and applied to the appropriate **Delivery Group** or user filter.



> **Note:**
>
> If the Visual Quality policy is explicitly set to 'Build to Lossless' or 'Always Lossless', those settings will always take precedence and override the new Intelligent Build to Lossless feature. For best results, leave the "Visual Quality" policy and the "Use a video codec for compression" setting at their default values.

Monitoring Intelligent Build to Lossless

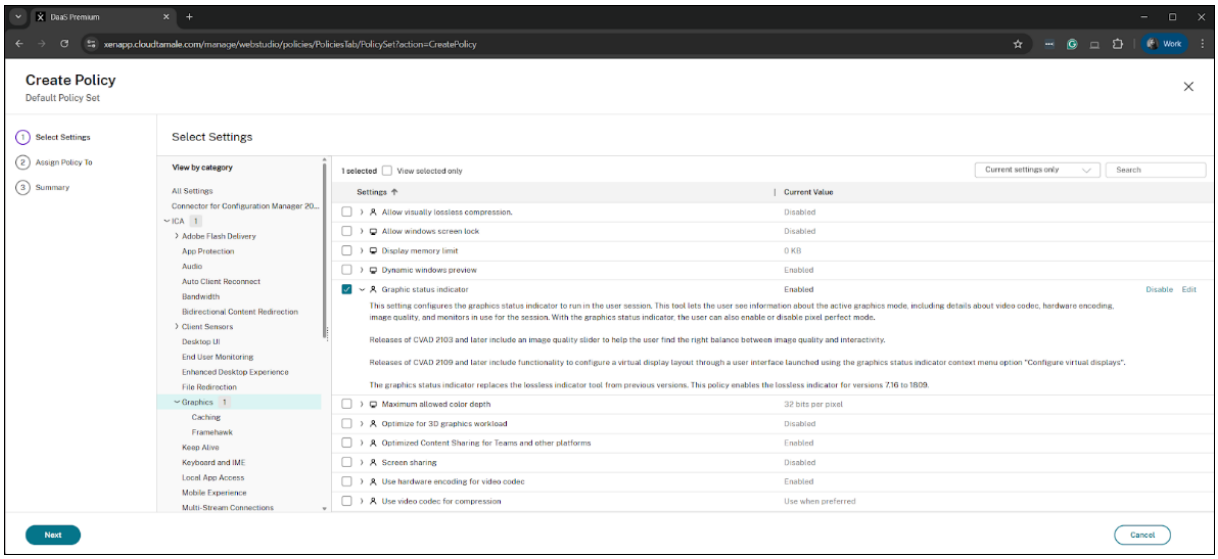
September 6, 2025

Intelligent Build to Lossless can be monitored with our Graphics Status Indicator from within a Citrix® session. Currently, the Graphics Status Indicator is not enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

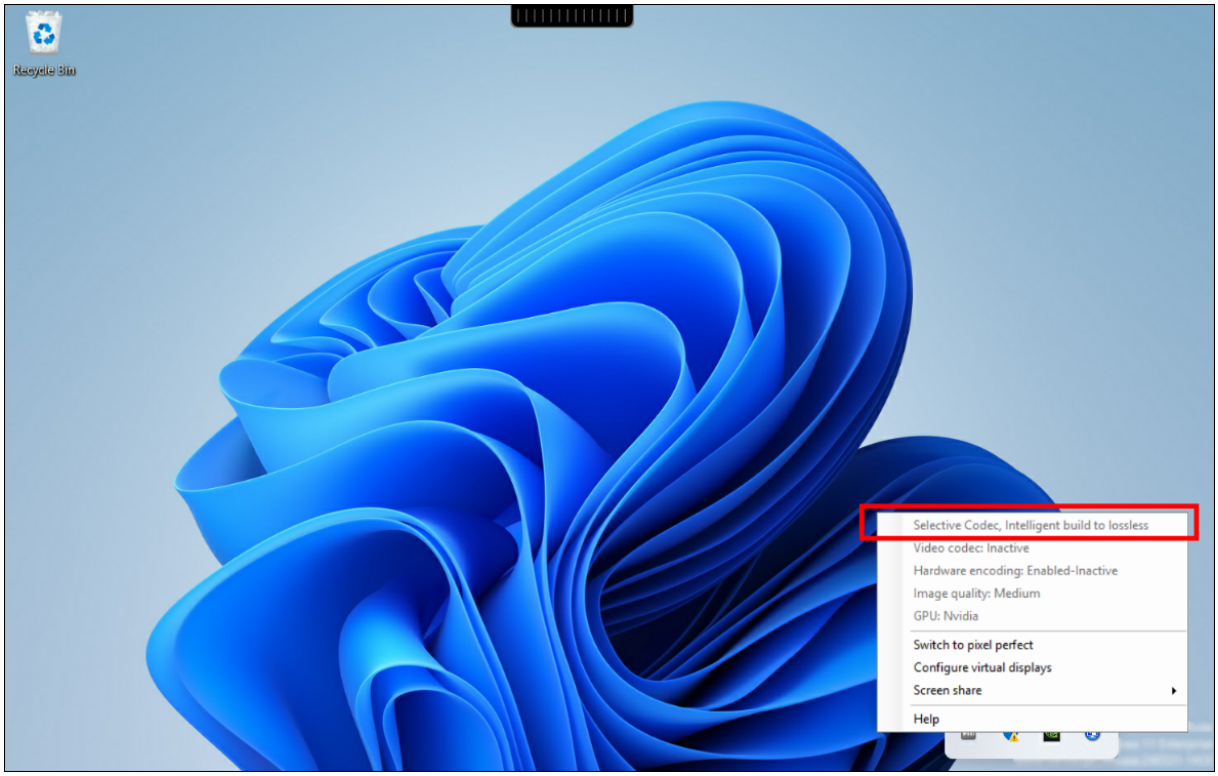
To enable the Graphics Status Indicator

1. Open the Citrix Studio.
2. In the left-hand pane, navigate to **Policies**.
3. Click **Create Policy** or edit an existing policy that applies to the target users or delivery group.
4. In the policy configuration window, use the search bar to find the **Graphics Status Indicator** policy, which is located under the **ICA®** > **Graphics** category.
5. Select the **policy** and click **Enable**.
6. Click **OK** to save the policy setting.
7. Ensure the policy is enabled, prioritized correctly, and applied to the appropriate **Delivery Group** or user filter.



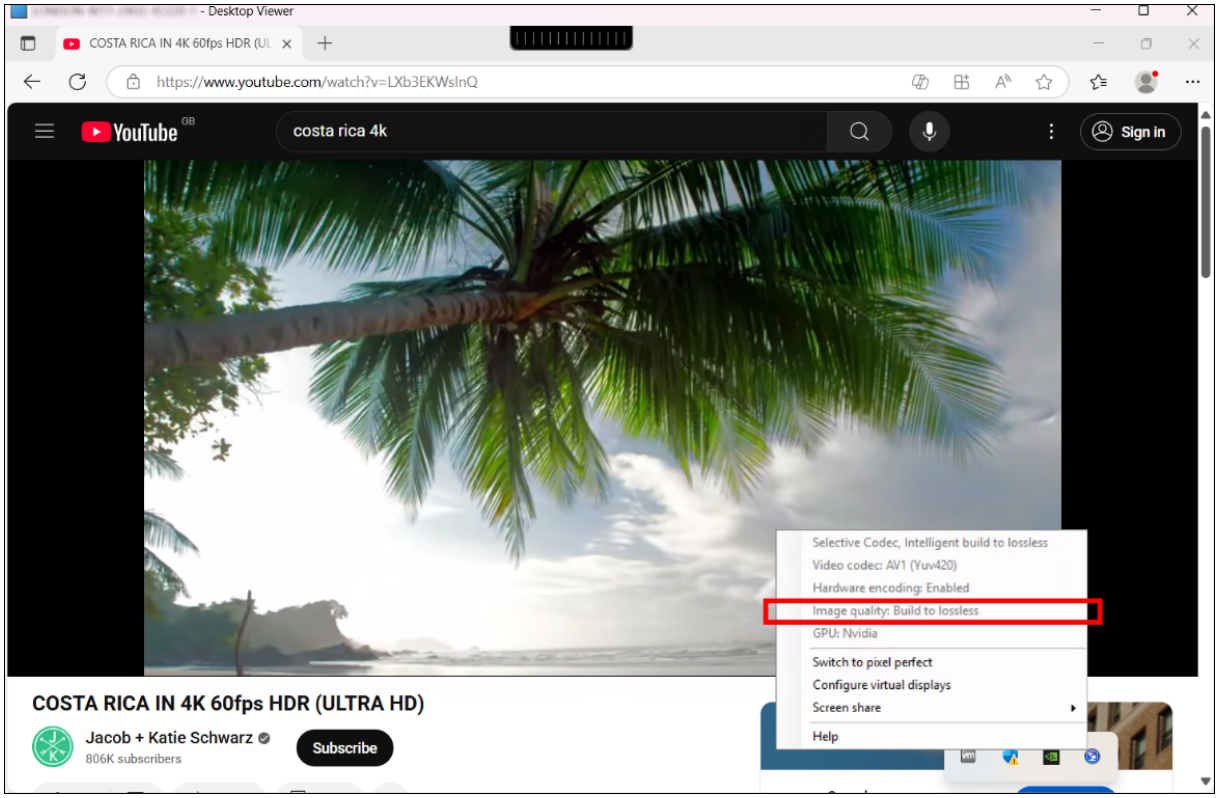
When Intelligent Build to Lossless is available in the user's session, but is not yet activated, the session will use regular Selective Encoding, and the Graphics Status Indicator will indicate this in the top row as 'Selective Codec, Intelligent Build to Lossless'. Because Intelligent Build to Lossless has not engaged yet, the 'Visual Quality'will list the currently configured Visual quality, e.g. Low, Medium or High.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When Thinwire detects the conditions favourable to enable Intelligent Build to Lossless on one or more connected monitors, the Graphics Status Indicator will change the Visual Quality in the fourth row to 'Build to Lossless'. This is the primary indicator that Intelligent Build to Lossless is active.

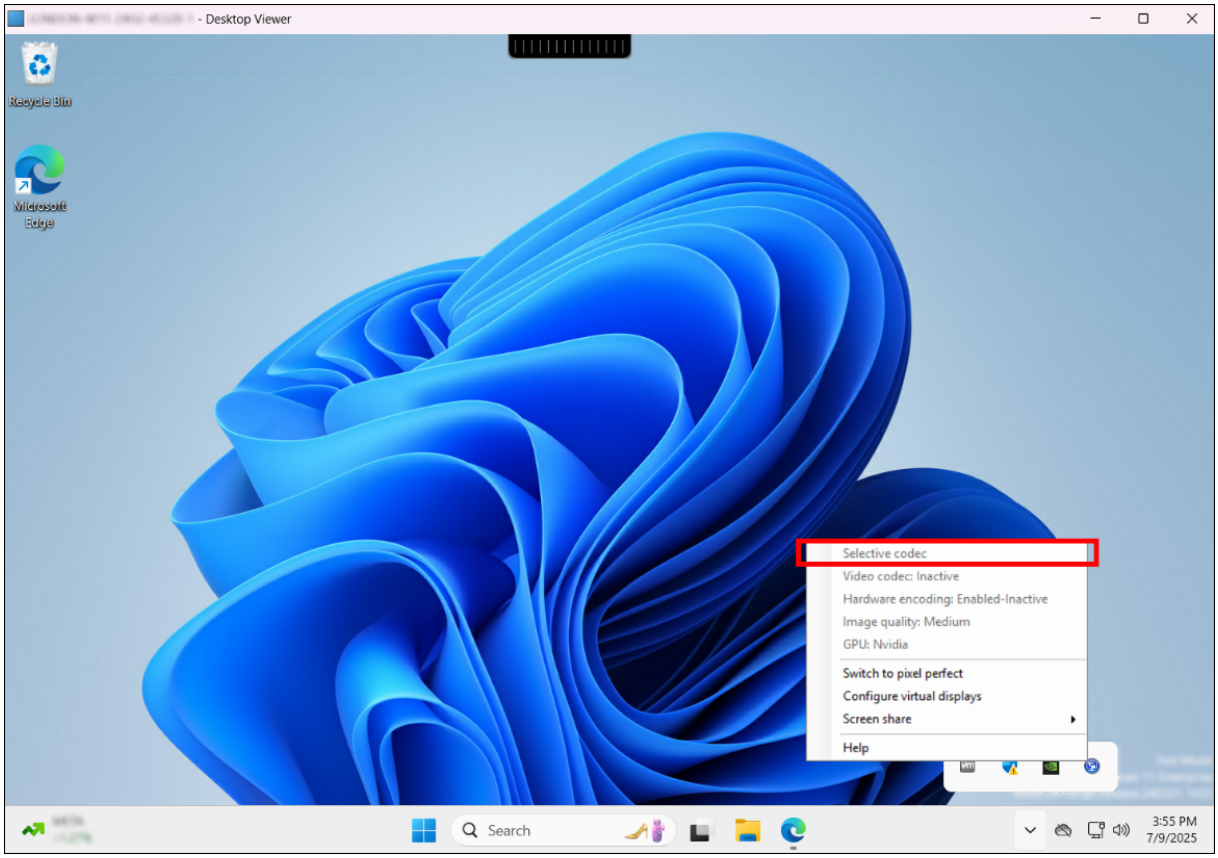
© 1997–2026 Citrix Systems, Inc. All rights reserved.



When Thinwire determines that the need for Build to Lossless has subsided, it will gradually build up to a pixel-perfect image and then revert back to regular Selective Encoding. The Graphic Status indicator will change the image quality back to the configured Visual Quality mode, e.g. Low, Medium or High.

If Intelligent Build to Lossless is not available, for example, when using a pre-2503 release VDA, a VDA without a server-side GPU, or if Intelligent Build to Lossless is explicitly disabled, the Graphics Status Indicator will show 'Selective Codec' in the top row instead:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more in-depth testing and monitoring of Intelligent Build to Lossless, you can also enable a per-monitor visual indicator that will show which monitor is in Build to Lossless mode.

This setting is intended for testing and troubleshooting only and should not be used in production. For more information, see the KB article to enable Intelligent Build to Lossless visual indicator.

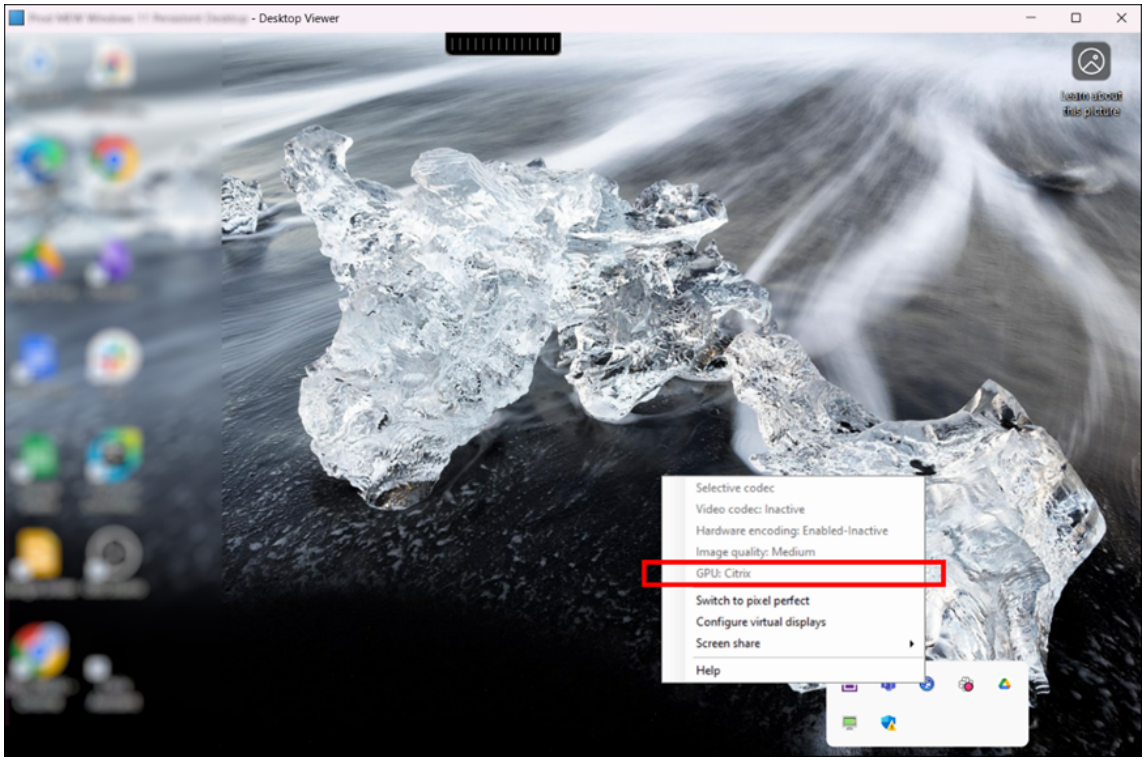
Troubleshooting

September 6, 2025

If Intelligent Build to Lossless is not available in the session, please check the following requirements:

1. Make sure that the VDA is running version 2503 or later.
2. Make sure that a server-side GPU is available in the session. The easiest way to validate this is to use the Graphics Status Indicator and check if the GPU row displays the GPU vendor name, e.g. NVIDIA, Intel or AMD. If no GPU is present and available, the GPU vendor name will show 'Citrix' :

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alternatively, you can use Citrix Monitor to view the presence of a server-side GPU for the VDA and troubleshoot GPU utilisation.

3. Validate that the "Use a video codec for compression"policy is either not set (and using the default value) or is set to 'Use when preferred'.

You can use the Policy Modelling Wizard to determine if the policy has been correctly applied to the session.

For more information on the DaaS side, see policy processes.

Overview

September 6, 2025

Using a videocodec for encoding the remote session has several advantages, it's fast and relatively lightweight. Video codecs are designed for and very good at moving images as is often the case with remote sessions.

However, there might be scenarios where using a video codec might not be the best solution, like when image quality or colour accuracy is paramount. Our selective encoder will in most cases do a very good job to determine which parts of the screen benefit from encoding with a video codec, you can also force thinwire to never use a video codec for screen compression.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When Thinwire is set not to use a videocodec, Twinwire will only use JPEG and Lossless RLE for compression, maintaining the best image quality possible. Thinwire will use considerably more bandwidth than when using selective encoding or full screen encoding.

When to use do not use a video codec

September 6, 2025

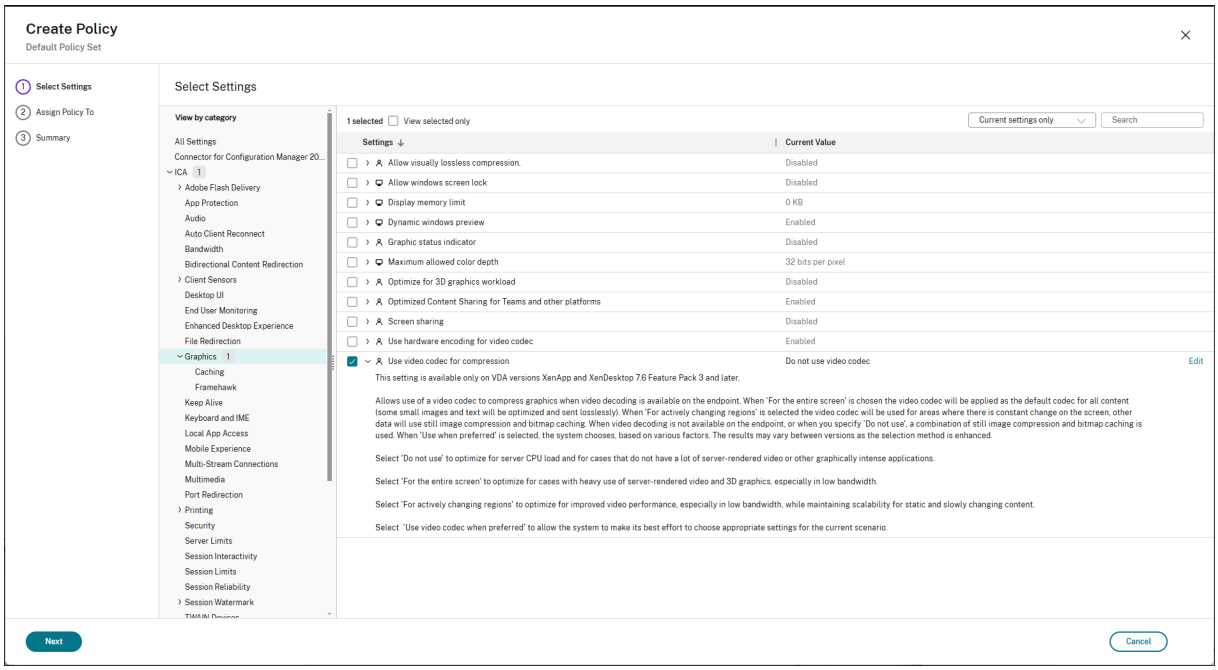
In scenarios where image quality in combination with VDA scalability are the most important factors, you can consider using our Thinwire Full Screen Encoder mode. Not using a video codec can maximize VDA scalability as in general it has a lower CPU overhead than using a video codec for compression

In most of these cases, however, our selective encoder, especially when paired with Build to lossless or intelligent build to lossless will deliver the same quality, better performance and lower bandwidth than when not using video codec compression.

Configuration

September 6, 2025

Set the Thinwire policy ‘Use a video codec for compression’to ‘Do not use a video codec’



© 1997–2026 Citrix Systems, Inc. All rights reserved.

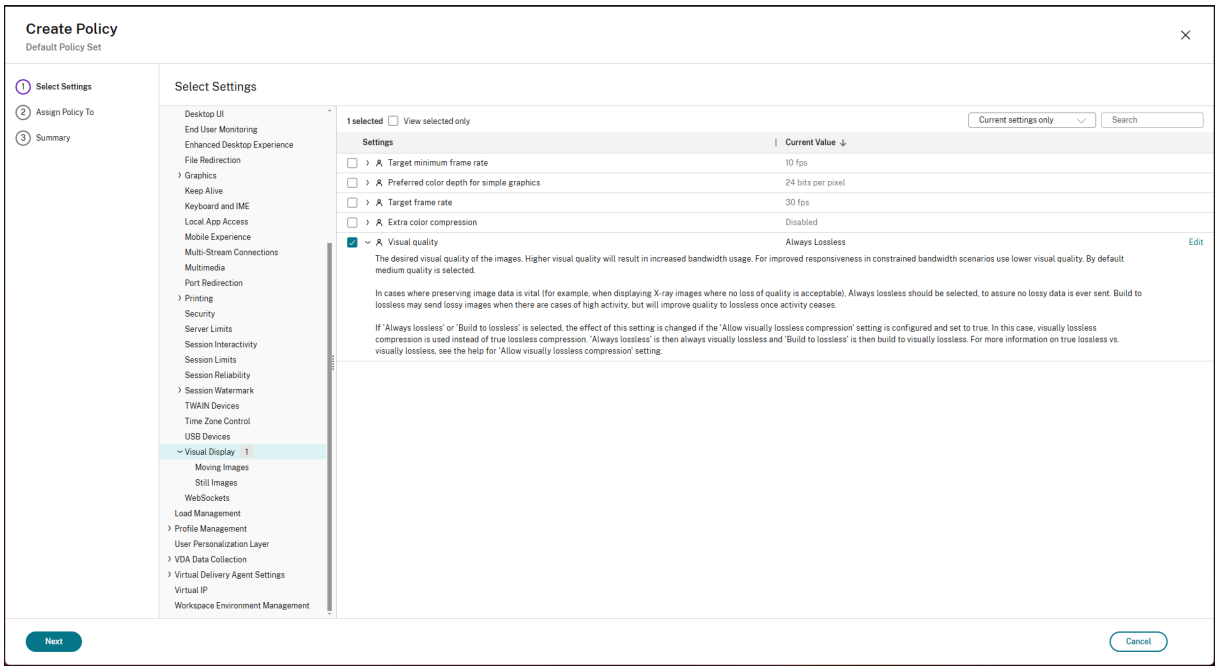
Always Lossless mode

September 6, 2025

Using Always lossless mode will ensure that no image lossy data is ever sent to the client. This means that every frame will only be encoded with a lossless codec and the quality will be pixel perfect.

The compression ratio of always lossless is not nearly as good as with using other modes and setting always lossless mode will use a significant amount of bandwidth. This can significantly impact interactivity when there is not enough bandwidth available.

Citrix® only recommends using this setting for specific use cases where lossless image quality is required such as medical imaging use cases.



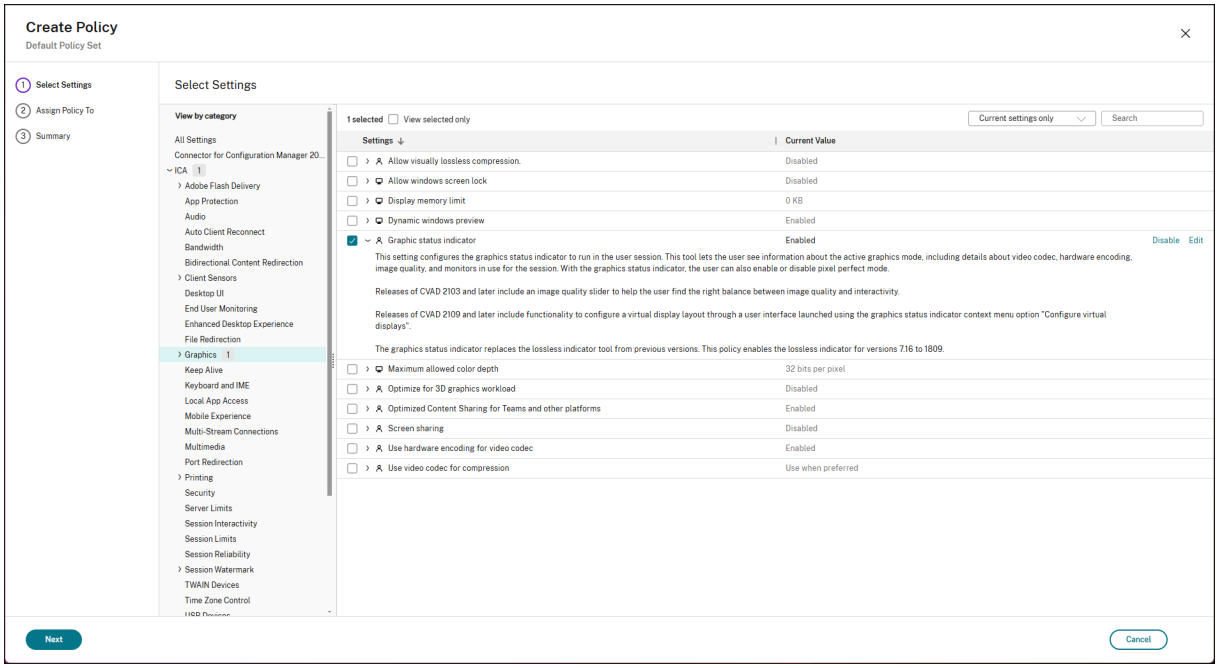
In addition to setting Always Lossless mode explicitly, end users can also toggle between Lossless mode in-session when the Graphics Status Indicator is available for them.

Currently the Graphics Status Indicator is not enabled by default.

To enable the Graphics Status Indicator:

1. Navigate to the graphics policy settings in Citrix Studio.
2. Locate the ‘Graphics Status Indicator”policy.
3. Set the policy to ‘Enabled’.
4. Apply and propagate the policy changes to your delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

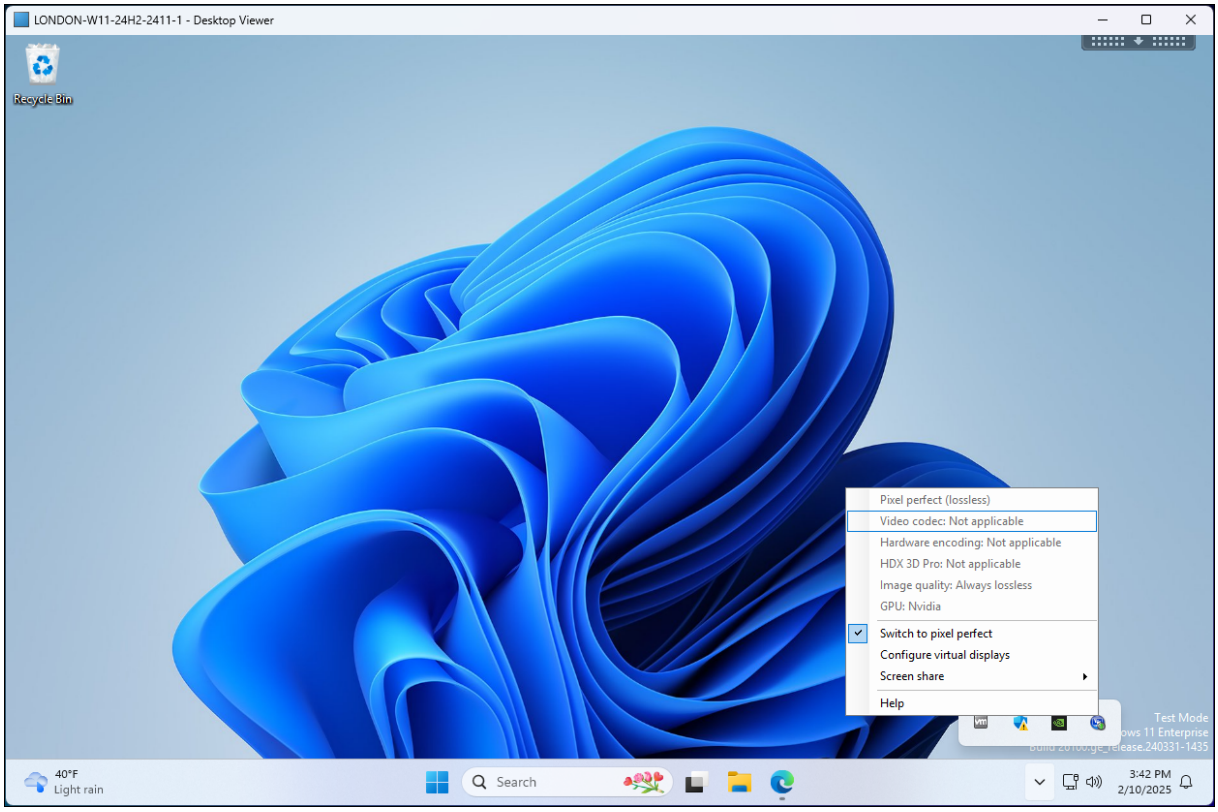


To Toggle Always Lossless mode as an end user:

1. Locate the Graphics Status Indicator in the tasktray.
2. Right-click on the Graphics Status 1. 1. Indicator in the tasktray of the VDA.
3. Select “Switch to Pixel Perfect”.

The Graphics Status indicator will show a green indicator in the icon to indicate that Lossless mode is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

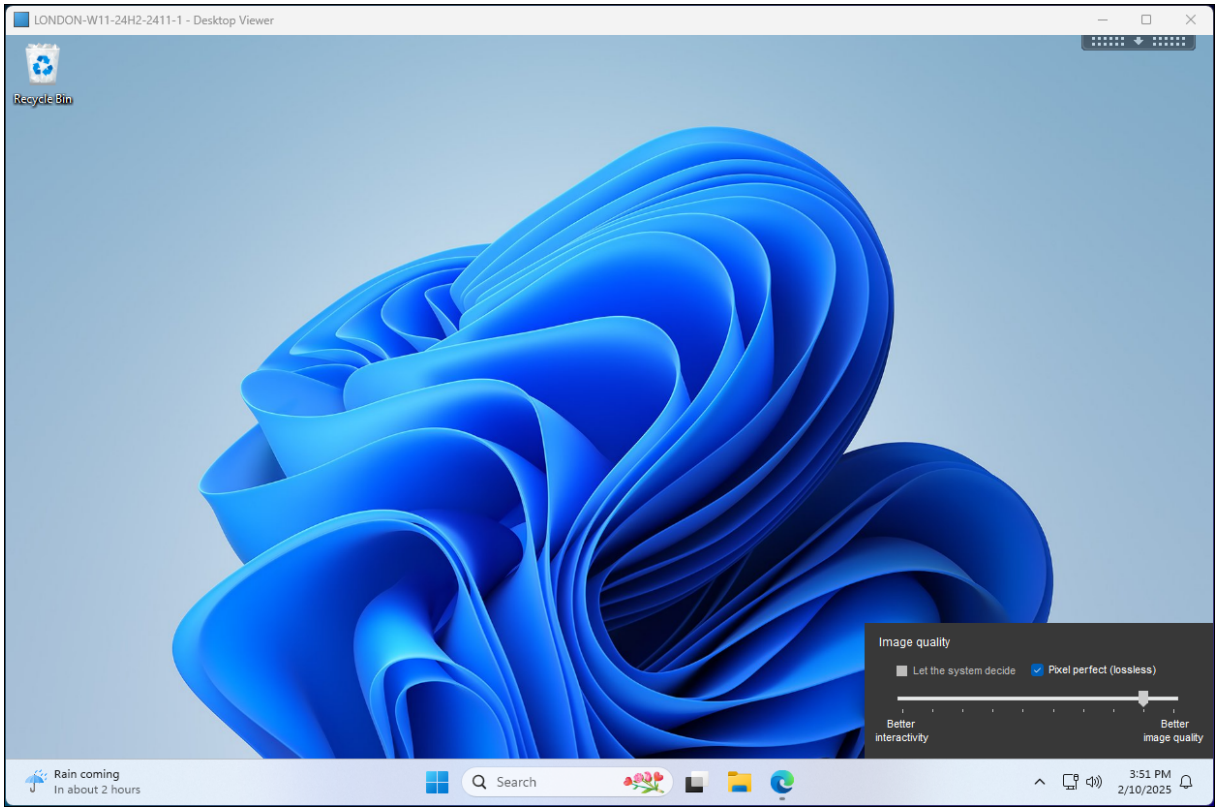


Alternatively:

1. Locate the Graphics Status Indicator in the tasktray.
2. Click on the Graphics Status Indicator in the tasktray of the VDA.
3. Deselect “Let the system decide”.
4. Select “Pixel perfect (lossless)”.

The Graphics Status indicator will show a green indicator in the icon to indicate that Lossless mode is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Color space

September 6, 2025

This is a new section to discuss the color space and color compression settings for YUV 4:2:0 and YUV 4:4:4.

Overview

The color space selected will determine if and what color compression mode (also known as chroma subsampling) will be used by HDX™ Graphics. By default, HDX Graphics uses YUV 4:2:0 chroma subsampling.

Chroma subsampling is a technique used to reduce the bandwidth needed to transmit video data from the VDA to the client. It works by reducing the amount of color information that is transmitted, since the human eye is more sensitive to changes in brightness (luminance) than to changes in color (chrominance).

Different chroma subsampling schemes exist, denoted by ratios like 4:2:0, 4:2:2, and 4:4:4. These ratios represent the amount of chrominance information sampled relative to the luminance informa-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

tion.

4:4:4 - No chroma subsampling. All color information is retained. This provides the highest image quality and color accuracy, but requires the most bandwidth.

4:2:0 - Chrominance information is subsampled both horizontally and vertically by a factor of 2. This offers the greatest bandwidth reduction but may result in noticeable color artifacts.

Citrix HDX graphics utilizes chroma subsampling to optimize bandwidth usage in virtual desktop environments. By default, HDX uses YUV 4:2:0 for encoding screen content. This provides a good balance between image quality and bandwidth efficiency for typical office productivity applications/ for the majority of the use cases.

When the entire screen is encoded with a video codec (by using the full screen encoder), color compression can degrade high-contrast details like text, making them fuzzy and harder to read.

For scenarios where color accuracy is paramount, such as medical imaging, video editing, or CAD/CAM applications, HDX also supports YUV 4:4:4.

This ensures that no color information is lost during encoding, delivering the highest possible image fidelity and color accuracy. Please note that YUV 4:4:4 uses significantly more bandwidth than YUV 4:2:0.

Please validate the bandwidth usage in a test scenario before enabling YUV 4:4:4 in production environments to avoid bandwidth congestion related issues.

Configuration

September 6, 2025

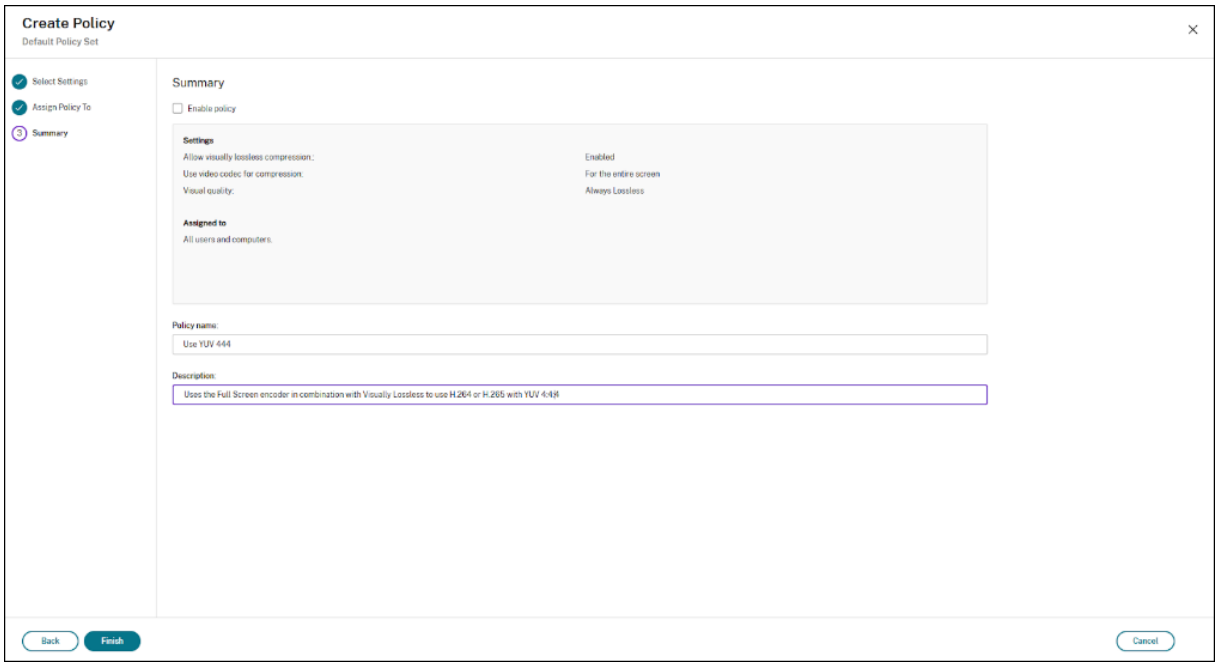
To use the higher image quality and color accuracy with YUV 4:4:4, Enabling YUV 4:4:4 involves adjusting several HDX™ policy settings within Citrix Studio:

Use Video Codec for Compression: Set this to "For the Entire Screen"to apply the video codec (and thus the chosen chroma subsampling) to the entire screen content.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Visual Quality: Select "Build to Lossless"or "Always Lossless"to prioritize image quality over bandwidth consumption.

Allow Visually Lossless: Enable this policy to allow for visually lossless compression.



By default, Thinwire uses H.264 YUV 4:4:4 and if compatible hardware is detected on the client, thinwire will automatically use H.265 YUV 4:4:4 hardware decoding.

With H.265 YUV 4:4:4, internal testing shows a 4X increase in Frames per Second (FPS) compared to H.264 4:4:4 and a 2.5X reduction in size per frame compared to H.264, due to H265's superior efficiency.

Requirements

September 6, 2025

For YUV 4:4:4 with H.264 there are no additional requirements. H.265 YUV 4:4:4 has the following client requirements:

- Citrix Workspace™ App for Windows 2305 or newer
- Enable H.265 support
- Client GPU that supports H.265 4:4:4 decoding:
  - NVIDIA Turing or newer
  - Intel 10th Gen or newer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> At the moment of writing, AMD does not support H.265 4:4:4 decoding.

H.265 YUV 4:4:4 will automatically be used when the VDA is configured to use YUV 4:4:4 with automatic video codec selection. See the Automatic Video Codec documentation for more information.

High resolution displays

September 6, 2025

Customers deploying high-resolution displays (6K, 8K, and equivalent megapixel counts) with Citrix Virtual Apps and Desktops™, might experience issues with performance or issues such as mouse tracking inconsistencies and display scaling and DPI-related problems.

Traditional resolutions for typical office monitors are 4K, 6k or 8K resolutions where the 'K' notation is specifying the horizontal resolution.

Examples of 6K displays are the Apple Pro Display XDR and Dell UltraSharp U3224KB, with a resolution of 6016×3384, and 6144×3456.

Currently there are only a handful of 8K monitors available, one such example is the Dell UltraSharp UP3218K with a resolution of 7680 x 4320.

Barco lists their monitors with a MP or Megapixel count instead of their resolution. The newest Barco monitors are 32MP monitors with an advertised resolution of 6848 x 4560.

Citrix® supports up to 8 monitors, depending on the hardware resources. Depending on the GPU used, there can be other hardware restrictions on this maximum.

To optimize performance and mitigate potential issues with high-resolution displays, Citrix recommends using CVAD 2402.

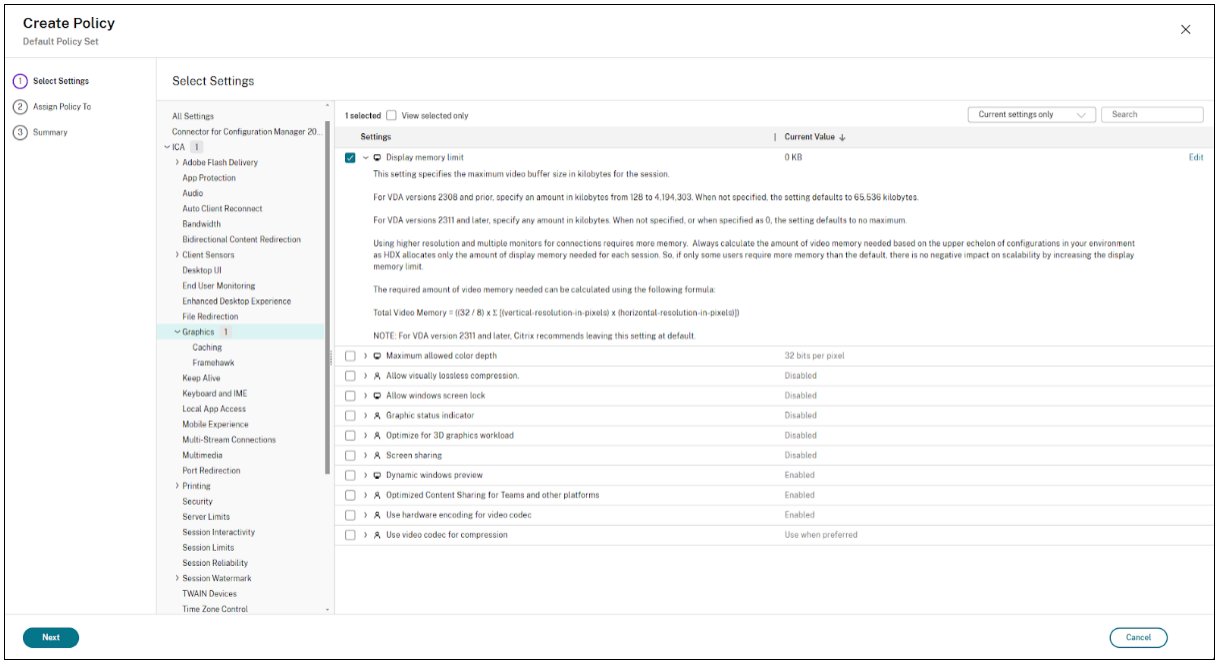
VDA versions 2402 and later

For VDA 2402 and later, leave the 'Display Memory Limit' policy to the default of 0, meaning no Display memory limit. This allows the VDA to dynamically allocate necessary display memory.

Older VDA Versions (Prior to 2402)

If upgrading to CVAD 2402 or later is not feasible, configure the "Display memory limit" policy to its maximum value of 4,194,303 KB. This provides the VDA with the maximum available display memory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



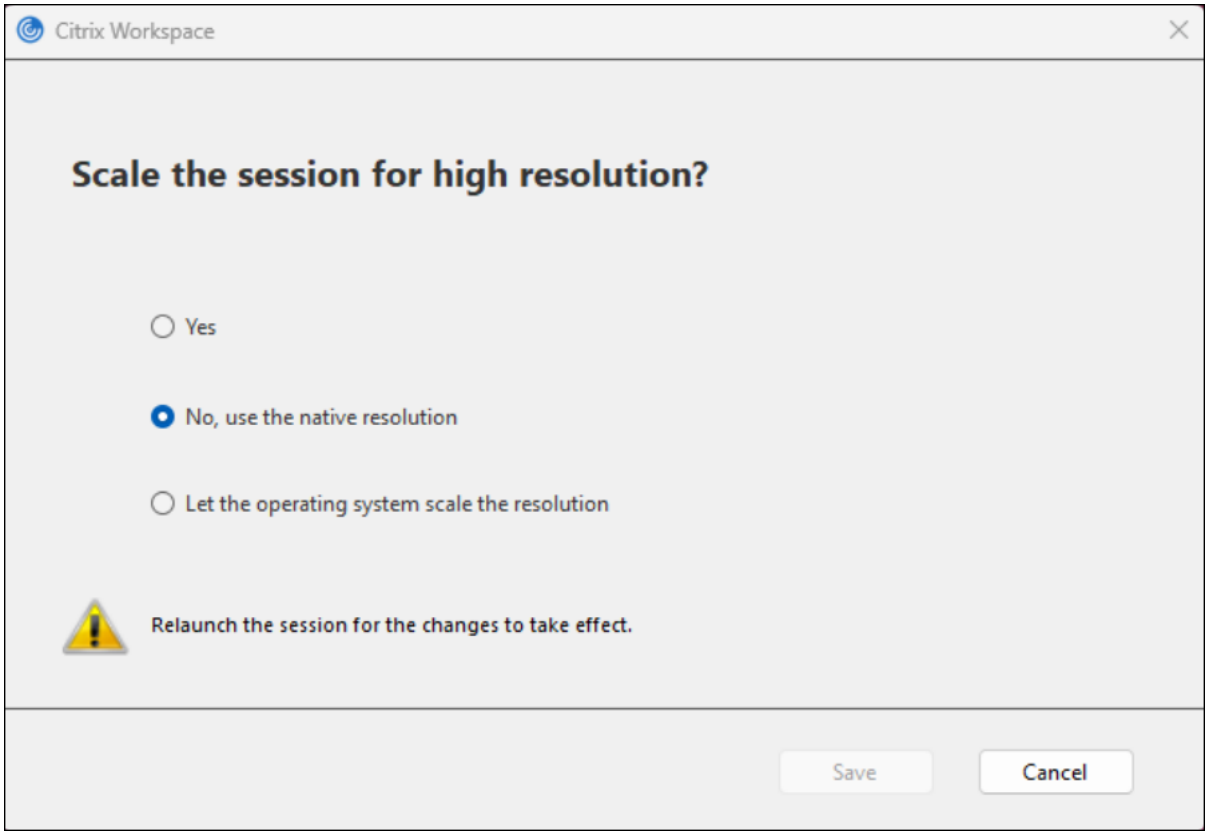
DPI scaling

September 6, 2025

CWA for Windows will match display resolution and DPI scale settings of the local Windows client to the Citrix® session. This is the recommended mode for all cases that meet the following system requirements:

- Citrix Virtual Apps and Desktops™ 2203 LTSR or newer
- Multi-session OS VDAs running on Windows Server 2019 or newer
- Single-session OS VDAs running on Windows 10 or newer
- CWA for Windows 2203 LTSR or newer

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix recommends using Citrix Workspace™ App version 2402 or later.

For more information, please refer to the Citrix Workspace documentation.

GPU

September 6, 2025

For high resolution displays, please ensure the GPUs used (both on the VDA and endpoint) meet the requirements for driving high-resolution displays. Refer to your GPU vendor's documentation for supported resolutions and refresh rates.

When using a server side GPU, Citrix® recommends the following minimal GPU frame buffer sizes:

Monitors and resolution	Recommended Frame buffer size
1 x 4K	2GB
4 x 1080p	2GB
2 x 4K	4GB

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitors and resolution	Recommended Frame buffer size
1 x 6K	4GB
1 x 8K	8GB
2 x 6K	8GB
4 x 4K	8GB

> **Note:**
>
> These are the minimum recommended frame buffer sizes for HDX™ Graphics Encoding. Please consult the application frame buffer requirements and factor these into your sizing as well.

Refer to the NVIDIA sizing guide for more information about Frame buffer sizing for NVDIA GPUs.

Refer to the Intel Virtual Desktop Infrastructure (VDI) Performance on Intel® Data Center GPU Flex Series Whitepaper for more information about GPU Sizing for Intel GPUs.

Refer here for more information.

Performance and scalability considerations

September 6, 2025

Higher resolutions and the number of monitors directly impacts session performance and server scalability.

Bandwidth consumption will increase with higher resolutions and the multiple monitors in use. Bandwidth constraints could limit frame rates and reduce image quality affecting session interactivity and user experience as a result.

The endpoint device must have adequate hardware resources available to support the desired display configuration. This could mean having enough CPU resources and in some cases a GPU that can handle the graphics workload.

Known issues

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

There is a known issue with NVIDIA GPUs in combination with the Full Screen video codec, H.265 encoding and resolutions higher than 4096x4096.

Refer here for more information.

As a work around, use the default **Use video codec for compression"graphics policy setting or explicitly set the policy to either "Let the system decide"or for "Actively changing regions**.

Loss tolerant mode for graphics

September 6, 2025

Loss Tolerant Mode for Graphics enhances the user experience for interactive sessions on networks with high packet loss and latency.

It ensures the session remains responsive by dynamically adjusting the graphics data transmission strategy. Loss Tolerant Mode for Graphics is enabled by default.

When to use loss tolerant mode for graphics

September 6, 2025

When users connect to virtual apps and desktops over networks with challenging network conditions, like high packet loss and latency, their session interactivity and experience can suffer significantly.

This could result in a degraded user experience, characterised by lag and visual stuttering, which negatively impacts productivity and user satisfaction.

To mitigate the effects of these poor network conditions, Loss Tolerant Mode for Graphics automatically switches the Citrix® graphics encoder to a more aggressive packet delivery mechanism when packet loss and latency exceed the configured thresholds. This mode proactively increases bandwidth usage, proportional to the level of packet loss, to ensure data is delivered effectively and the session remains interactive.

Loss Tolerant mode for Graphics has the following benefits:

- **Improved User Experience:** Provides a smoother and more responsive graphics experience on challenging networks.
- **Seamless Operation:** The mode automatically activates and deactivates based on real-time network conditions, without the need for user intervention.
- **Maintained Productivity:** Users can continue to work effectively without being hindered by poor network quality.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System Requirements

September 6, 2025

- Citrix Virtual Delivery Agent (VDA) version 2311 or later
- Citrix Workspace™ app for Windows 2311 or later.

> **Note:**
>
> Both the **HDX™ Adaptive Transport (EDT)** and **loss tolerant mode** for graphics policies must be enabled for this feature to work.

Important requirement considerations

Bandwidth Threshold

Starting with version CVAD 2507, a minimum bandwidth of 30 Mbps is required for Loss Tolerant Mode for Graphics to activate. Even if the latency and packet loss thresholds are met, the feature will not engage if the available in-session bandwidth is below 30 Mbps. This bandwidth threshold is a hardcoded value and cannot be configured.

Configuration

September 6, 2025

The feature is managed through Citrix® policies in Web Studio or Group Policy Management.

Loss tolerant mode for Graphics is enabled by default:

- Policy: Loss tolerant mode for graphics
- Default: Enabled

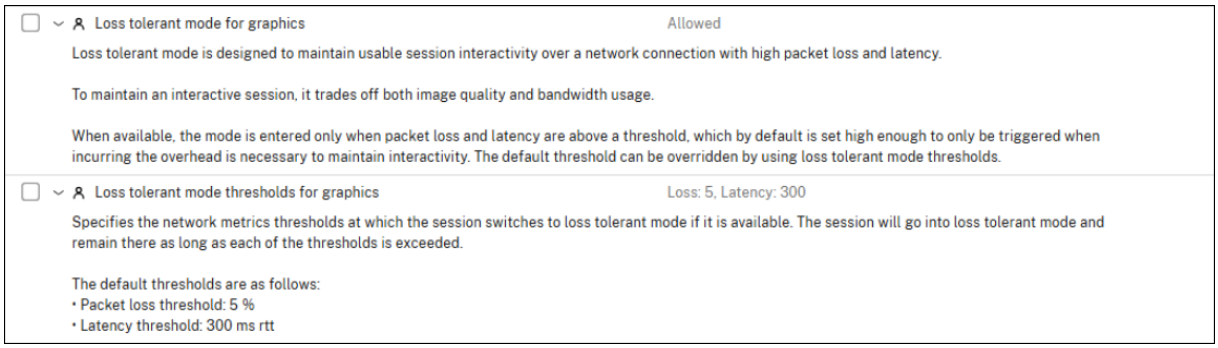
Set this policy to **Disabled** to turn off the loss tolerant mode for graphics feature.

To configure Loss Tolerant mode for Graphics thresholds:

- Policy: Loss tolerant mode thresholds for graphics
- Default Values:
    - Packet loss: 5%
    - Latency: 300 ms

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This policy allows you to adjust the network condition thresholds that trigger loss tolerant mode for Graphics. The mode will activate when both the packet loss and latency values are met or exceeded, and the available bandwidth is at least 30 Mbps.



HDX™ Graphics Superresolution Upscaling (Preview)

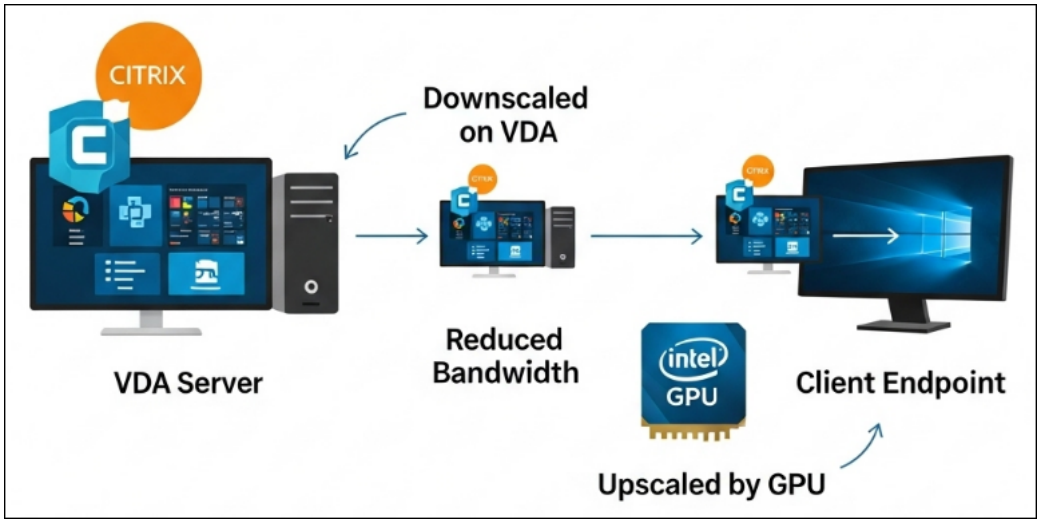
September 6, 2025

HDX Graphics Superresolution upscaling Preview for Intel GPUs is a new joint collaboration between Citrix® and Intel.

Enhance session performance and significantly reduce bandwidth consumption with Citrix HDX Graphics Superresolution Upscaling, a new preview feature in Citrix Virtual Apps and Desktops™ 2507.

Citrix HDX is the first remoting protocol to add support for Superresolution upscaling. This industry-first technology adaptation seamlessly applies additional compression on video resolution on the Virtual Desktop Agent (VDA) and utilises a compatible endpoint Graphics Processing Unit (GPU) to up-scale them back to their original resolution, without any noticeable degradation of quality or adverse effects on the endpoint's performance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The technology is currently available for select Intel endpoint GPUs with this Preview, see the system requirements for more information.

How it works?

September 6, 2025

Delivering graphics-intensive applications can inherently consume a significant amount of bandwidth, especially with high resolutions and multiple displays.

Using HDX™ Graphics Superresolution upscaling can lower bandwidth usage for mixed workloads.

With HDX Graphics Superresolution upscaling, the VDA applies extra compression to the video resolution during encoding. The client then automatically upscales the regions back to their original resolution and quality using the GPU. This process is seamless to the end user and doesn't cause any noticeable quality loss or affect the endpoint's performance.

All Citrix® workloads will benefit from the HDX Graphics Superresolution upscaling technology. As the technology is not dependent on the presence of a server-side GPU, HDX Graphics Superresolution upscaling can reduce bandwidth consumption without the need for costly server-side GPUs.

When a server-side GPU is available, HDX Graphics Superresolution upscaling can work in tandem with new video codecs like H.265 and AV1.

Use cases

High resolution workloads with high-definition video content and endpoints with 10th-generation Intel CPUs or later with integrated Graphics, for example, will benefit from a reduction in bandwidth

© 1997–2026 Citrix Systems, Inc. All rights reserved.

utilization and an increase in user experience by leveraging the integrated GPU's capabilities for upscaling with Citrix HDX Graphics Superresolution upscaling technology.

System Requirements

September 6, 2025

VDA requirements

- Windows VDA 2507 or later
- Citrix HDX™ Graphics Superresolution upscaling is independent of the presence of a server-side GPU and will work either with or without a server-side GPU.
- No additional requirements are needed on the VDA.

Client requirements

- Windows Citrix Workspace™ App 2507 GA or later

In this Preview, the following client-side Intel GPUs are supported:

- Intel Arc A-Series Graphics
- Intel Iris Xe MAX Graphics
- Intel 10th (Ice Lake generation and newer)

Citrix recommends using the latest available Intel GPU drivers. Intel driver updates can be obtained directly from the official Intel driver download page.

Policies

HDX Graphics Superresolution upscaling is designed for use with our default Selective Encoding.

Make sure that the following policies are set:

Use video codec for compression: set to **use when preferred** or **for actively changing regions**.

For the Preview, HDX Graphics superresolution technology is compatible with H.264 video encoding.

When enabled, H.264 video encoding will be enforced, even when a H.265 or AV1 compatible server-side GPU is available.

No additional policies need to be set.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

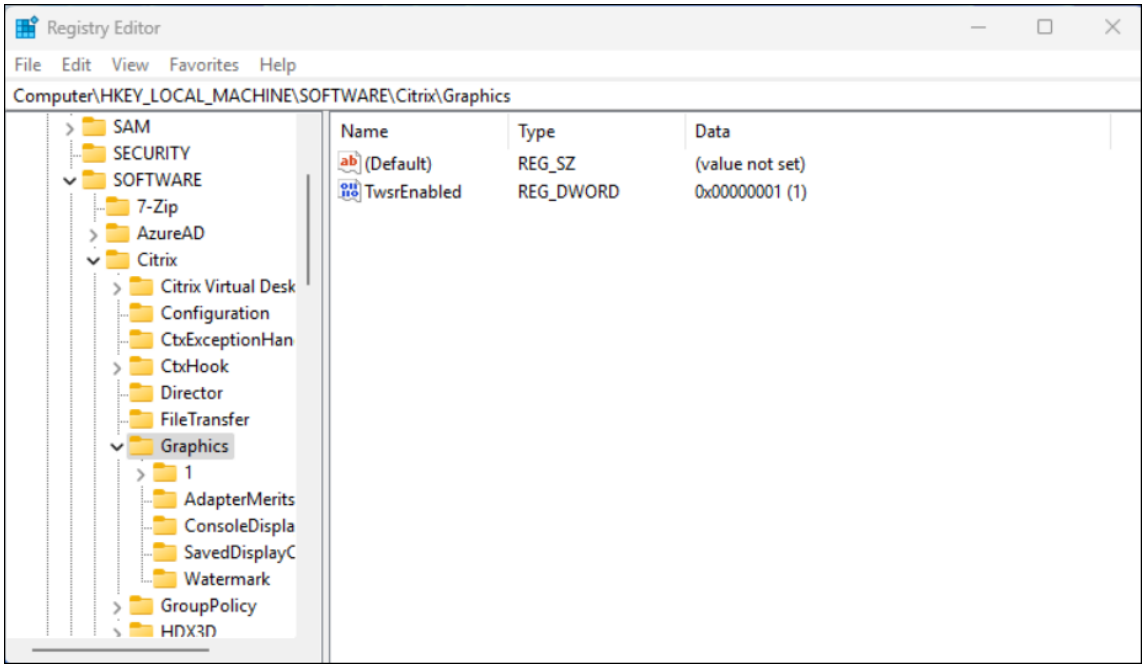
Configuration

September 6, 2025

Enable on VDA

The HDX™ Graphics Superresolution upscaling Preview can be enabled by creating the following registry entry on the VDA:

1. Open Windows Registry Editor (regedit.exe)
2. Navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\`
3. Create a DWORD value named TwsrEnabled and set the value to 1.



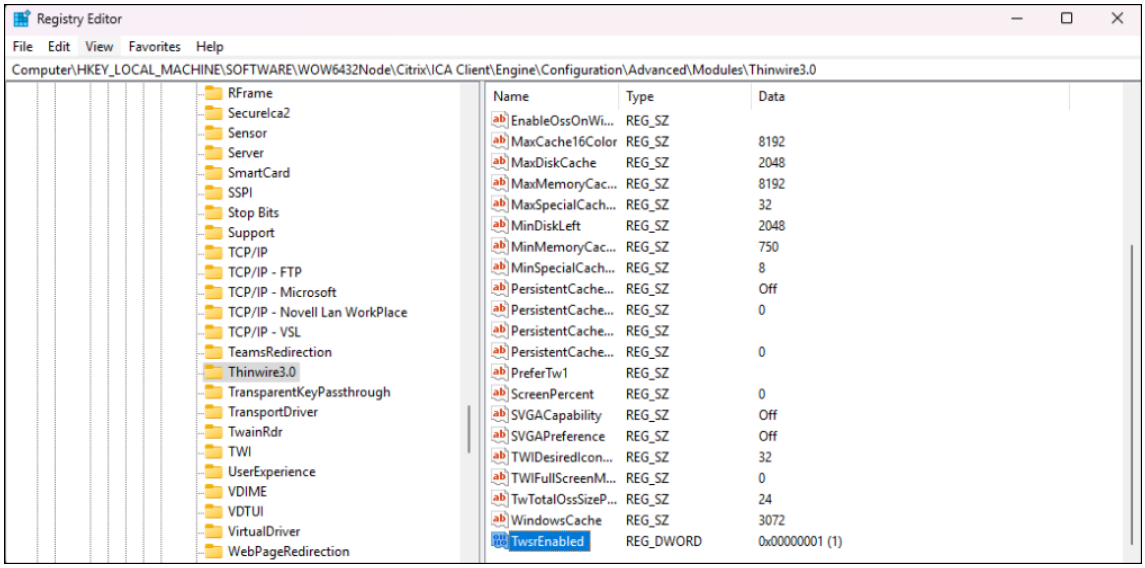
Enable on Client

To enable HDX Graphics Superresolution upscaling Preview on the client, the following registry entry needs to be created:

1. Open Windows Registry Editor (regedit.exe)
2. Navigate to `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Thinwire3.0\`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Create a DWORD value named TwsrEnabled and set the value to 1.



> **Note:**
>
> Both registry keys must be configured and the client device must meet system requirements for the feature to work.

Monitoring and Troubleshooting

September 6, 2025

Known issues

There are currently no known issues with the Preview implementation of HDX™ Graphics Superresolution upscaling.

Important considerations

With this Preview, HDX Graphics Superresolution upscaling is only available with select Intel GPUs and CPUs with integrated graphics. Please refer to the System requirements for the list of supported configurations.

While HDX Graphics Superresolution upscaling will not affect the client's CPU, it will impact the client's GPU. When upscaling large video content regions at high frame rates, this can impact overall client performance. Please monitor client performance when evaluating HDX Graphics Superresolution.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations

> **Note:**
>
> Multi-GPU endpoints, such as for example those equipped with an Intel Lunar Lake CPU and a secondary discrete GPU, are not supported for the Preview.

Furthermore, the Intel GPU must drive all connected monitors.

Unsupported scenarios

Currently, only the default Selective Encoding is supported with the Preview of HDX Graphics Super-resolution upscaling.

The following scenarios are not supported in this Preview:

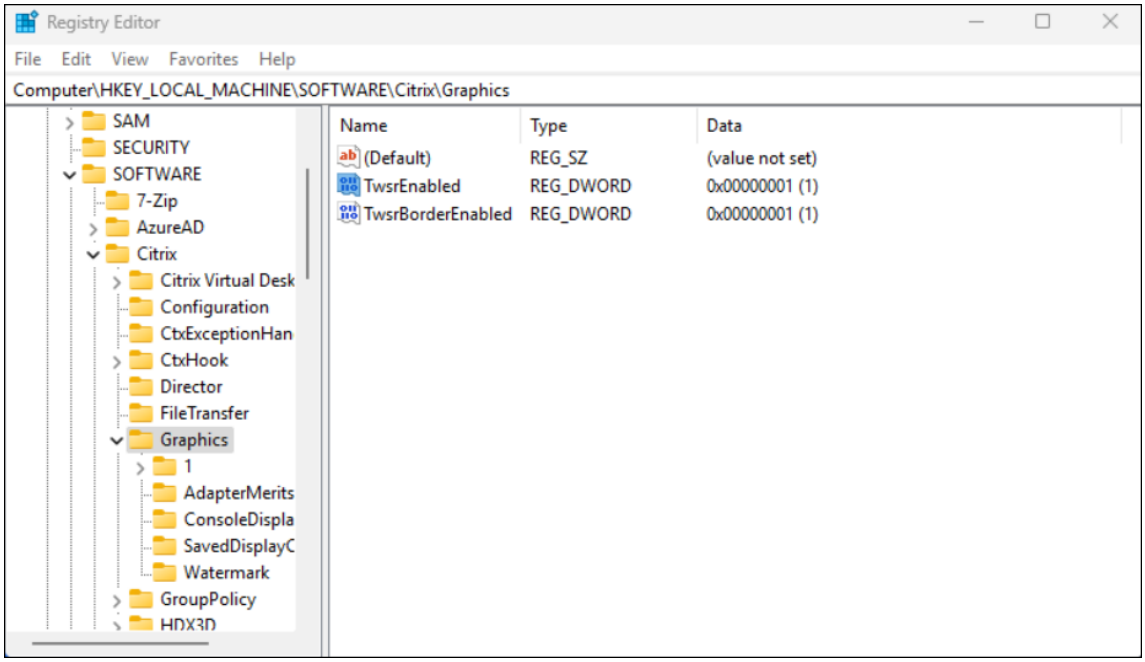
- Build to Lossless mode is not supported.
- Always lossless mode is not supported.
- Full screen encoding is not supported.
  Visually lossless with YUV 4:4:4 is not supported.

Monitoring and Troubleshooting

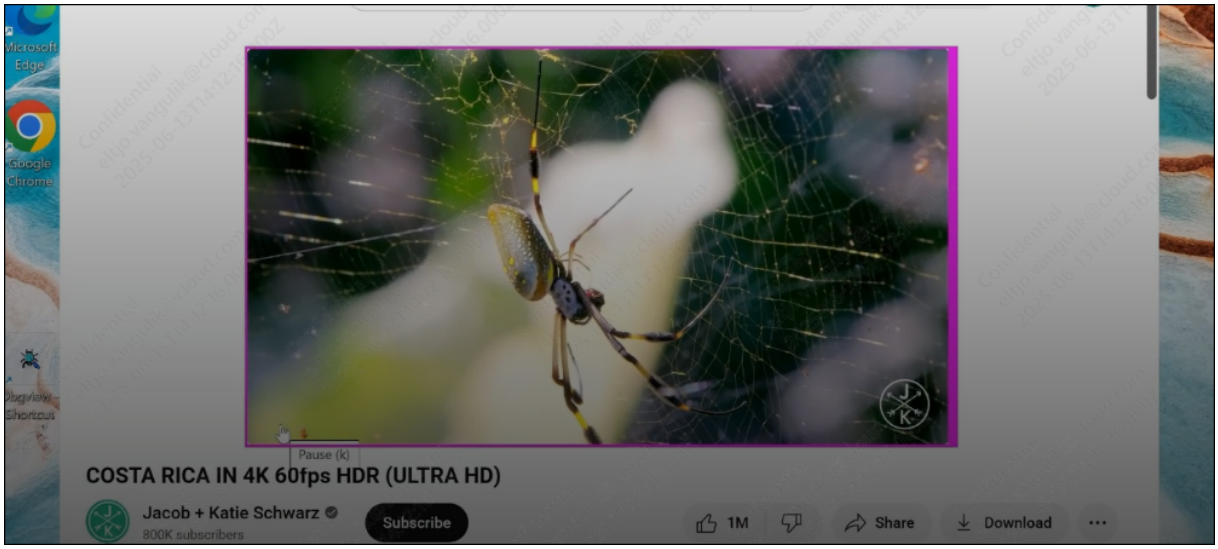
For monitoring purposes, you can enable a visual indicator that demarcates which parts of the screen are currently being upscaled by drawing a border around the video regions being upscaled. To activate the visual indicator, please enable the following registry setting on the VDA.

1. Open Windows Registry Editor (regedit.exe) on the VDA.
2. Navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\.`
3. Create a DWORD value named TwsrBorderEnabled and set the value to 1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enabling the border will show a purple border around the area that is actively being upscaled using HDX Graphics Superresolution upscaling.



To monitor the overall client performance, customers can utilise the **Performance** tab in the client's task manager.

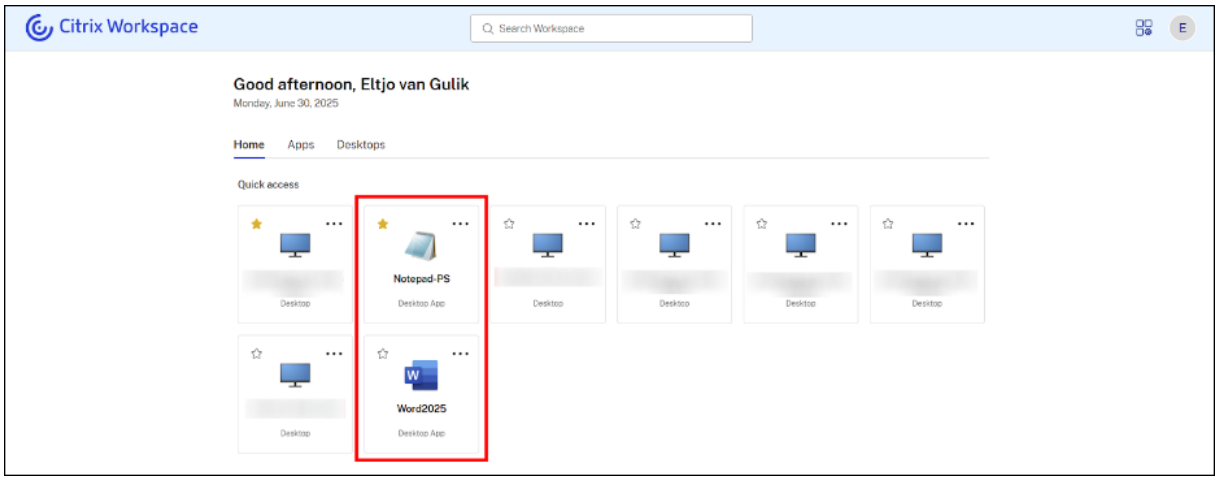
Seamless

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Published Applications are a central feature of Citrix Virtual Apps and Desktops. They enable customers to deliver individual Windows or Linux applications directly to users without requiring a full desktop.

This removes the need for users to install and manage applications locally, simplifying their workflow and easing the burden on IT. Instead of interacting with a full remote desktop environment, users interact directly with the application windows, creating a seamless and streamlined experience.



The technology behind published applications, also known as seamless applications, enables applications to be delivered to users so that they appear to be running directly on the user's local device, even though they are actually operating on a remote server. This is accomplished by concealing the Windows Server desktop where the applications are hosted and presenting the applications to the user seamlessly.

Seamless applications are available from both Windows VDA and Linux VDAs. For Windows VDAs, seamless applications support TSVDA, running Microsoft Windows Server Operating Systems, as well as WSVDA, running Microsoft Windows 10 or Windows 11.

Seamless applications offer numerous benefits, including:

- **Improved user experience:** Users can access their applications from any device without worrying about the underlying operating system.
- **Increased security:** Applications are run on a remote server, which helps protect them from malware and other threats.
- **Reduced IT costs:** Seamless applications will help to reduce IT costs by simplifying application management and deployment.
- **Centralized Management:** Applications can be managed and updated in a central location, simplifying IT administration and ensuring consistency across the organization. This reduces the time and effort required to deploy patches, updates, and new applications.
- **Application Compatibility:** By running applications on a standardized server environment, you can mitigate compatibility issues that may arise from different client operating systems or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

hardware configurations.

- **Streamlined Application Delivery:** Citrix leverages advanced technologies like HDX™ to deliver a rich, interactive experience to users, even over limited bandwidth connections for both published desktops as well as published applications.
- **Heterogeneous application support:** Admins can publish Linux applications alongside Windows applications, allowing seamless access to application from both platforms.

Applications

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Introduction

If your deployment uses only delivery groups (and not application groups), you add applications to the delivery groups. If you also have application groups, generally you add applications to the application groups instead. This guidance provides easier administration. An application must always belong to 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 Web 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.

For details, see:

- Create delivery groups
- Create application groups
- Tags

Add applications

You can add applications when you create a delivery group or application group. Those procedures are detailed in Create delivery groups and Create application groups. 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.

To add one or more applications:

1. Select **Applications** in the left pane and then select **Add Applications** in the action bar.
2. The Add Applications wizard launches with an **Introduction** page, which you can remove from future launches of this wizard.
3. The wizard guides you through the **Groups**, **Applications**, and **Summary** pages. When you are done with each page, click **Next** until you reach the **Summary** page.

Alternatives to step 1 if you want to add applications to a single delivery group or application group:

- **To add applications to only one delivery group:** In step 1, select **Delivery Groups** in the Web Studio left pane, select a delivery group in the middle pane, and then select **Add Applications** in the action bar. The wizard does not display the **Groups** page.
- **To add applications to only one application group:** In step 1, select **Applications** in the Web Studio left pane, select an application group in the middle pane, and then select the **Add Applications** entry under the application group's name in the action bar. The wizard does not display the **Groups** page.

Groups page

This page lists all the delivery groups in the site. If you have also created application groups, the page lists the application groups and delivery groups. You can choose from either group, but not from both groups. In other words, you cannot add applications to an application group and a delivery group at the same time. Generally, if you are using application groups, add applications to application groups, rather than delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When adding an application, select the check box next to at least one delivery group (or application group, if available). Every application must always be associated with at least one group.

Applications page

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 check boxes of applications to add, and then click **OK**.

  This source cannot be selected if you (1) selected application groups with no associated delivery groups, (2) selected application groups with associated delivery groups that contain no machines, or (3) selected a delivery group containing no machines.

- **Manually:** Applications located 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 check boxes of applications to add and then click **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**. For more information, see Deploy and deliver App packages.

- **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 check boxes 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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` already exists in the **Applications** folder, and you attempt to add another application named `app` to that folder, the new name `app_1` is offered.

Summary page

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.

Review the summary information and then click **Finish**.

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 (1) the delivery group contains shared machines and was created with a XenDesktop 7.x version earlier than 7.9, and (2) you have `Edit delivery group` permission. The delivery

© 1997–2026 Citrix Systems, Inc. All rights reserved.

group type is automatically converted to `desktops and applications` when the properties dialog is committed.

1. Sign in to Web Studio, select **Applications** in the left pane, and then select the application.
2. Select **Properties** in the action bar.
3. Select the **Groups** page.

    - 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 group association would result 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select one or more applications in the middle pane and then select the appropriate task in the action bar.
3. Confirm the action, when prompted.

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.
2. Select a delivery group. In the lower middle pane, on the **Applications** tab, select the application you want to remove.
3. Select **Remove Application** 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 in the middle pane, and then select one or more applications.
3. Select **Remove from Application Group** in the action bar.
4. Confirm the removal.

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 **Edit Application Properties** in the action bar.
3. Select the page containing the property you want to change.
4. When you are finished, click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the following list, the page is shown in parentheses.

Property	Page
Category/folder where application appears in Citrix Workspace app	Delivery
Command line arguments; see Pass parameters to published applications	Location
Delivery groups and application groups where the application is available	Groups
Description	Identification
File name extensions and file type association: which extensions the application opens automatically	File Type Association
Icon	Delivery
Keywords for StoreFront™	Identification
Limits; see Configure application limits	Delivery
Name: Names seen by the user and by the administrator	Identification
Path to executable; see Pass parameters to published applications	Location
Shortcut on user's desktop: enable or disable	Delivery
Visibility: Limits which users can see the application in Citrix Workspace app. An invisible application can still be started. To make it unavailable and invisible, add it to a different group.	Limit Visibility
Working directory	Location

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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.
- **Maximum number of simultaneous instances per machine, and using tag restrictions:** Application `Charlie` has licensing and performance requirements that dictate how many

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 will be 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 **Edit Application Properties** in the action bar.
3. On the **Delivery** page, choose one of the following options.
    - **Allow unlimited use of the application**. 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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For guidance, use the `Get-Help` cmdlet. For example:

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

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 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 executed, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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]\LogoffCheckerBloc` 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 [ID] 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:

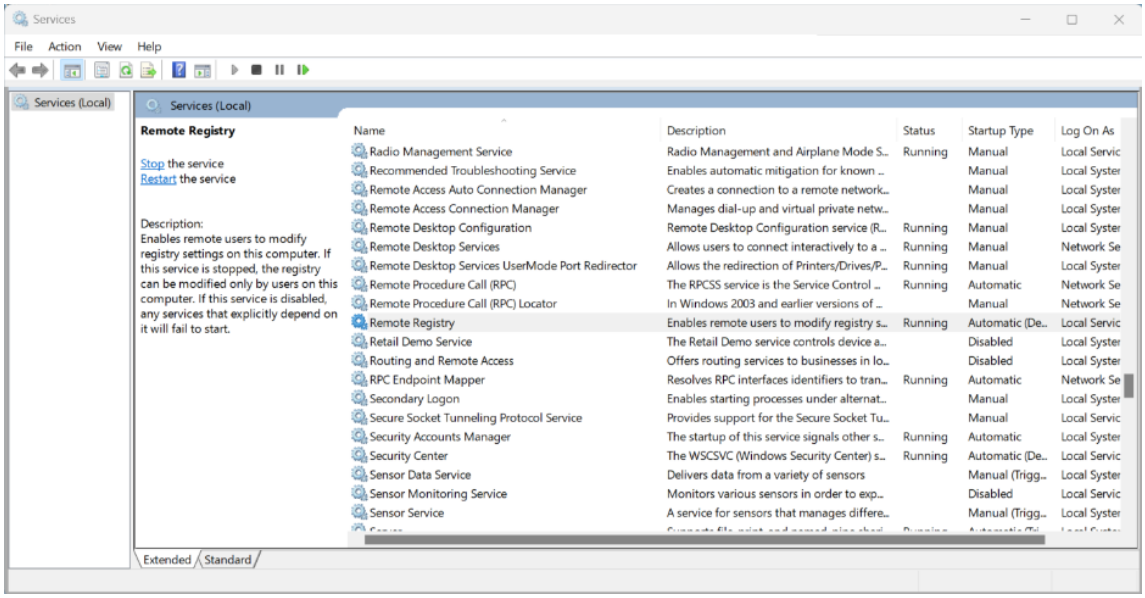
```
Add the process file name to the following registry key:
Caution! Refer to the Disclaimer at the end of this article before
   using the Registry Editor.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI
Value Name:LogoffCheckSysModules
Type:REG_SZ
String:MyAppName.exe
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information about `LogoffCheckSysModules`, see Graceful logoff from a published application renders the session in an active state.

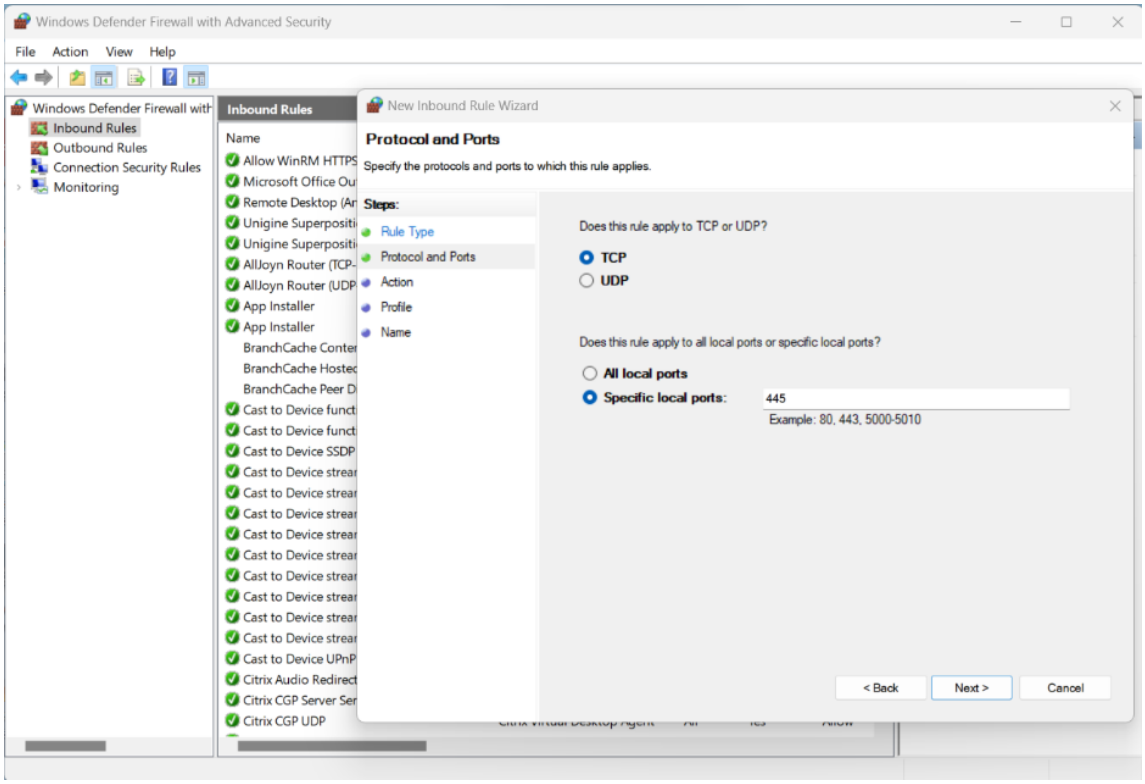
Step-by-step troubleshooting guide

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.

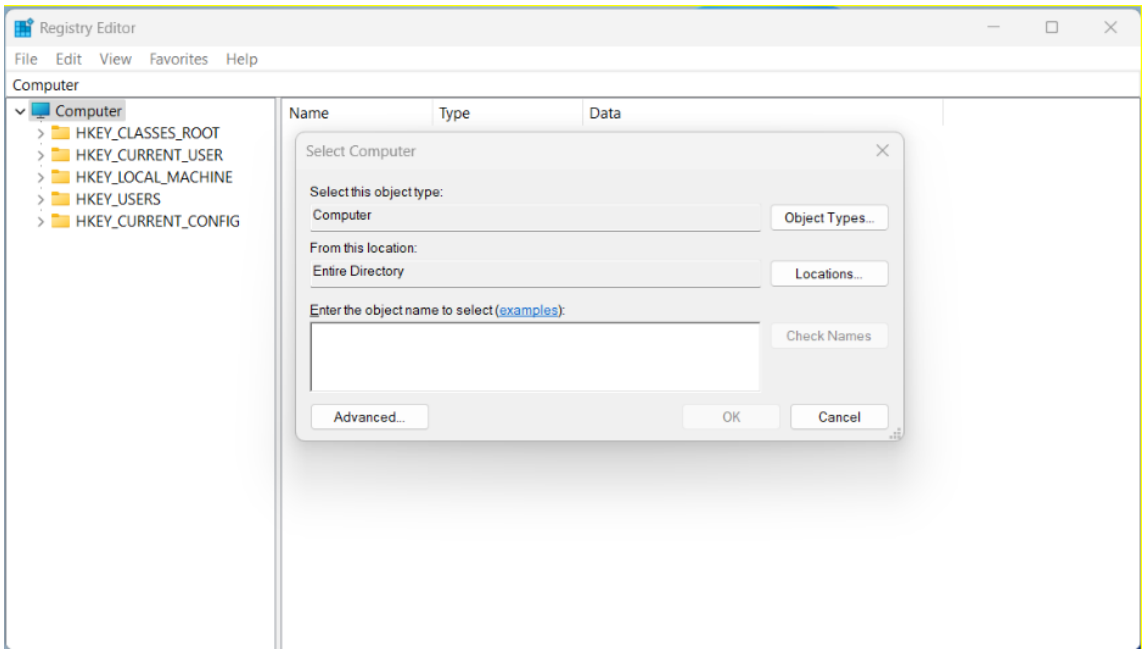


2. Turn off the Windows Firewall on the VDA under test or create an inbound firewall rule to enable port 455:
   a) In the Control Panel, select **Windows Defender Firewall > Advanced Settings**.
   b) Right-click **Inbound Rules** and select **New Rule**.
   c) In **New Inbound Rule Wizard**, select **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.

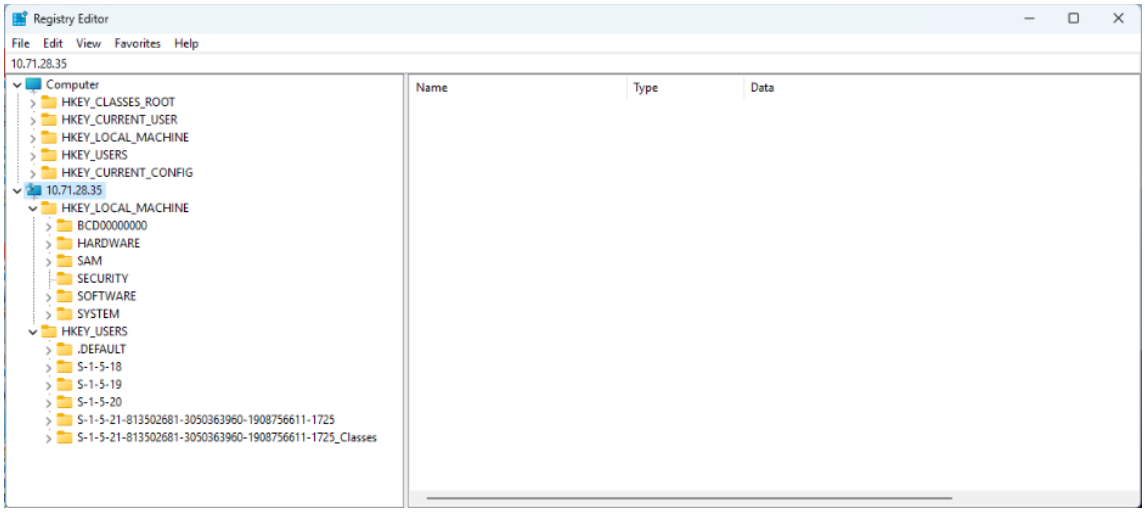


3. From another VM on the same domain (it could be DC, DDC, or another VDA), run `Regedit` and connect to a remote registry.

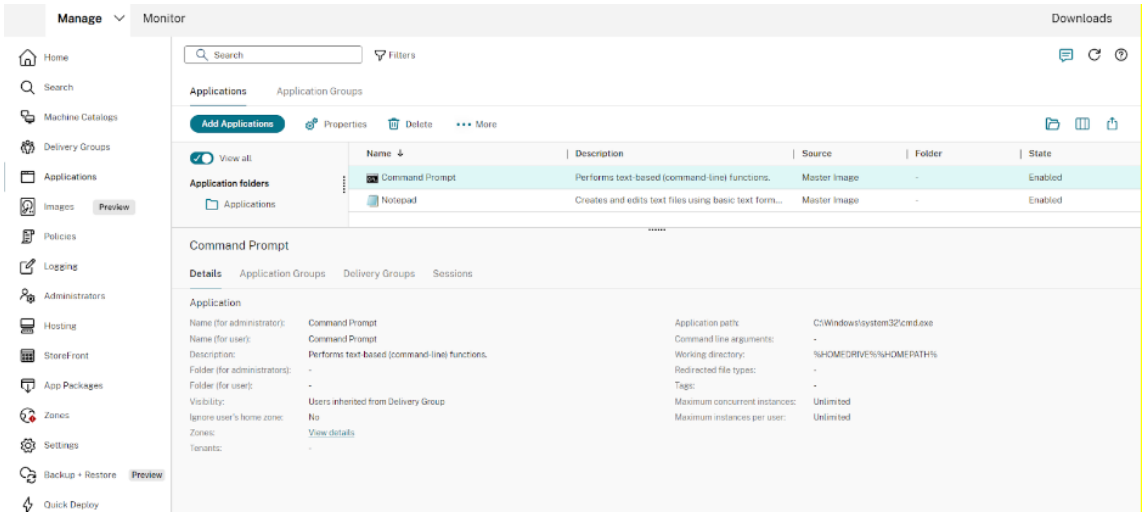


4. Enter the IP address of the VDA under test and click **OK**. The `regedit` tree must display branches for the VDA under test.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

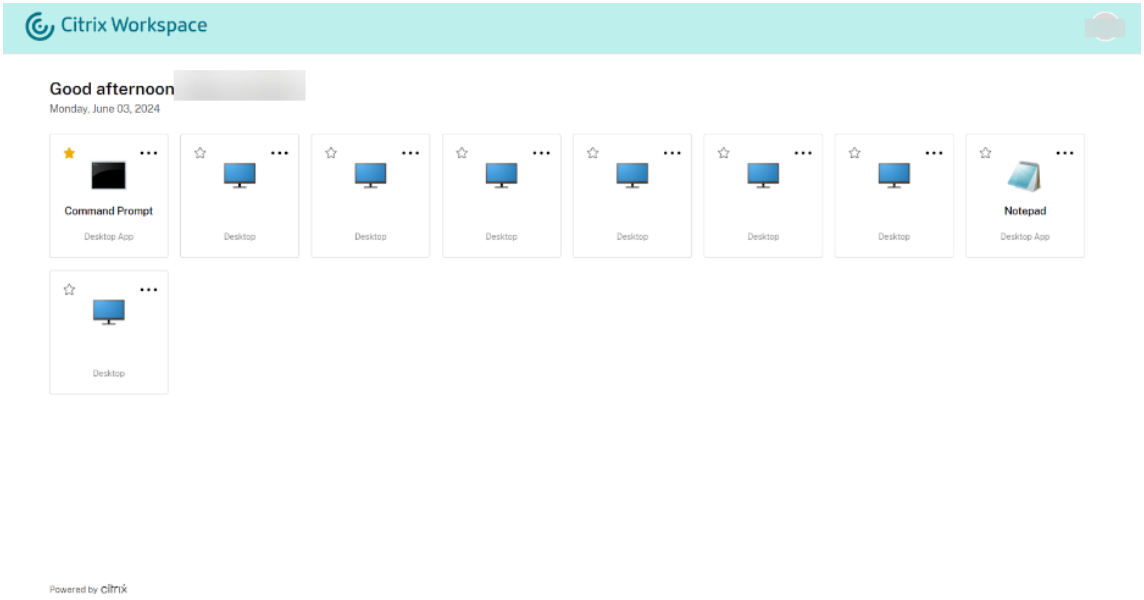


5. Open the **Command Prompt** published application.



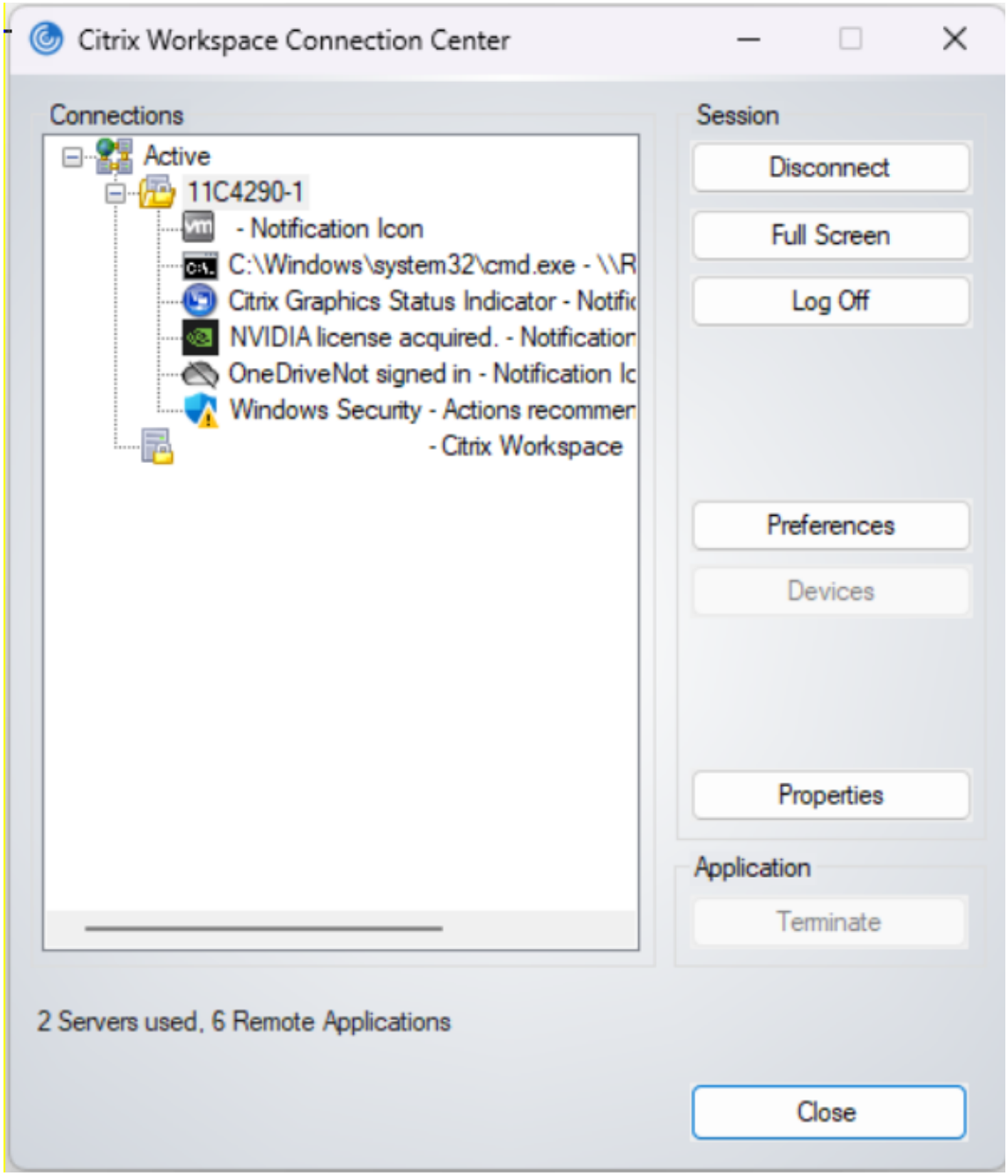
The **Command Prompt** app is displayed on Citrix Workspace.

© 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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\`

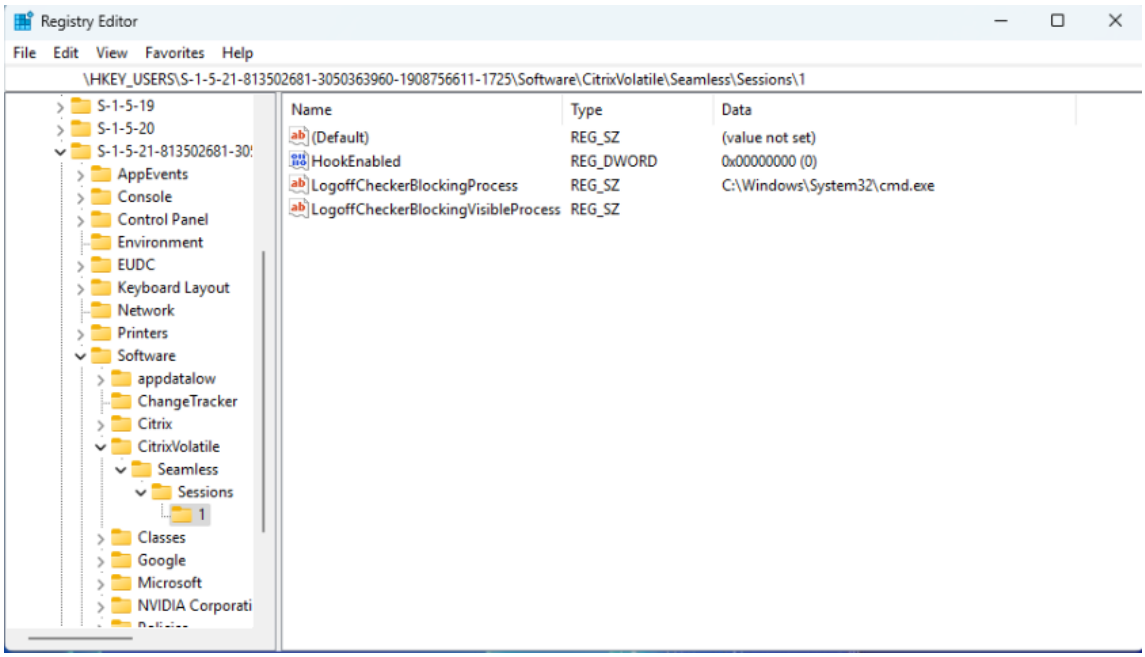
   > **Note:**
   >
   > This path changes every time you open a new session.

8. There are two keys to read here (do not change them here): **LogoffCheckBlockingProcess** and **LogoffCheckerBlockingVisibleProcess**. These keys display any programs that are blocking

© 1997–2026 Citrix Systems, Inc. All rights reserved.

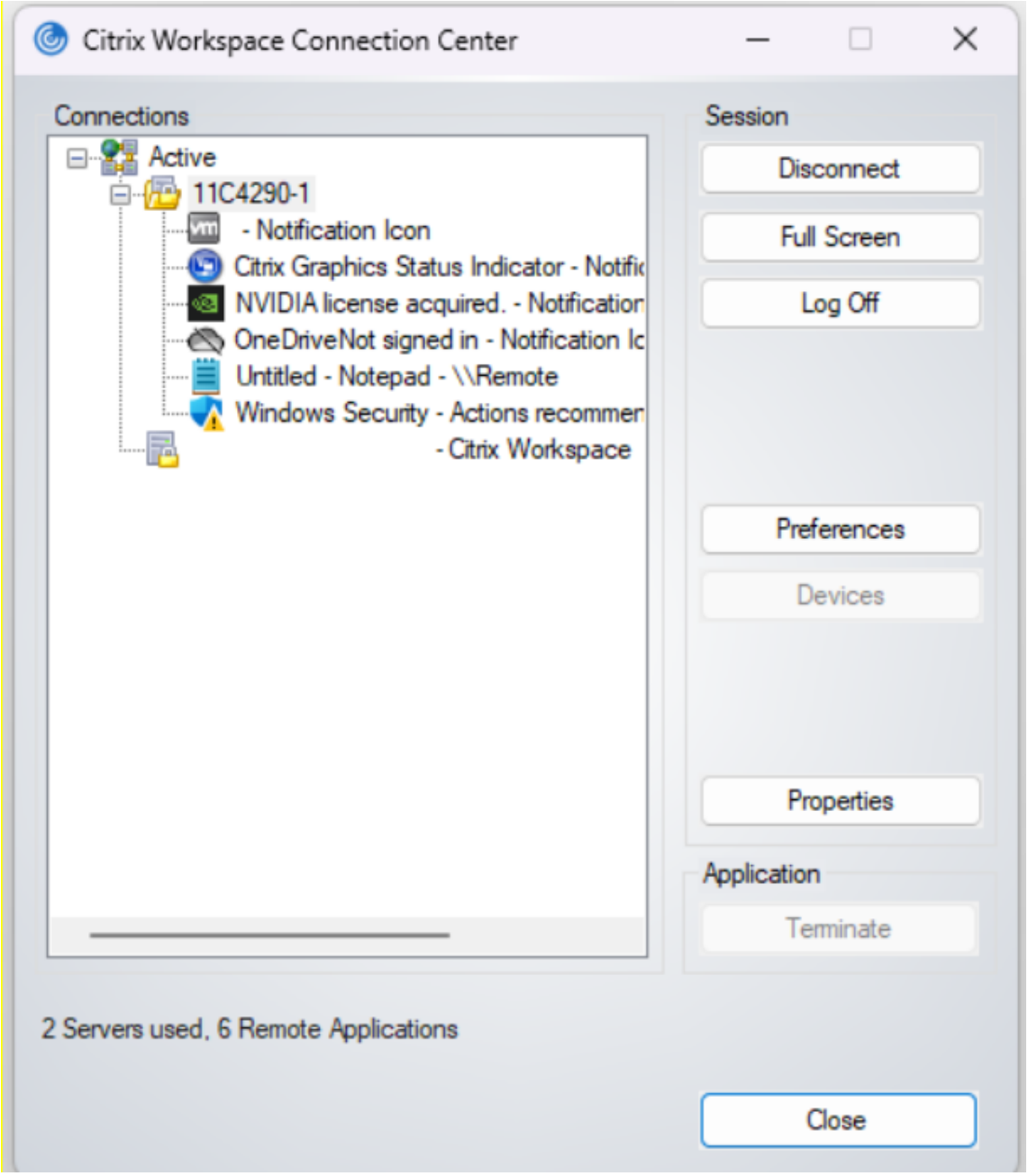
sign-out. The first one must display `C:\Windows\System32\cmd.exe` since that was open and has not been closed yet.

> **Note:**
>
> **LogoffCheckBlockingProcess** and **LogoffCheckerBlockingVisibleProcess** must not be manually edited. Manually editing these registry values could 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.

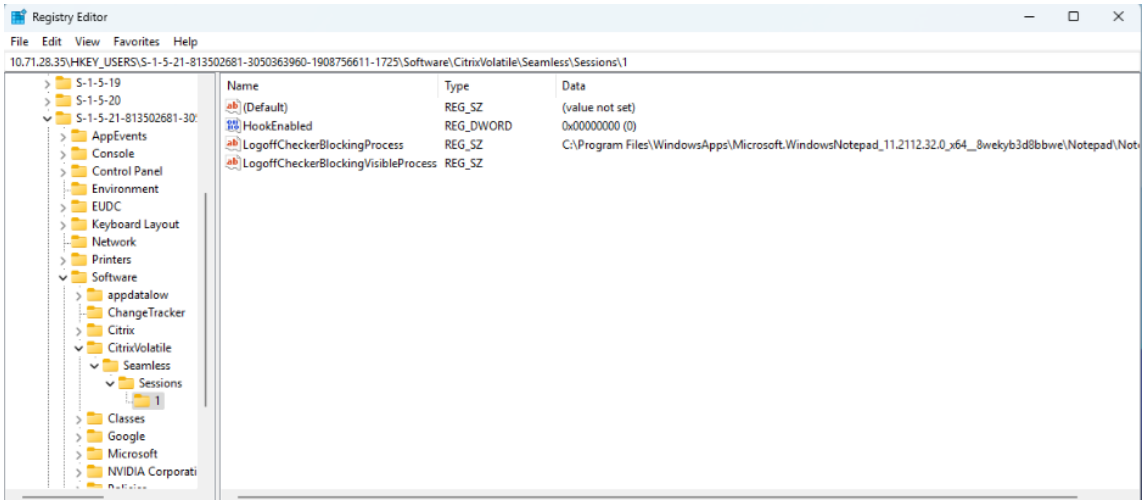
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

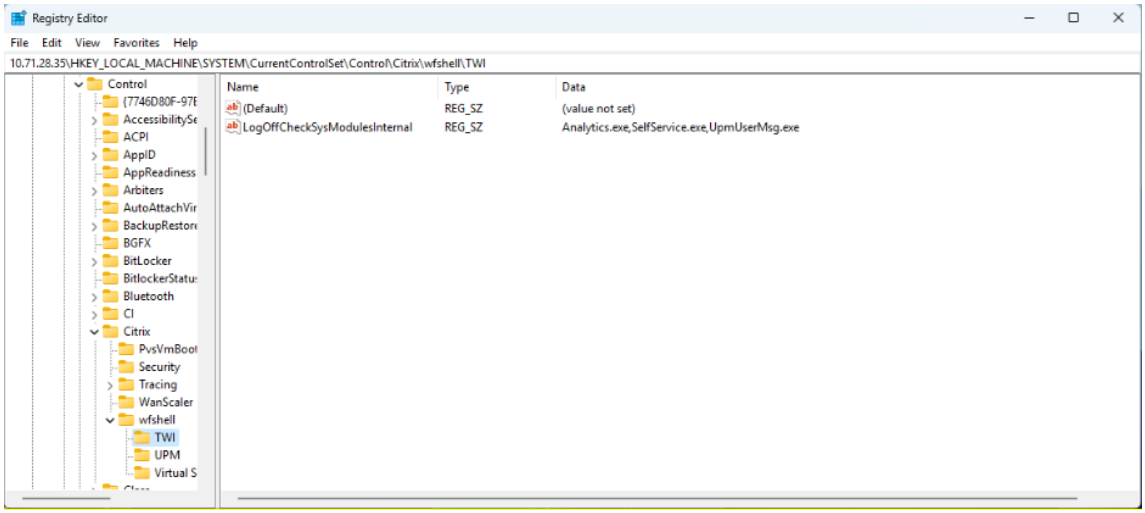
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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\TWILogoffCheckSysModulesInternal`
    - 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.
15. Repeat steps 9-16 until the session is signed out automatically within 30 seconds of closing the Remote Application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

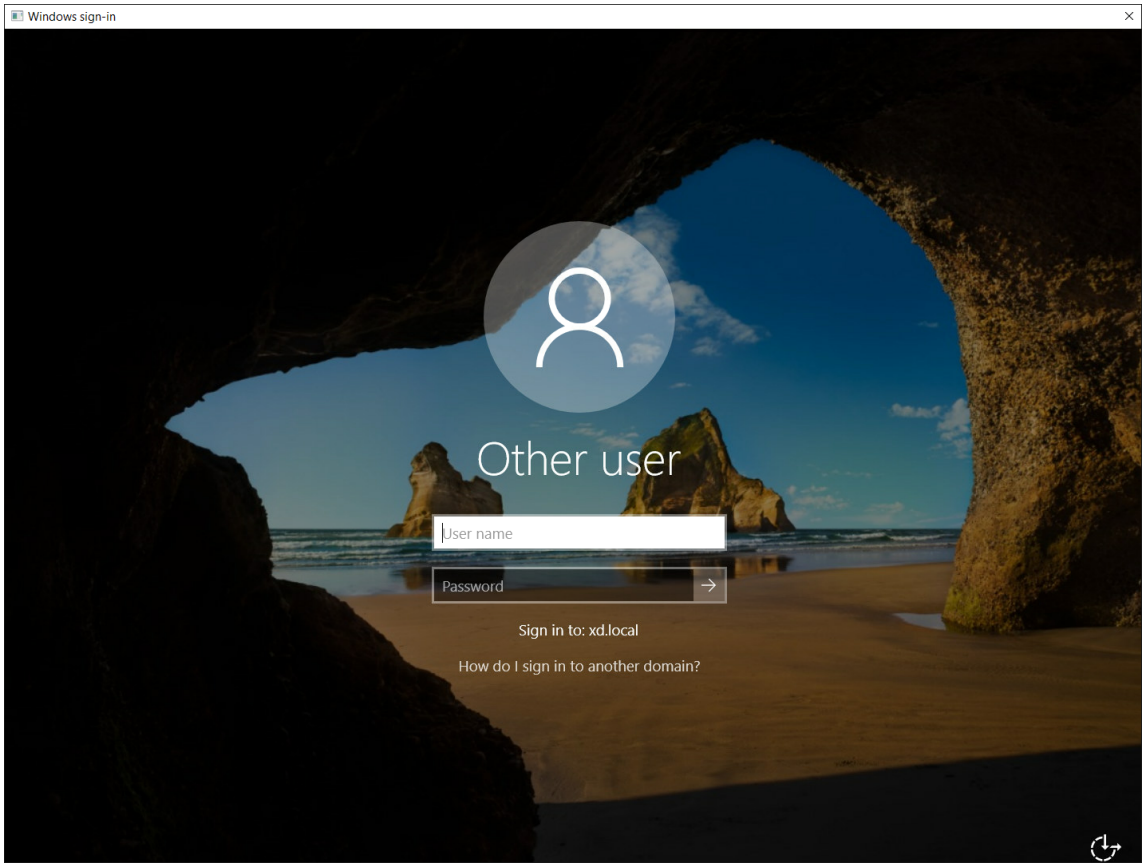
By default, the **LogonUI** window includes a title bar with a close button which enables the end user to disconnect from the session if needed.

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 Web 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.
- **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Create application groups

September 13, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Introduction

Application groups let you manage collections of applications. Create application groups for applications shared across different delivery groups. Or, applications 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. Associate delivery groups with more than one application group, and associate an application group with more than one delivery group.

Using application groups can provide application management and resource control advantages over using more delivery groups:

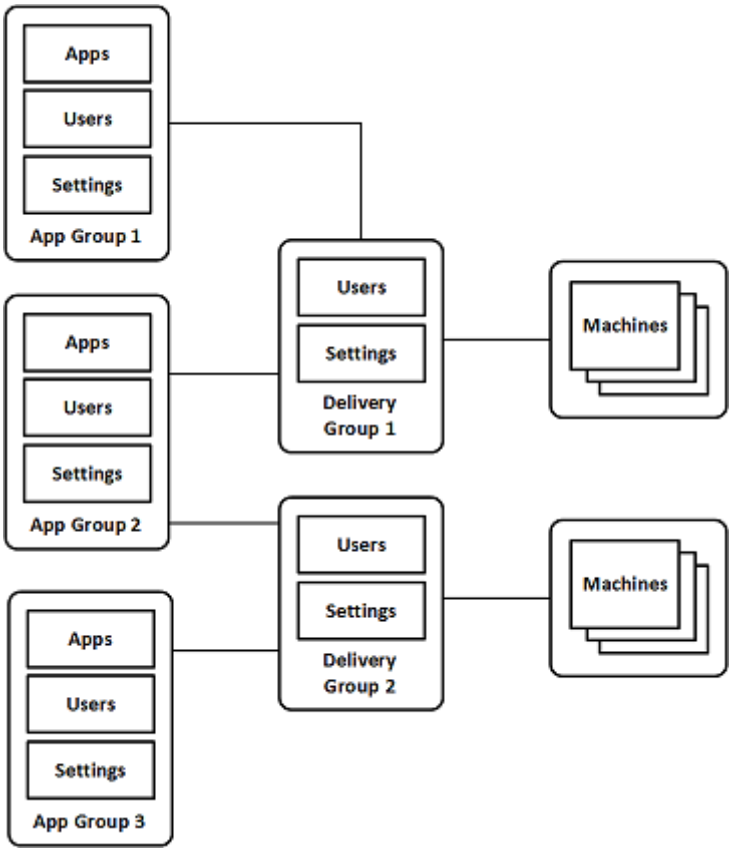
- The logical grouping of applications and their settings lets you manage those applications as a single unit. For example, you don't have to add (publish) the same application to individual delivery groups one at a time.
- Session sharing between application groups can conserve resource consumption. In other cases, disabling session sharing between application groups can be beneficial.
- 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 extra 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 Citrix Virtual Apps and Desktops deployment that includes application groups:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this configuration, applications are added to the application groups, not the delivery groups. The delivery groups specify which machines are used. (Although not shown, the machines are in machine catalogs.)

Application group 1 is associated with delivery group 1. Access the applications in application group 1 by the users specified in application group 1. These groups only appear as long as they are also in the user list for delivery group 1. This configuration follows the guidance that the user list for an application group is 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 groups) apply to applications and users in that group. The settings in delivery group 1 apply to users in application groups 1 and 2, because those application groups have been associated with that delivery group.

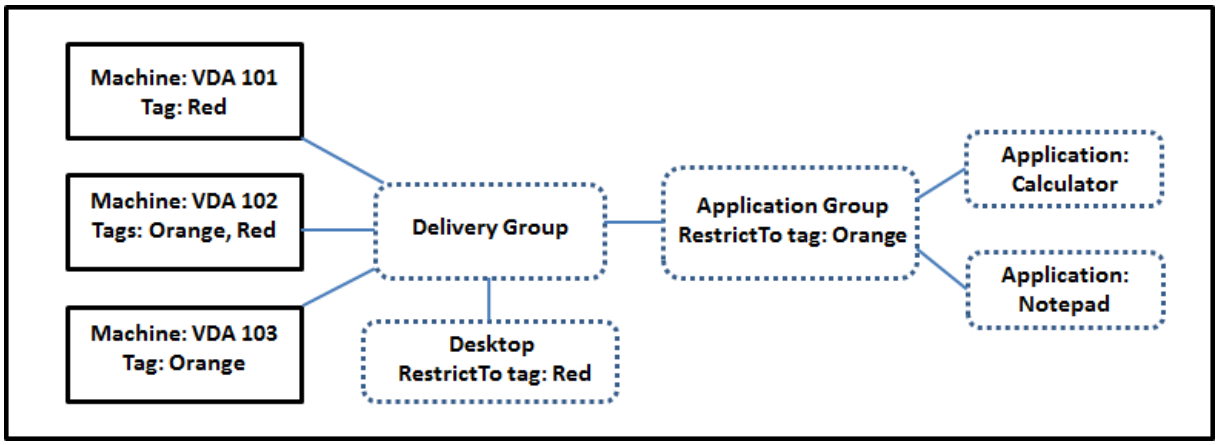
Application group 2 is associated with two delivery groups: 1 and 2. Each of those delivery groups is assigned a priority in application group 2, indicating the order in which the delivery groups are checked when an application is launched. Delivery groups with equal priority are load balanced. Access the applications in application group 2 by the users specified in application group 2. However, they must also appear in the user lists for delivery group 1 and delivery group 2.

Example 2:

This simple layout uses tag restrictions to limit which machines are considered for certain desktop

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. Each of its applications is 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.

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 process requires:

1. Upgrading VDAs on the machines used in the delivery group.
2. Upgrading the machine catalogs containing those machines.
3. Upgrading 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This article refers to "associating" an application with more than one application group. It differentiates that action from adding instances of that application from an available source. Similarly, delivery groups are associated with application groups, 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 more application sessions, and allows the use of application features that involve the clipboard, such as copy-paste operations. However, in some situations you can clear 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.

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 controller finds that 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:**

  A configuration with 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. The user can still run other applications at the same time, but not in the same session. When launching one of the different-versioned applications, or any application that is not contained in an application group, 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.

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.

By default, application session sharing is enabled when you create an application group. You cannot change this setting 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

To create an application group:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Sign in to Web Studio.
2. Select **Applications** in the left pane, and then select the **Application Groups** tab.
3. To organize application groups using folders, create folders under the **Application Groups** root folder. For more information, see Organize application groups using folders.
4. 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.
5. 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 that you can select. Compatible delivery groups contain random (not permanently or statically assigned) multi-session or single-session OS machines.
- The **Incompatible Delivery Groups** list contains delivery groups that you cannot select. Each entry explains why it is not compatible, such as containing statically 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 application 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. Also, you cannot add applications to the application group from the **From Start** menu source if there are no delivery groups specified.

The delivery groups that you select specify the machines that are used to deliver applications. Select the check boxes next to the delivery groups that 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 drop-down list.

Step 2. Users

Specify application users in the application group. Either allow all users and user groups in the delivery groups that you selected on the previous page, or select specific users and user groups from those delivery groups. If you restrict use to specified users, then only the users specified in the delivery group, the application group can access the applications in this 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 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 Web Studio. Otherwise, users see duplicate names in 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.

Click the **Add** from the drop-down menu 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 click **OK**.

  This source cannot be selected if you selected any of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - 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 defined:** 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, click **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 click **OK**. This source cannot be selected If the site has no applications.
- **App-V**: Applications in App-V packages. When you select this source, a new page launches where you select **App-V server** or **Application Library**. From the resulting display, select the check boxes of applications to add, and then click **OK**. For more information, see Deploy and deliver App-V applications. This source cannot be selected (or might not appear) if App-V is not configured for the site.

As noted, certain entries in the **Add** drop-down menu are not 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.

Step 5. Summary

Enter a name for the application group. You can also (optionally) enter a description.

Review the summary information and then click **Finish**.

Publish content

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

You can publish an application that is simply a URL or UNC path to a resource, such as a Microsoft Word document or a web link. This feature is known as published content. The ability to publish content adds flexibility to how you deliver content to users. You benefit from the existing access control and management of applications. You can also specify whether to use local or published applications to open the content.

The published content appears just like other applications in StoreFront™ and Citrix Workspace™ app. Users access it in the same way they access applications. On the client, the resource opens as usual.

- If a locally installed application is appropriate, it is launched to open the resource.
- If a File Type Association has been defined, a published application launches to open the resource.

You publish content using the PowerShell SDK. You cannot use Web Studio to publish content. However, you can use Web Studio to edit application properties later, after they are published.

Configuration overview and preparation

Publishing content uses the `New-BrokerApplication` cmdlet with the following key properties. (See the cmdlet help for descriptions of all cmdlet properties.)

```
1 New-BrokerApplication –ApplicationType PublishedContent -
    CommandLineExecutable location -Name app-name -DesktopGroup delivery
    -group-name
```

The `ApplicationType` property must be `PublishedContent`.

The `CommandLineExecutable` property specifies the location of the published content. The following formats are supported, with a limit of 255 characters.

- HTML website address (for example, http://www.citrix.com)
- Document file on a web server (for example, `https://www.citrix.com/press/pressrelease.doc`)
- Directory on an FTP server (for example, `ftp://ftp.citrix.com/code`)
- Document file on an FTP server (for example, `ftp://ftp.citrix.com/code/Readme.txt`>)
- UNC directory path (for example, `file://myServer/myShare or \\\\\myServer\\myShare`)
- UNC file path (for example, `file://myServer/myShare/myFile.asf` or `\\myServer\myShare\myFile.asf`)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ensure that you have the correct SDK.

- For Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) deployments, download and install the Citrix Virtual Apps and Desktops Remote PowerShell SDK.
- For on-premises Citrix Virtual Apps and Desktops deployments, use the PowerShell SDK that is installed with the Delivery Controller. Adding a published content application requires a minimum version 7.11 Delivery Controller.

The following procedures use examples. In the examples:

- A machine catalog has been created.
- A delivery group named `PublishedContentApps` has been created. The group uses a multi-session OS machine from the catalog. The WordPad application has been added to the group.
- Assignments are made for the delivery group name, the `CommandLineExecutable` location, and the application name.

Get started

On the machine containing the PowerShell SDK, open PowerShell.

The following cmdlet adds the appropriate PowerShell SDK snap-in, and assigns the returned delivery group record.

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

If you are using Citrix DaaS, authenticate by entering your Citrix Cloud™ credentials. If there is more than one customer, choose one.

Publish a URL

After assigning the location and application name, the following cmdlet publishes the Citrix home page as an application.

```
1 $citrixUrl = "https://www.citrix.com/"
2 $appName = "Citrix Home Page"
3
4 New-BrokerApplication –ApplicationType PublishedContent –
    CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
    Uid
```

Verify success:

- Open StoreFront and log on as a user who can access applications in the PublishedContentApps delivery group. The display includes the newly created application with the default icon. To

© 1997–2026 Citrix Systems, Inc. All rights reserved.

learn about customizing the icon, see https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.

- Click the **Citrix Home Page** application. The URL launches in a new tab in a locally running instance of your default browser.

Publish resources located at UNC paths

In this example, the administrator has already created a share named `PublishedResources`. After assigning the locations and application names, the following cmdlets publish an RTF and a DOCX file in that share as a resource.

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf
    "
$rtfAppName = "PublishedRTF"

New-BrokerApplication  –ApplicationType PublishedContent
 –CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.
    docx"
$docxAppName = "PublishedDOCX"

New-BrokerApplication  –ApplicationType PublishedContent
 –CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
```

Verify success:

- Refresh your StoreFront window to see the newly published documents.
- Click the **PublishedRTF** and **PublishedDOCX** applications. Each document opens in a locally running WordPad.

View and edit PublishedContent applications

You manage published content using the same methods that you use for other application types.

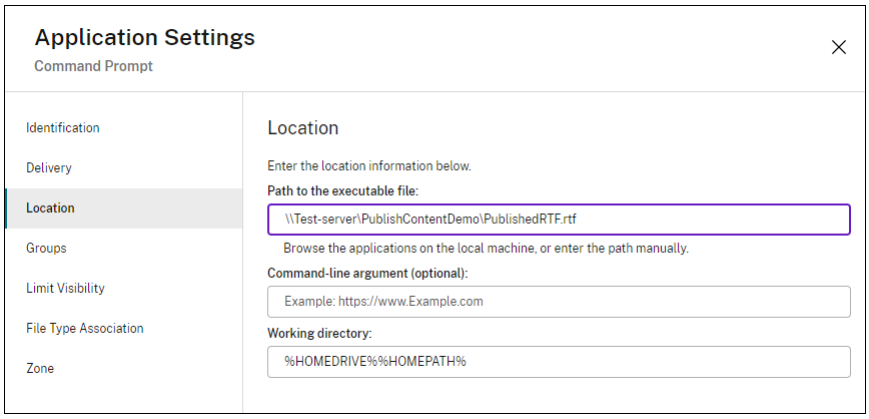
To view and edit `PublishedContent` applications, follow these steps:

1. Sign in to Web Studio and select **Applications** in the left pane.
2. On the **Applications** tab, select a PublishedContent application, and then select **Properties**.

   Application properties (such as user visibility, group association, and shortcut) apply to the published content. However, you cannot change the command-line argument or working directory properties on the **Location** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. To change the resource, modify the **Path to the executable file** field on that page.



4. To use a published application to open a `PublishedContent` application (rather than a local application), follow these steps:

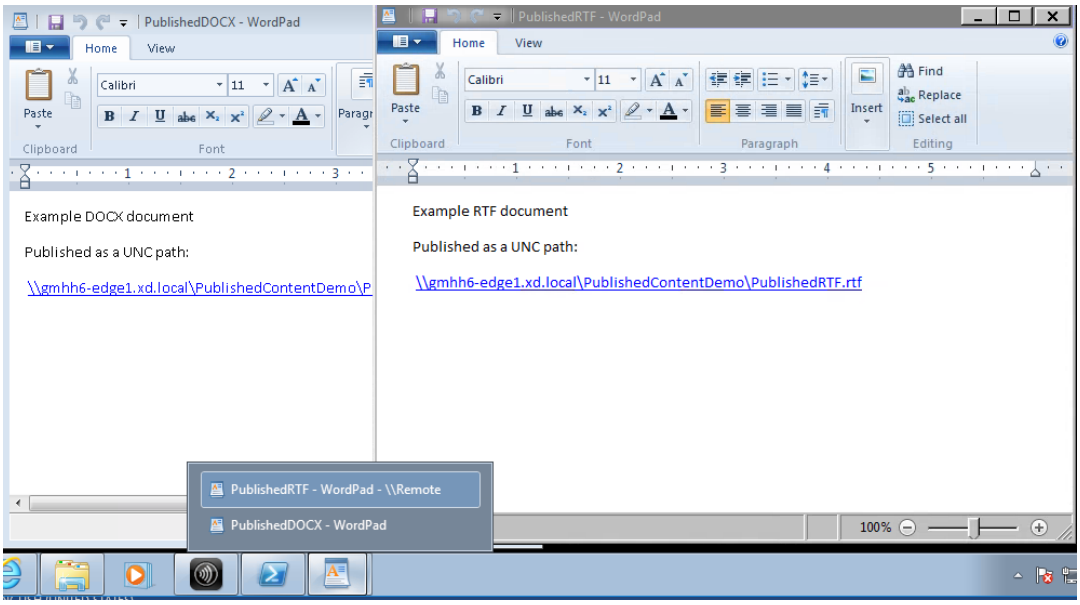
   In this example, the published WordPad application is edited to create a File Type Association for .rtf files.

   a) Turn on maintenance mode for the delivery group.

   b) Edit the **File Type Association** property.

   c) Turn off maintenance mode when you're done.

   d) Refresh StoreFront to load the File Type Association changes, and then click the **PublishedRTF** and **PublishedDOCX** applications. Notice the difference. **PublishedDOCX** still opens in the local WordPad. However, **PublishedRTF** now opens in the published WordPad due to the file type association.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information

- Create machine catalogs
- Create delivery groups
- Change application properties

App packages

January 5, 2026

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

This article walks you through how to deploy and deliver these packaged applications in your Citrix Virtual Apps and Desktops™ environment.

> **Note:**
>
> - You can manage your Citrix Virtual Apps and Desktops deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.
> - We don't recommend using Web Studio and Citrix Studio interchangeably for deploying and delivering app packages. Each uses different mechanisms, which can lead to discrepancies, such as App-V server information appearing correctly in one but not the other. Also, note that Citrix Studio supports only App-V.

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 Virtual Apps and Desk-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

tops 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.
- **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:

  1. User SID
  2. Username
  3. AD Group SID (First found wins)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. AD Group Name (First found wins)
5. 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
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 Virtual Apps and Desktops and App-V servers work together to deliver and manage packages. This method requires Citrix Virtual Apps and Desktops to periodically refresh the snapshot view of the App-V server's state. It incurs hardware, infrastructure, and administration overhead. Citrix Virtual Apps and Desktops 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 Virtual Apps and Desktops 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.

> **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 sources. The **Package type** column indicates which technology is used to deliver the package and where they are referenced in the **Application Library**. When you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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 Virtual Apps and Desktops 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.

> **Note:**
>
> - We support native MSIX Packages on Desktop and server VDAs and MSIX app attach on `.vhd`, `.vhdx`, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deploy and deliver app packages

Prerequisites

To support the delivery of App-V, MSIX, MSIX app attach and FlexApp packages, 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, and FlexApp 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.
- 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.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. Accept any prompts that appear.

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.
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.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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:
  - The connecting entity must be a user account, not a machine account, as Azure AD 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Preparations Citrix Virtual Apps and Desktops 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:
  - 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
- 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 **Sources** tab, click the **Add Source** button. The **Add Source** page appears.
3. In the **Name** field, enter a descriptive name for the package source.
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** or **Network share** based on where you store the packages, and then complete the corresponding settings:
   - If you select **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.
     - 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\`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select the package types that you want to upload. Options include App-V, MSIX, MSIX app attach, and FlexApp.
- 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.

6. Click **Add Source**.

   The **Add Source** page closes and the newly added source appears in the source list. Citrix Virtual Apps and Desktops uploads the packages to your environment 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 source location and import them to your environment, select the location in the source list and click **Check for Package Updates**.

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. Click **Add Package**.

   The application package appears on the **Packages** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 one or more applications in the package as needed, and then click **Next**.
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.

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 source 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.

When a user starts an App-V application marked as *Explicit* in an isolation group, Citrix Virtual Apps and Desktops 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- 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

Automate packaged application publishing

You can use PowerShell commands to automate packaged application publishing:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Virtual Apps and Desktops ISO on the path mentioned in step 1.

2. The package discovery module must be from the ISO of a Citrix Virtual Apps and Desktops 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:

```
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 Virtual Apps and Desktops 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

> **Note:**
>
> Packaged Applications published to Single Session Static desktops are never available in Workspace App regardless of the value configured in this setting.

Universal Windows Platform Apps

September 13, 2025

For information about Universal Windows Platform (UWP) apps, see the following Microsoft documentation:

- What's a Universal Windows Platform (UWP) app?
- Windows Package Manager

Requirements and limitations

Citrix Virtual Apps and Desktops™ supports the use of UWP apps with VDAs on the following Windows machines:

- Windows 10 and later versions
- Windows Server 2016 and later versions

VDAs must be minimum version 7.11.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following Citrix Virtual Apps and Desktops features are either not supported or limited when using UWP apps:

- File type association is not supported.
- Local App Access is not supported.
- Dynamic preview: If apps running in the session overlap, the preview shows the default icon. The Win32 APIs used for Dynamic Preview are not supported in UWP apps.
- Action Center remoting: UWP apps can use the Action Center for displaying the messages in the session. These messages are currently not redirected to the endpoint to be displayed to the user.

Launching UWP apps and non-UWP apps from the same server is not supported. Instead, place UWP apps and non-UWP apps in separate delivery groups or application groups.

Because all UWP apps installed on the machine are enumerated, Citrix® recommends disabling user access to the Windows Store. This precludes the UWP apps installed by one user from being accessed by a different user.

During sideloading, the UWP app is installed on the machine and is available for use by other users. When another user launches the app, then it is installed, and the OS updates its AppX database to indicate "as installed"by that user.

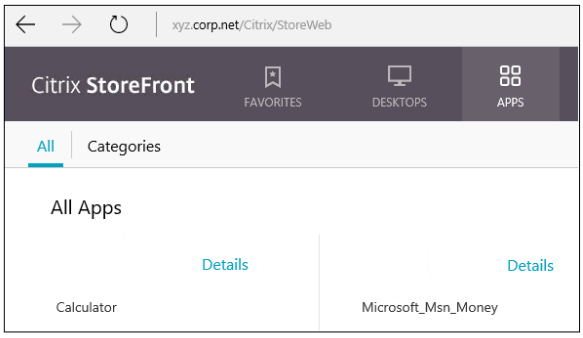
A graceful logoff started from a published UWP app that was launched in a fixed or seamless window might prevent the VDA session from closing and forcibly log off the user. When this occurs, several processes remaining in the VDA session prevent it from properly closing. To resolve this, determine which process is preventing the VDA session from closing, and then add it to the "LogoffCheckSysModules"registry key value, following the guidance in CTX891671.

Application Display Names and Descriptions for UWP apps might not have correct names. Edit and correct these properties when adding the applications to the delivery group.

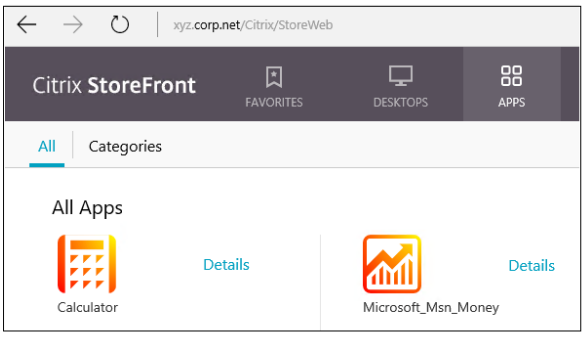
Check Known issues for any additional issues.

Currently, several UWP apps have white icons with transparency enabled, which results in the icon not being visible against the white background of the StoreFront display. To avoid this issue, you can change the background. For example, on the StoreFront machine, edit the file `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`. At the end of the file, add `.storeapp-icon { background-image: radial-gradient( circle at top right, yellow, red ); }`. The following graphic illustrates the before-and-after for this example.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Before



After

On Windows Server 2016 and later versions, the Server Manager might also launch when a UWP app is launched. To prevent this from occurring, you can disable Server Manager from auto-starting during logon with the `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon` registry key. For details, see https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/.

Install and publish UWP apps

Support for UWP apps is enabled by default.

To install one or more UWP apps on VDAs (or a master image), use one of the following methods:

- Complete an offline install from the Windows Store for Business, using a tool such as Deployment Image Servicing and Management (DISM) to deploy the apps to the desktop image. For more information, see Windows Package Manager.
- Sideload the apps. For more information, see Sideload line of business (LOB) apps in Windows client devices.
- Install the UWP apps for each intended user directly from the Windows Store for Business.

To add (publish) one or more UWP apps in Citrix Virtual Apps or Citrix Virtual Desktops™:

1. After the UWP apps are installed on the machine, add the UWP apps to a delivery group or application group. You can do this when you create a group, or later. On the **Applications** page, in the **Add** menu, select **From Start menu**.
2. When the applications list appears, select the UWP apps you want to publish.
3. Continue with the wizard or close the edit dialog.

To disable the use of Universal Apps on a VDA, add the registry setting **EnableUWASeamlessSupport** in `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` and set to **0**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Uninstall UWP apps

When you uninstall a UWP app with a command such as `Remove-AppXPackage`, the item is uninstalled only for administrators. To remove the app from the machines of users who may have launched and used the app, run the removal command on each machine. You cannot uninstall the AppX package from all users' machines with one command.

Publish applications

August 5, 2025

With Linux VDA Version 7.13, Citrix added the seamless applications feature to all the supported Linux platforms. No specific installation procedures are required to use this feature.

> **Tip:**
>
> With Linux VDA version 1.4, Citrix added support for non-seamless published applications and session sharing.

Publish applications using Citrix Studio

You can publish applications installed on a Linux VDA when you create a delivery group or add applications to an existing delivery group. The process is similar to publishing applications installed on a Windows VDA. For more information, see the Citrix Virtual Apps and Desktops documentation (based on the version of Citrix Virtual Apps and Desktops being used).

> **Note:**
>
> - When configuring delivery groups, ensure that the delivery type is set to **Desktop and applications** or **Applications**.
> - We recommend that you create separate VDAs and delivery groups for app and desktop deliveries.
> - To use seamless applications, do not disable the seamless mode on StoreFront. The seamless mode is enabled by default. If you have already disabled it by setting "TWIMode=Off," remove this setting instead of changing it to "TWIMode=On."Otherwise you might not be able to launch a published desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitation

The Linux VDA does not support the launch of multiple concurrent instances of the same application by a single user.

In an app session, only shortcuts that are specific to the app work as expected.

Known issues

The following known issues are identified during publishing applications:

- Non-rectangular windows are not supported. The corners of a window might show the server-side background.
- Preview of the content of a window from a published application is not supported.
- When you run multiple LibreOffice applications, only the one launched first shows on Citrix Studio because these applications share the process.
- Published Qt5-based applications like "Dolphin"might not show icons. To resolve the issue, see the article at https://wiki.archlinux.org/title/Qt.
- Linux applications often have an About window containing information about the application in use, and web links for more information are commonly found in those windows. Clicking the web links in the About window can launch a web browser from within published applications such as **calc**, **gedit**, **calendar**, and **LibreOffice Suite**. The unintentional launch of a web browser bypasses application isolation and can compromise security. To address the issue, change the default web browser by completing the following steps:

  1. Create a none.sh file in a custom location, for example:

     ```
     sudo mkdir /home/none

     sudo touch /home/none/none.sh

     sudo chmod +x /home/none/none.sh
     ```

  2. Add the following lines to the none.sh file:

     ```
     #!/bin/bash

     echo "NONE"
     ```

  3. Create the /etc/xdg/mimeapps.list file with sudo, and then add the following lines to the mimeapps.list file:

     ```
     [Default Applications]

     text/html=none.desktop

     x-scheme-handler/http=none.desktop
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
6
7  x-scheme-handler/https=none.desktop
8
9  x-scheme-handler/about=none.desktop
10
11 x-scheme-handler/unknown=none.desktop
```

4. Create the /usr/share/applications/none.desktop file with sudo, and then add the following lines to the none.desktop file:

```
1  [Desktop Entry]
2
3  Encoding=UTF-8
4
5  Version=1.0
6
7  Type=Application
8
9  Terminal=false
10
11 Exec=/home/none/none.sh
12
13 Name=None
14
15 Icon=/home/none/none.sh
```

Because you can put the none.sh file in a custom location, make sure that none.desktop can reference the none.sh file correctly.

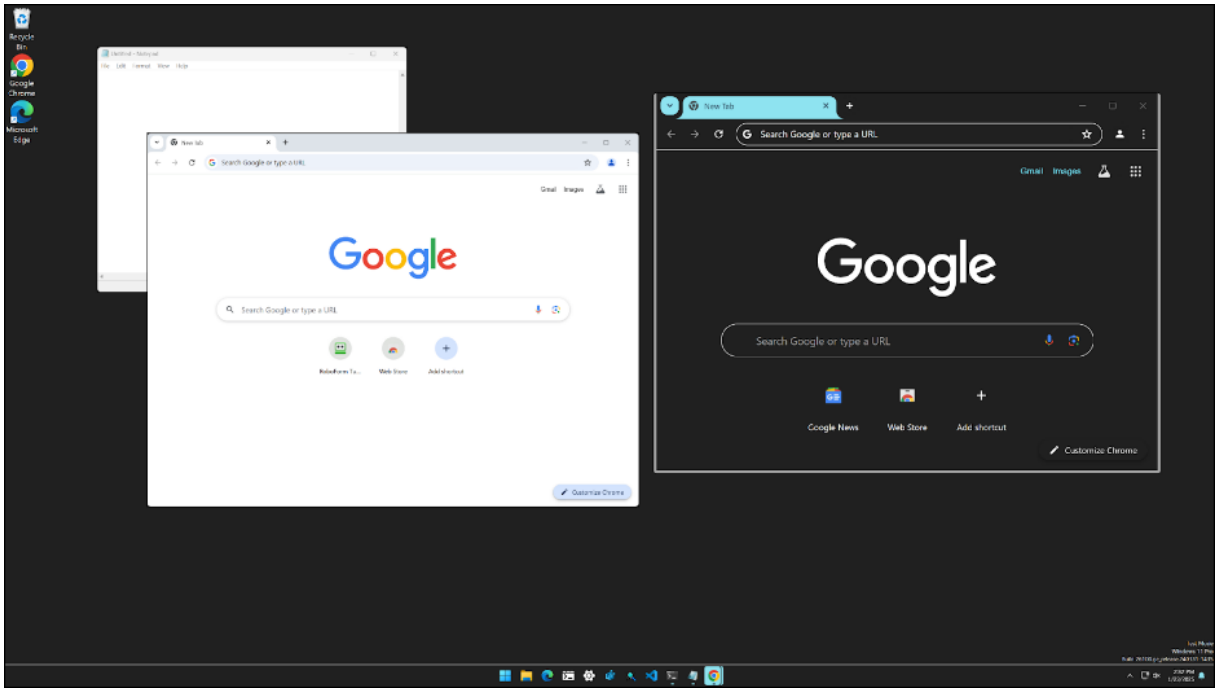
Windows Accessibility Settings

September 6, 2025

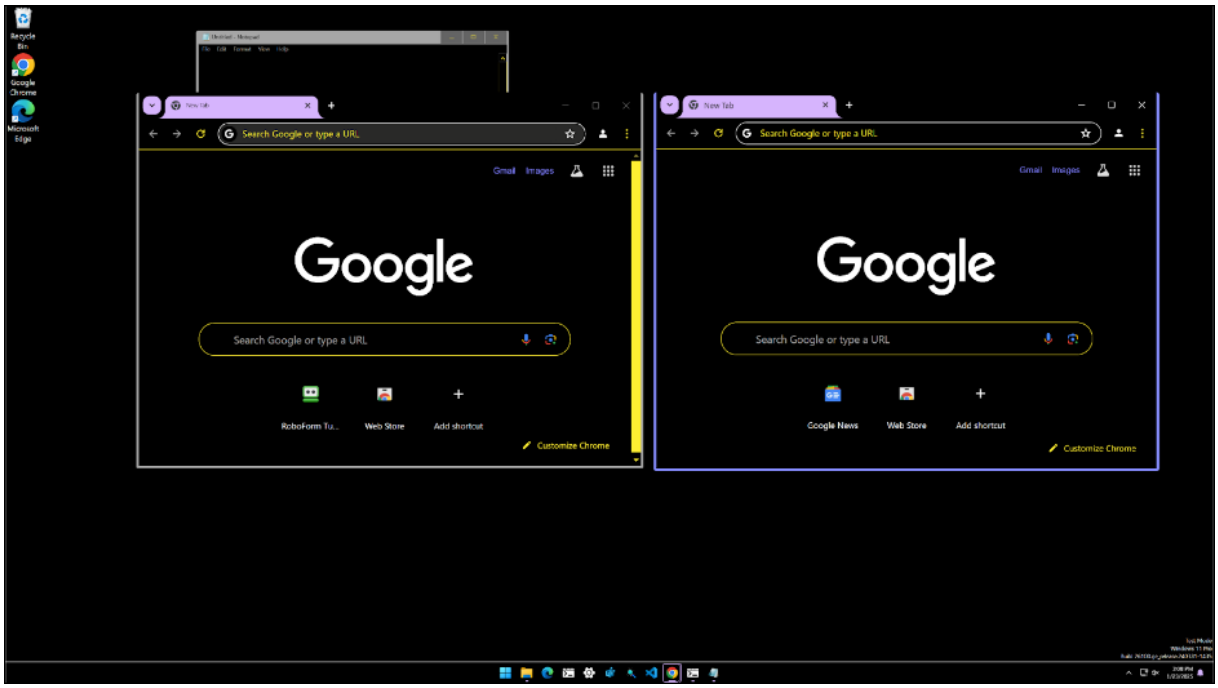
Windows Accessibility settings for Seamless Applications will automatically mirror a subset of accessibility settings from the user's local endpoint to the published app session upon launch. During the session, changes to the local endpoint's accessibility settings will be automatically applied to the remote session, when possible.

Without Windows accessibility settings for Seamless applications enabled:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



With Windows accessibility settings for Seamless applications:



Windows accessibility settings for Seamless Applications will automatically and dynamically apply the settings to the remote application during the session:

Accessibility mirroring will automatically mirror the following local accessibility settings from the user's local endpoint to the VDA. Currently, the following accessibility settings are supported:

- High contrast themes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Dark mode
- Mouse cursor size
- Text size

Prerequisites

September 6, 2025

The prerequisites for Accessibility settings for Seamless Applications are as follows:

- Windows endpoint running CWA for windows 2503 or later
- Windows VDA running VDA 2503 or later

Accessibility mirroring is available on the following VDA operating systems:

- Windows Server 2022
- Windows Server 2025
- Windows 10 Multi-session
- Windows 11 Single-session & Multi-session

And on the following client operating systems:

- Windows 10
- Windows 11

How to enable

September 6, 2025

Accessibility settings for Seamless applications is currently disabled by default.

On the VDA, Accessibility Settings for Seamless applications can be enabled with the following registry setting:

1. Open the **Windows Registry Editor** using `regedit.exe`.
2. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\`
3. Create a **DWORD** value named `AccessibilityMirroring` and set the value to **1** to enable.

With CWA 2503, Accessibility Setting for Seamless applications will also be disabled on the client by default and can be enabled with the following registry setting:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the **Windows Registry Editor** using `regedit.exe`.
2. Navigate to `HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TWI`
3. Create a **DWORD** value named `AccessibilityMirroring` and set its value to **1** to enable.

> **Note:**
>
> For Accessibility Settings for Seamless applications to function, the registry keys must be present on both the VDA and the client.
>
> No additional user intervention or configuration is required to enable the new accessibility settings for seamless applications.

Window Dragging

September 6, 2025

When interacting with seamless applications, such as window dragging, we distinguish between client-side dragging and server-side dragging. In most use cases, a client drag is preferred over a server drag. Client dragging will have a much smoother experience, and the Window dragging operation is performed locally instead of on the server.

In most cases HDX™ will automatically perform a client drag, however, certain applications might only allow for server dragging. A server drag can be identified by black bars being shown 'behind' the application while dragging the window. Selecting a different part of the titlebar will usually result in a client drag.

See below for the difference between client drag and server drag.

Applications like Google Chrome allow for their tabs to be rearranged by dragging them across.

This could, in some cases, also result in a server drag. This is expected behaviour.

Troubleshooting

September 6, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 executed, 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

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]\LogoffCheckerBloc` 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 [ID] 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:

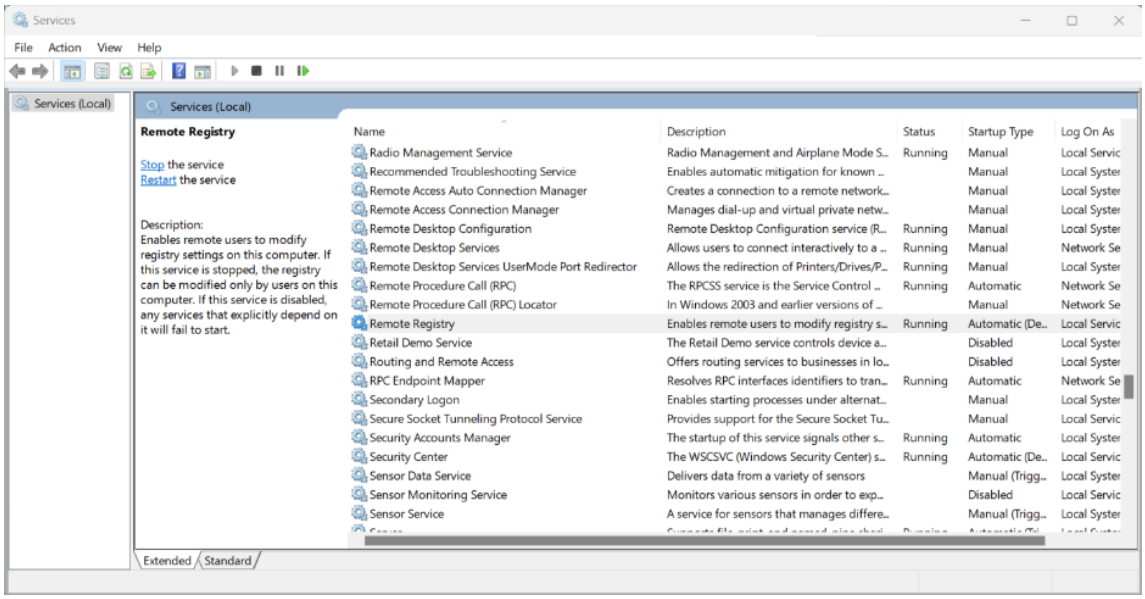
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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
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.



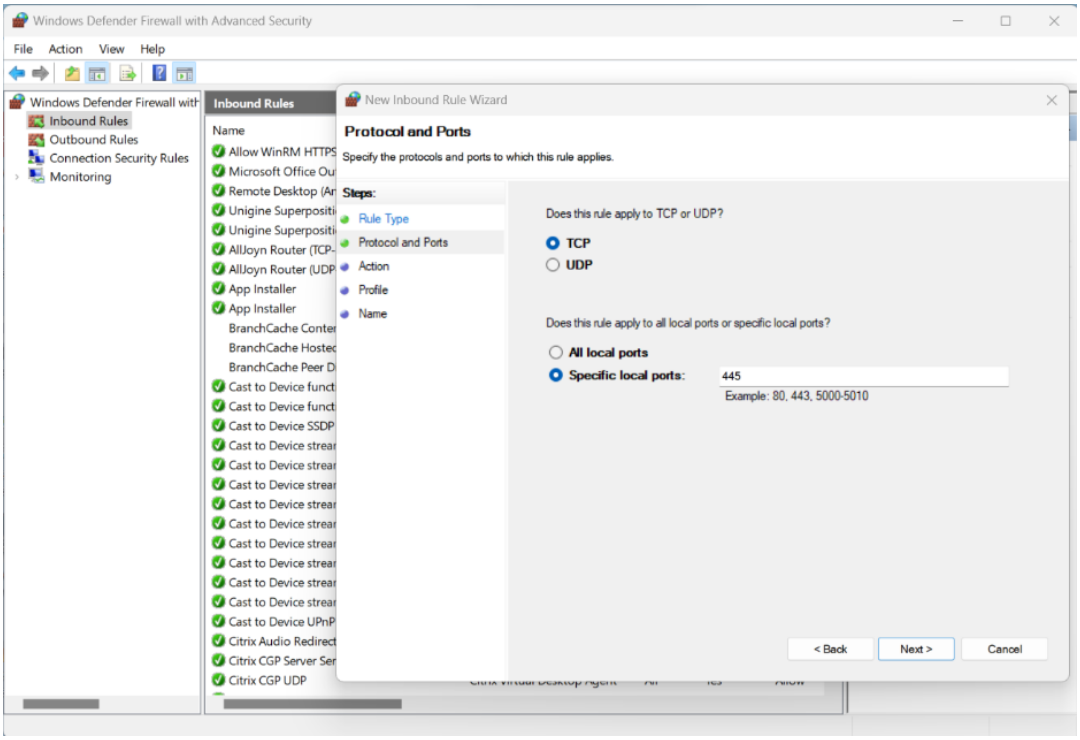
2. Turn off the Windows Firewall on the VDA under test or create an inbound firewall rule to enable port 455:
   a) In the Control Panel, select **Windows Defender Firewall > Advanced Settings**.
   b) Right-click **Inbound Rules** and select **New Rule**.
   c) In **New Inbound Rule Wizard**, select **Port**.
   d) On the **Protocols and Ports** page, select **TCP and Specific Local Ports**. Enter 445 as the local port.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

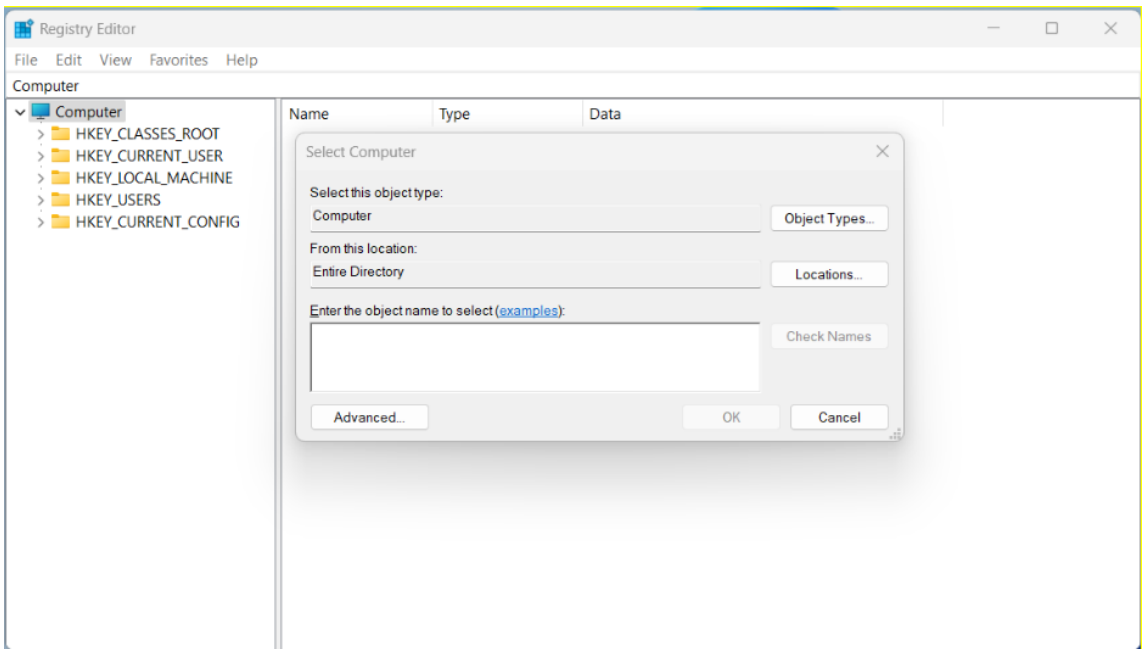
e) Select **Allow Connection** on the **Action** page.

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**.

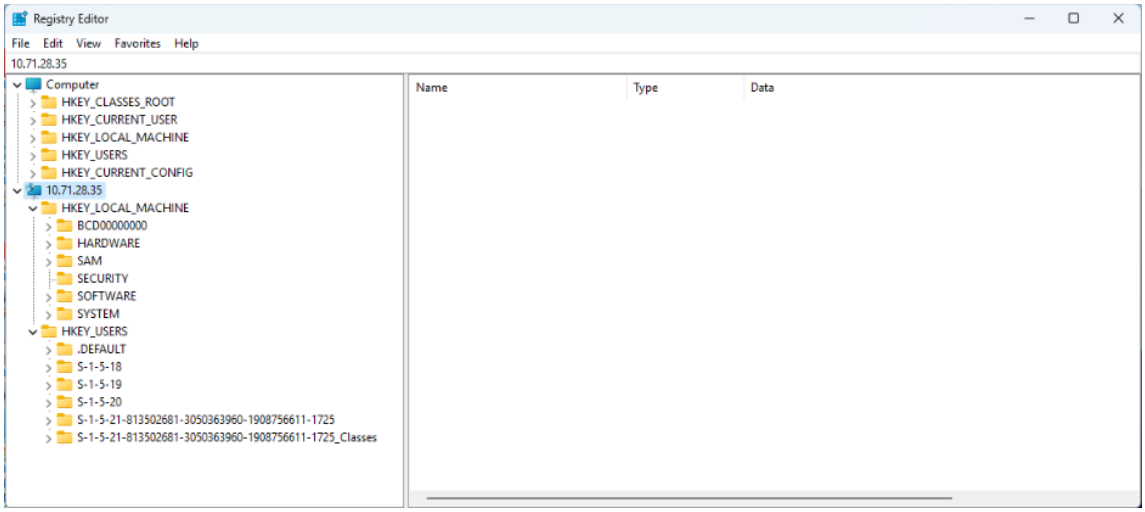


3. From another VM on the same domain (it could be DC, DDC, or another VDA), run `Regedit` and connect to a remote registry.

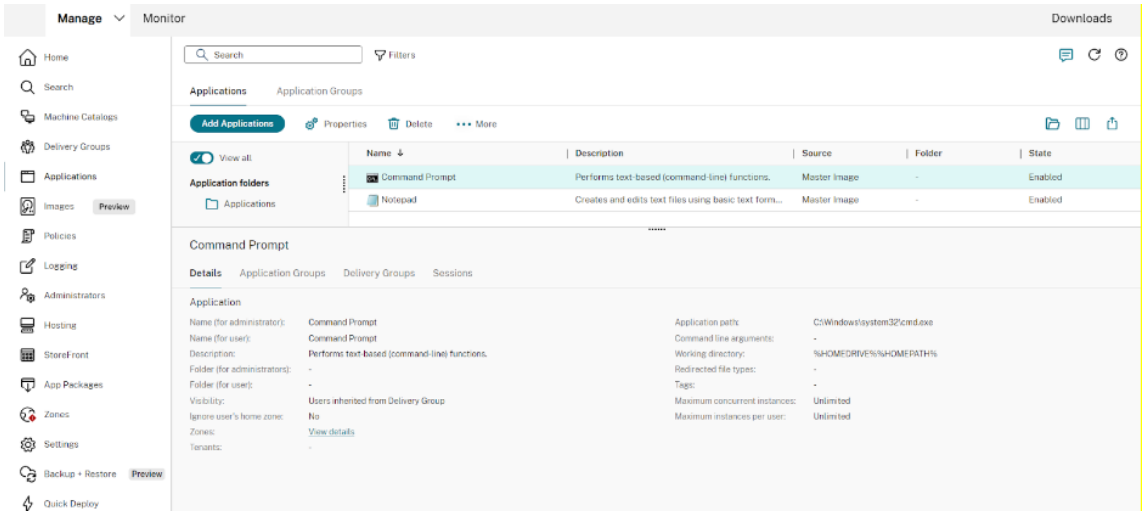


© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Enter the IP address of the VDA under test and click **OK**. The `regedit` tree must display branches for the VDA under test.

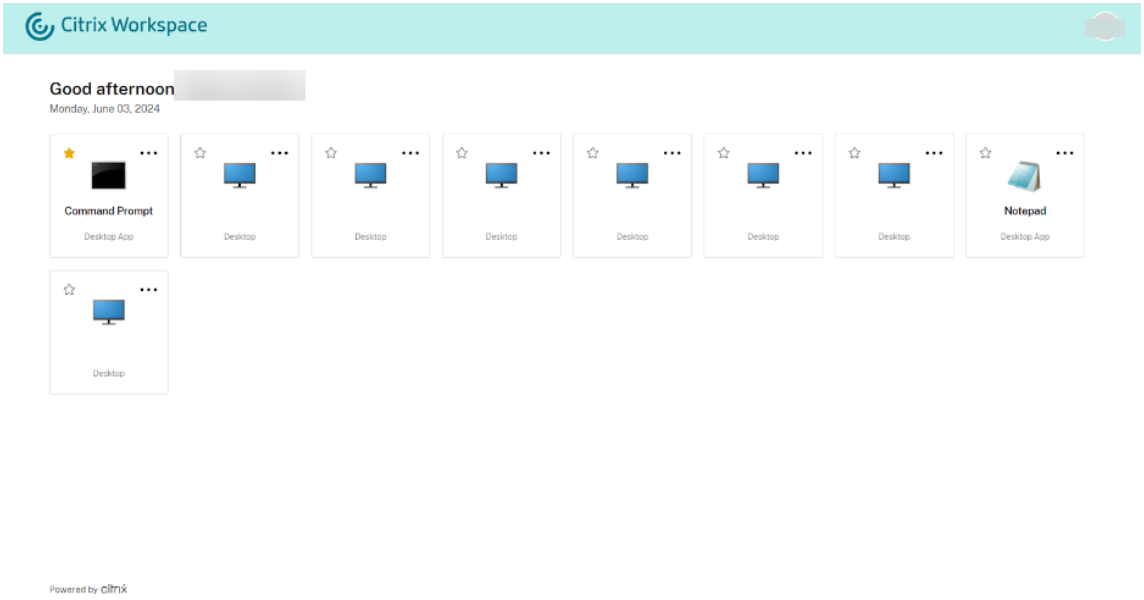


5. Open the **Command Prompt** published application.



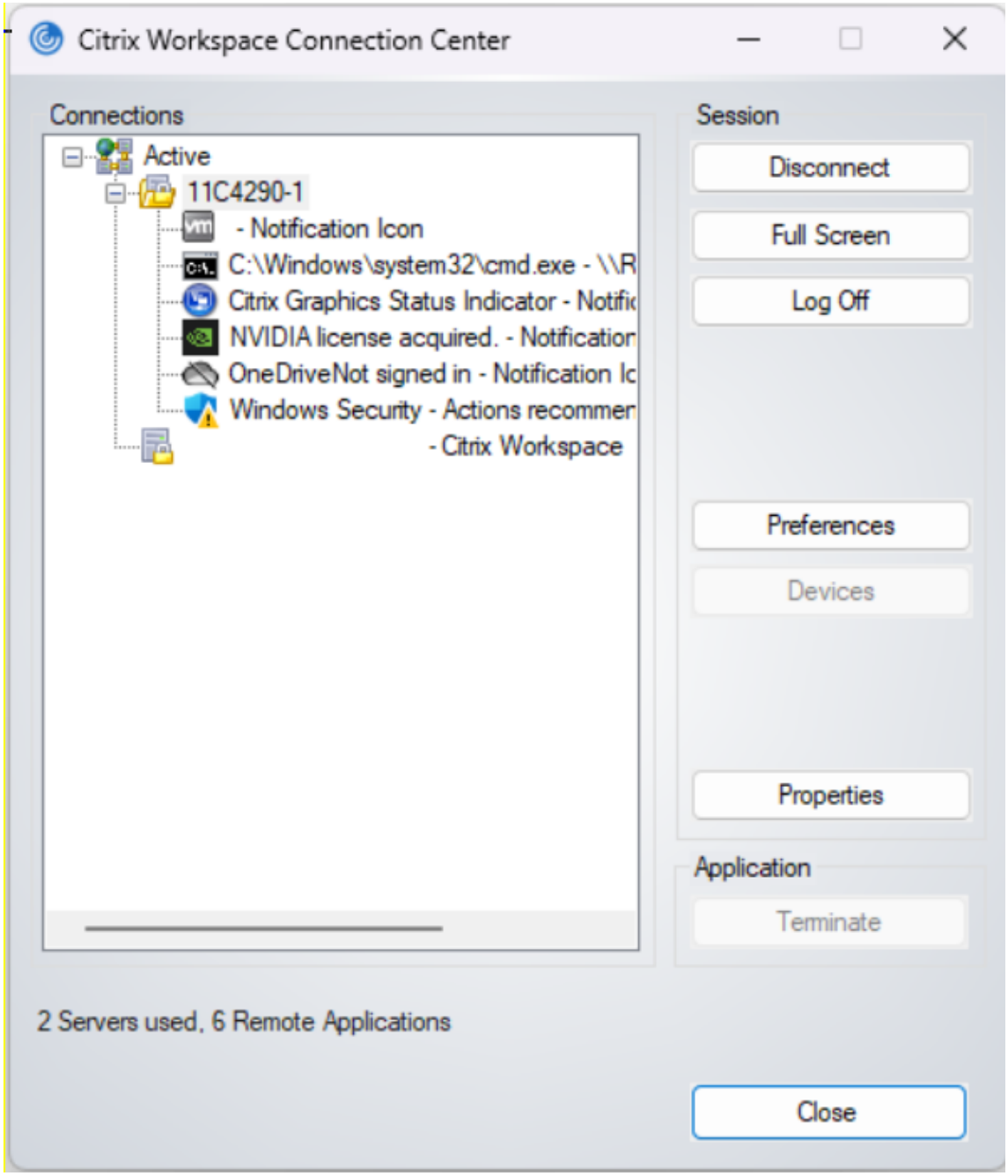
The **Command Prompt** app is displayed on Citrix Workspace.

© 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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\`

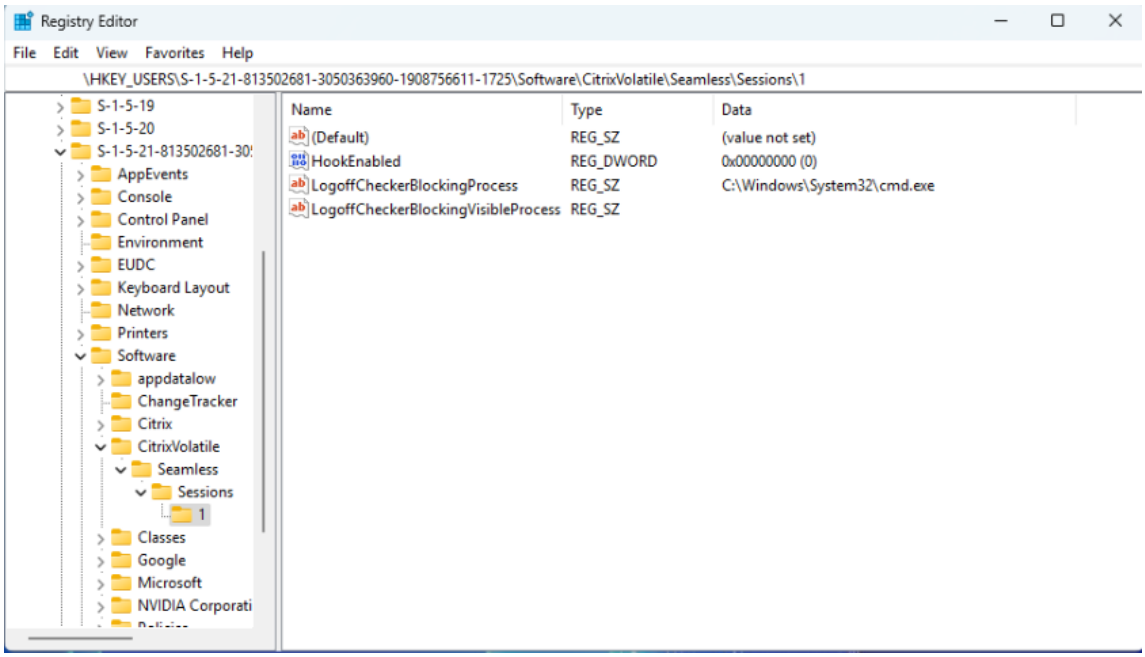
   > **Note:**
   >
   > This path changes every time you open a new session.

8. There are two keys to read here (do not change them here): **LogoffCheckBlockingProcess** and **LogoffCheckerBlockingVisibleProcess**. These keys display any programs that are blocking

© 1997–2026 Citrix Systems, Inc. All rights reserved.

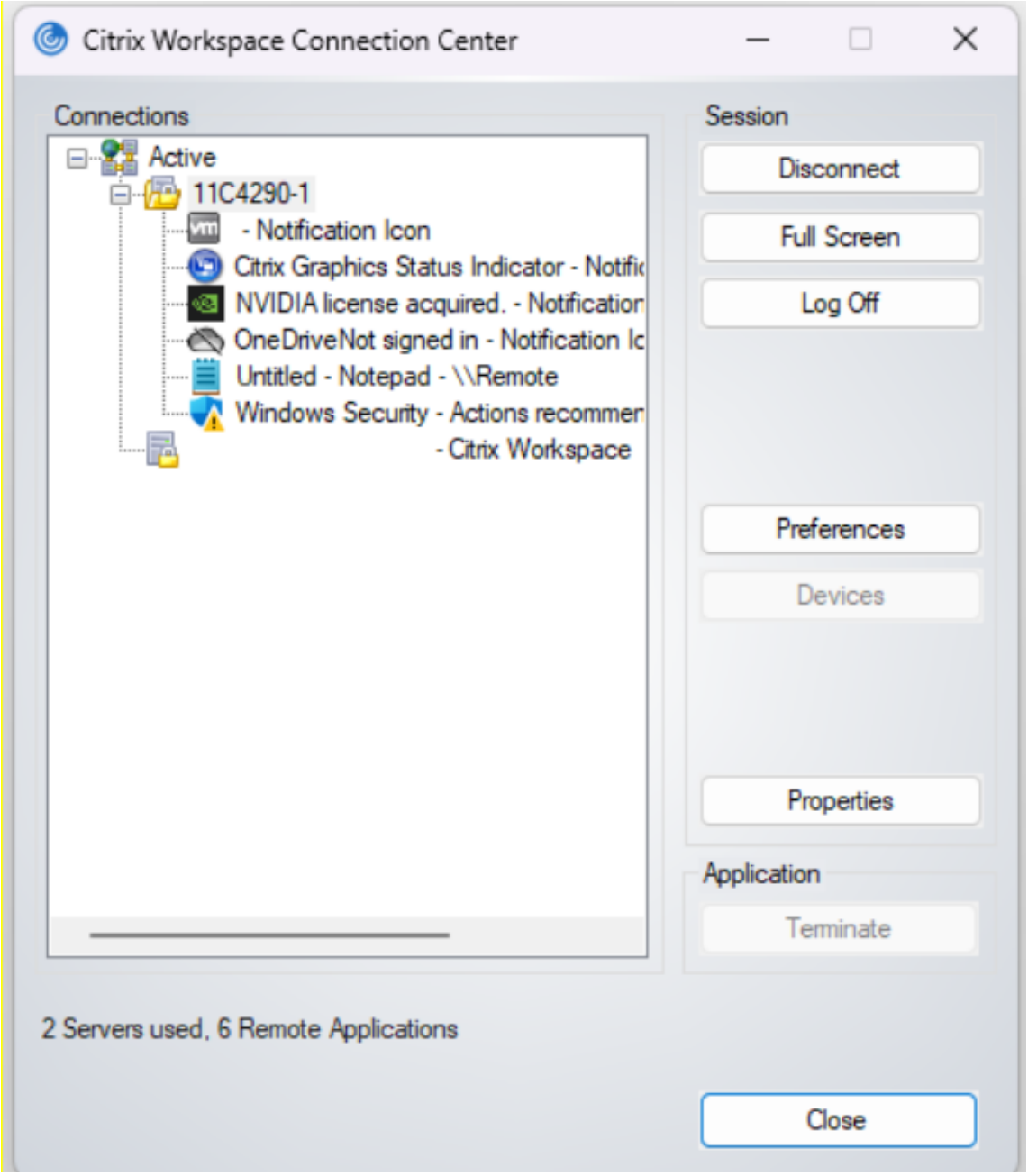
sign-out. The first one must display `C:\Windows\System32\cmd.exe` since that was open and has not been closed yet.

> **Note:**
>
> **LogoffCheckBlockingProcess** and **LogoffCheckerBlockingVisibleProcess** must not be manually edited. Manually editing these registry values could 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.

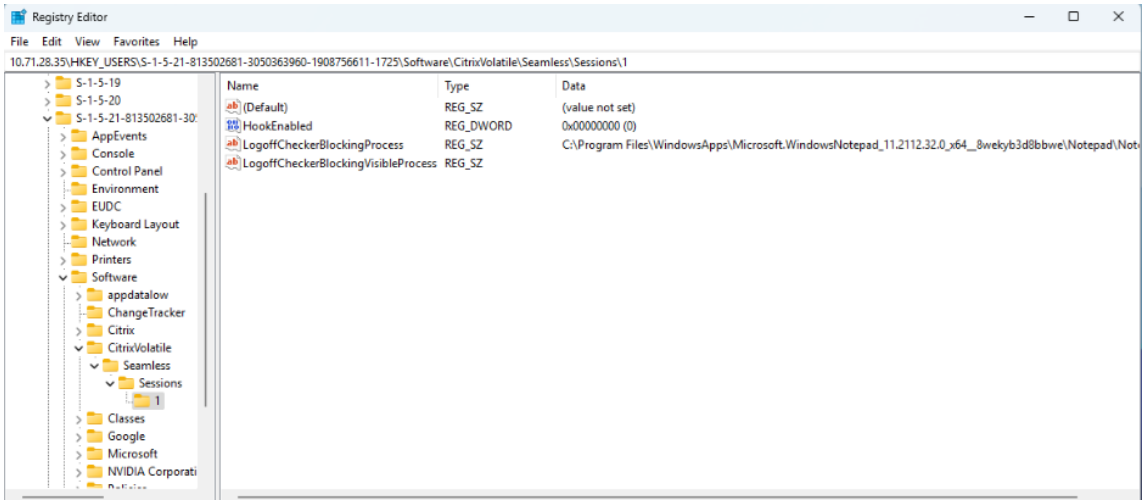
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

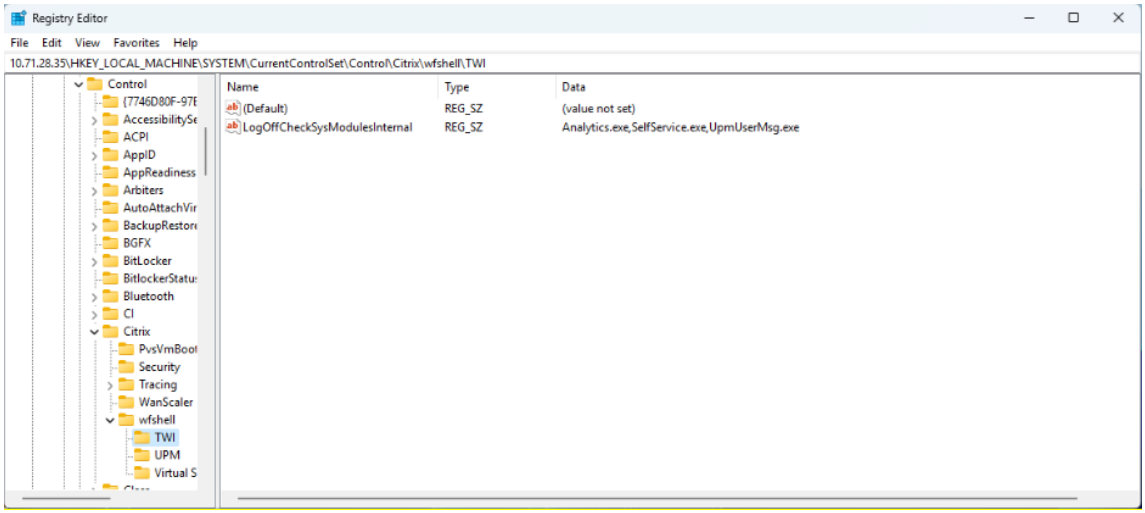
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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\TWILogoffCheckSysModulesInternal`
    - 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.
15. Repeat steps 9-16 until the session is signed out automatically within 30 seconds of closing the Remote Application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

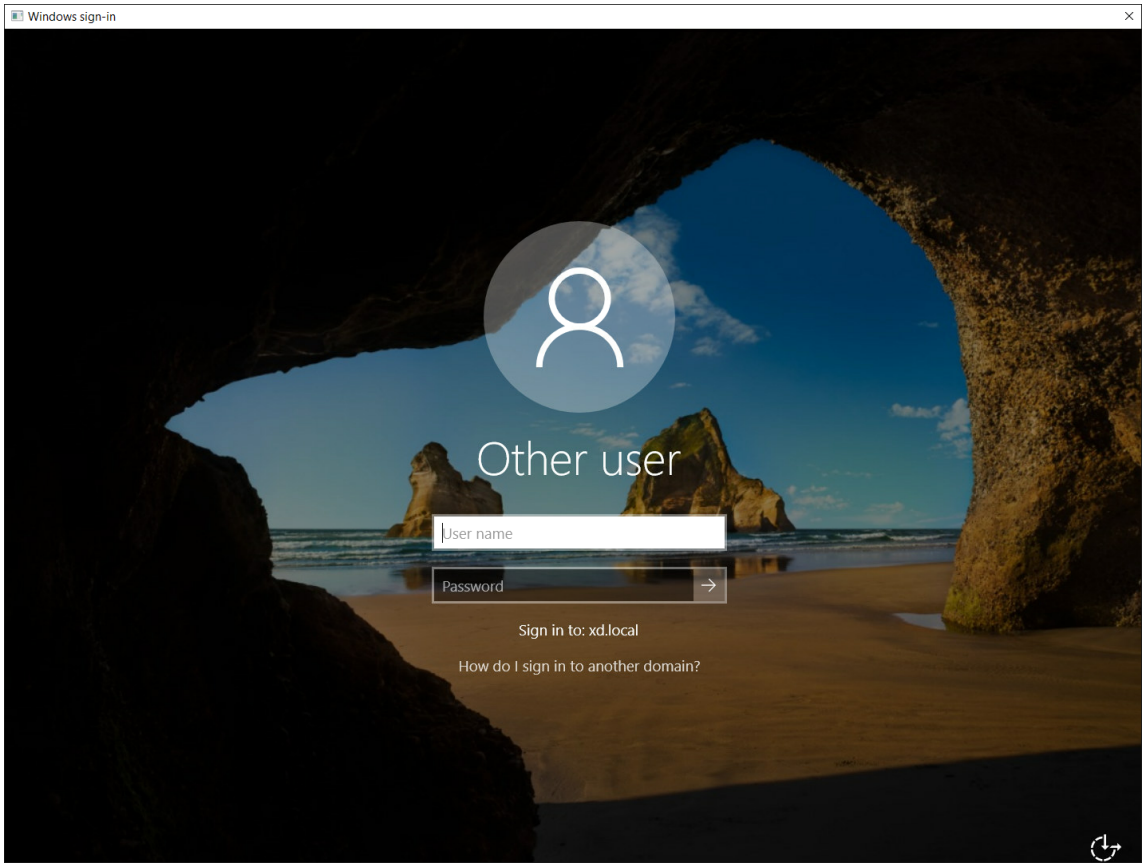
By default, the **LogonUI** window includes a title bar with a close button which enables the end user to disconnect from the session if needed.

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.



Published application does not appear

Refer to the support articles to troubleshoot instances when the published application do not launch or disappear during launch or when it fails to appear.

To troubleshoot instances

Additional Seamless configuration settings

Under most circumstances, the default server settings are sufficient for the majority of applications, and no additional settings are required for published applications.

In some cases, additional configuration is required, including controlling the interaction and display of specified application windows, as well as settings within the published application environment itself.

> **Note:**
>
> Citrix does not recommend changing these configuration settings unless explicitly instructed by Citrix support

© 1997–2026 Citrix Systems, Inc. All rights reserved.

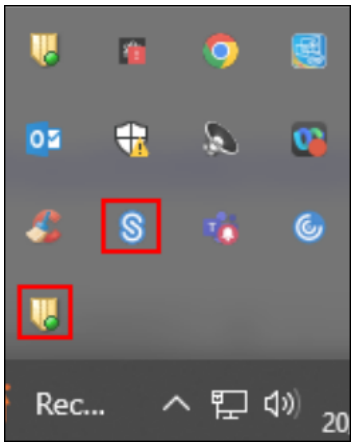
These settings are outlined in the Seamless configuration settings KB article.

System Tray Icon Redirection

September 6, 2025

Starting with Citrix Virtual Apps and Desktops™ release 2212, remote system tray icons that are present on the VDA will be automatically redirected to the client when using seamless applications.

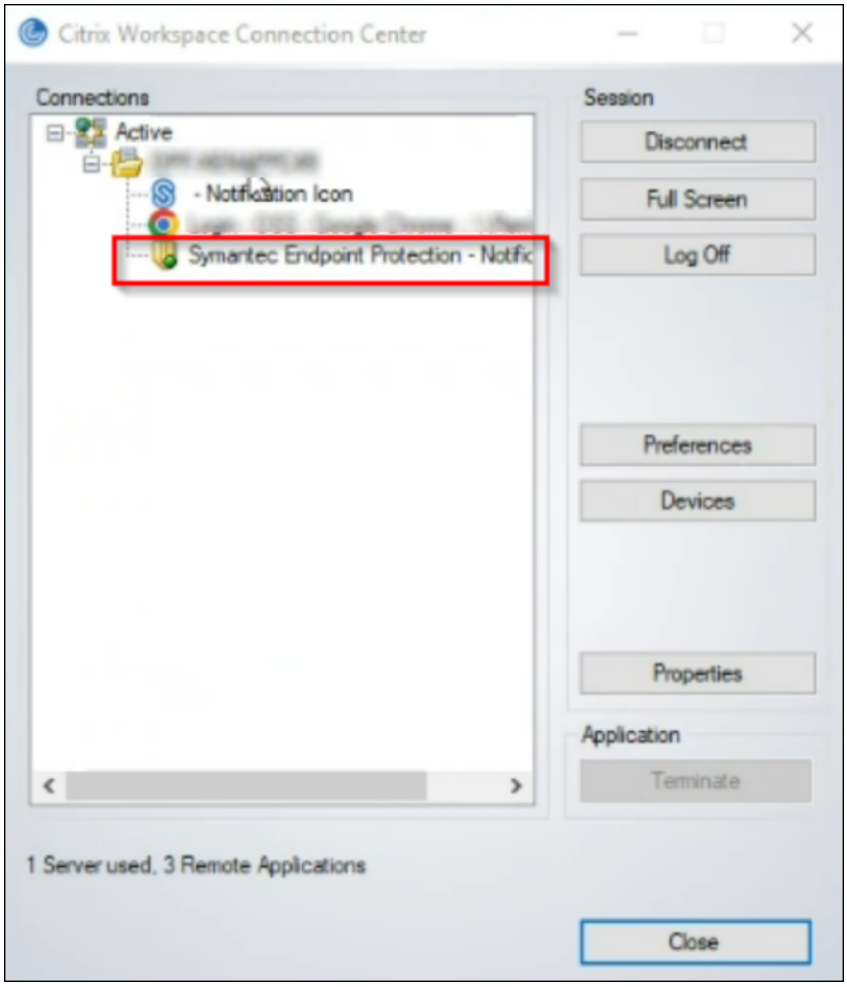
All system tray icons on the VDA hosting the seamless application will be redirected to the endpoint.



In the example above, the marked System Tray icons for Sharefile and Symantec are redirected from the VDA to the client.

These icons will also be present in the Citrix Workspace™ Connection Center.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



End users can interact with these redirected system tray icons in the same way as local system tray icons.

When using seamless applications hosted on different VDAs, this could cause duplicate system tray icons to appear on the endpoint when the VDAs have identical system tray icons.

This behaviour is enabled by default and is currently non-configurable.

Multimedia

September 6, 2025

The HDX™ technology stack supports the delivery of multimedia applications through two complementary approaches:

- Server-side rendering multimedia delivery
- Client-side rendering multimedia redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Virtual Apps and Desktops 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.

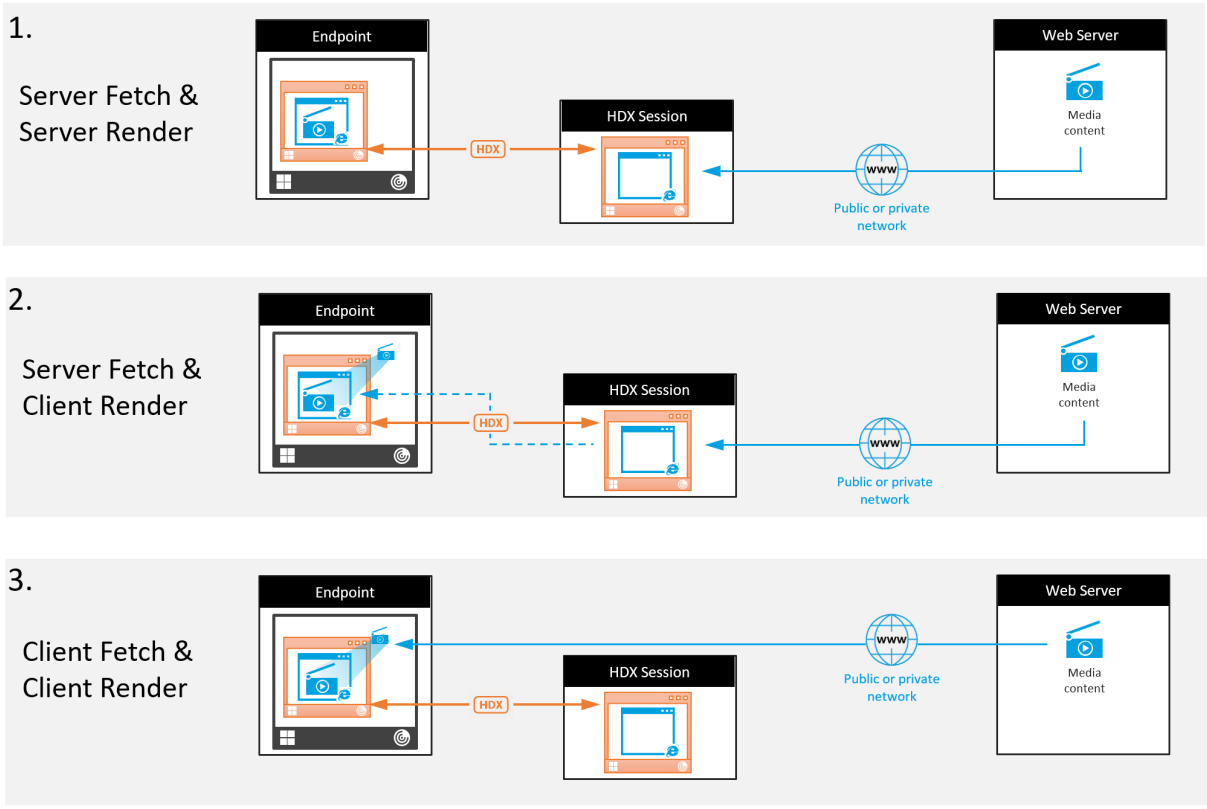
Because most servers do not offer any hardware acceleration for video compression, server scalability is negatively impacted if all video processing is done on the server CPU. You can maintain high server scalability, by redirecting many multimedia formats to the user device for local rendering.

- 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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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):

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
	HTML5 Video redirection	Yes
	Windows Media redirection	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Audio features

January 9, 2026

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.

Adaptive audio

With adaptive audio, you don't need to manually configure the audio quality policies on the VDA. Adaptive audio optimizes settings for your environment and replaces obsolete audio compression formats to provide an excellent user experience.

Adaptive audio is enabled by default. To disable adaptive audio, see Audio policy settings.

> **Important:**
>
> Citrix® recommends delivering audio using User Datagram Protocol (UDP) rather than TCP when real-time audio applications are required. The following audio transport options are available over UDP:
>
> - Audio over UDP
> - HDX™ Adaptive Transport (Enlightened Data Transport)
>
> 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.
>
> For more information on adaptive audio and UDP audio, see Audio over UDP Real-time Transport and audio UDP port range.

Loss tolerant mode for audio

Starting with the 2308 version, loss tolerant mode supports audio. This feature enhances the user experience for real-time streaming and improves audio quality over EDT when users are connecting through a network with latency and packet loss.

For more information about the loss tolerant mode and EDT, see Additional information in the Citrix Virtual Apps and Desktops documentation.

Loss tolerant mode for audio is enabled by default. If disabled or to re-enable, complete the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Enable HDX adaptive transport (EDT).
2. Enable loss tolerant mode for audio.

Client requirements and settings

The following are the minimum Citrix Workspace app versions that support loss tolerant mode:

- Citrix Workspace app for Windows 2309
- Citrix Workspace app for Linux 2311
- Citrix Workspace app for Mac 2311

In addition, please note the following:

- (Optional) For direct connections between Citrix Workspace app and VDA, enabling DTLS on VDAs is required.
- (Optional) For remote connections, loss tolerant mode must also be supported on the Citrix Gateway Service or NetScaler Gateway.

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 is 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 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:

- Adaptive audio (default)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Bitrate: variable adaptive
    - Number of channels: 2 (Stereo) for playback, 1 (mono) for microphone capture
    - Frequency: 48000 Hz
    - Bit-depth: 16-bit

- High quality
    - 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

Audio Quality Enhancer for EDT loss tolerant mode

Starting with the 2507 version, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio.

Audio quality enhancer maintains clear audio during brief network disruptions. This feature adapts to the network conditions to ensure consistent audio performance during playback and recording.

> **Note:**
>
> Adaptive audio must be enabled for this feature to work.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For setting details, see Audio policy settings. Remember to enable client audio settings on the user device.

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 the 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UDP Real-time Transport. If there is network congestion or packet loss, we recommend configuring UDP/RTP for audio to ensure the best possible user experience. For any real time audio such as soft-phone 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.

> **Note:**
>
> If Audio over UDP Real-time Transport is not required for adaptive audio, Citrix recommends configuring the policy setting to Disabled. This helps avoid Citrix Workspace app clients requesting open UDP connections or triggering unwanted Citrix Workspace app client firewall configuration dialog windows to appear.

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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
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 [Application] 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 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:

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 Studio console because it is not the default audio codec. The default is the HD Audio codec (High 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Audio diagnostic command line tool

The audio diagnostic command line tool on the VDA can be used to query session data related to audio policies, configuration, and data transport.

Usage

Open a command prompt and run `CtxAudio.exe` from the `C:\Program Files\Citrix\HDX\bin` folder.

- Running the tool as an administrator displays all active ICA session(s) audio information.
- Running the tool as a non-administrator displays the current user's ICA session audio information.

Output

The tool outputs various configuration settings that can help diagnose audio-related issues within a session.

Section	Description
Policy information	Audio policies applied to the current session(s).
Settings information	Audio related configuration settings stored in the registry.
State information	Audio state, version, codecs, and transport applied to the current session(s).
Devices information	Device names, their roles, and their statuses used in the session.

> **Note:**
>
> The output varies depending on if you run the tool on a multi-session (TS) VDA or a single-session VDA (WSVDA).

Limitation

You install an audio device on your client, enable the audio redirection, and start an RDS session. The audio files might fail to play and an error message appears.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Browser content redirection

September 3, 2026

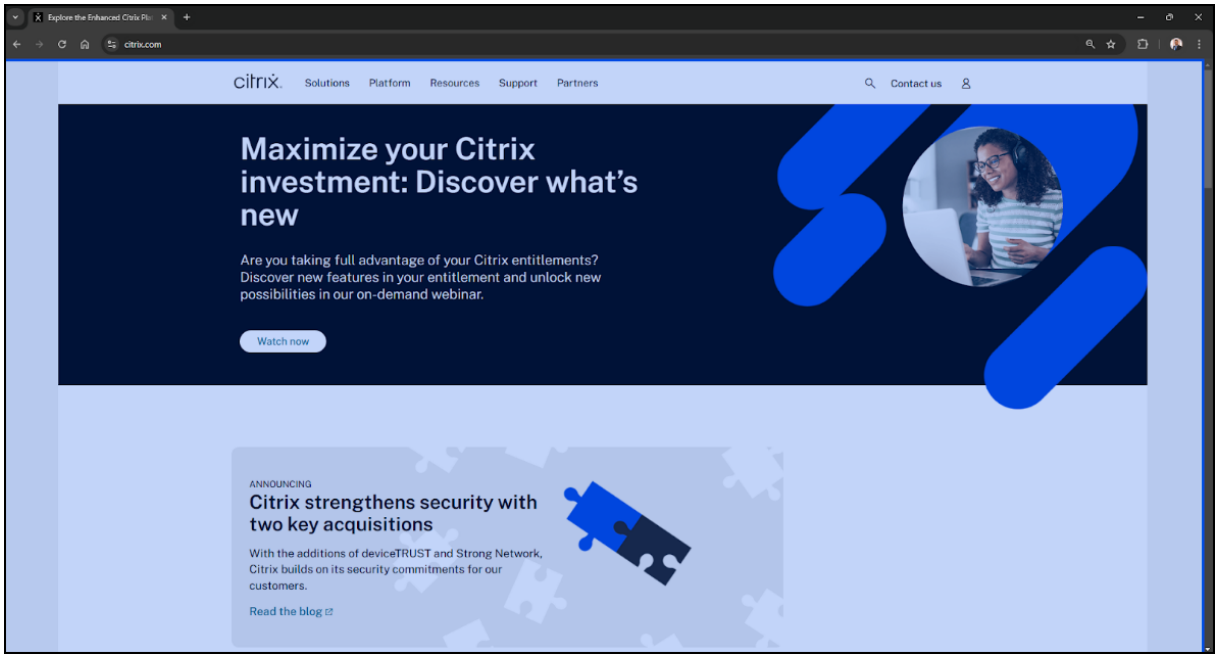
Introduction

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.

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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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™

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - Google Chrome Store
  - Microsoft Edge Store
- We recommend using the latest version of the browsers for best experience

> **Note:**
>
> - To enable Browser Content Redirection or Bi-directional Content Redirection, ensure you have Virtual Delivery Agent (VDA) version 2503 if you intend to use the Browser redirection extension from the Microsoft Edge Add-ons store. For older VDA versions, you can achieve the same functionality by installing the extension from the Chrome Web Store within your Microsoft Edge browser.
> - The extension links provided above are Generally Available (GA) and are relevant for production-level deployments. In addition to the GA extensions, Citrix also publishes a Beta (GA + 1) extension specifically on the Google Chrome Store.
> - Citrix recommends that customers have test users on the Beta version so upcoming updates are tested and any issues are reported early. This ensures a smooth process when the GA extensions officially roll out.
> - Extension releases typically match the Citrix Workspace App releases

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 for Windows 2402 CU4 or newer, Citrix Workspace App for Windows 2507
    - Current Release - Citrix Workspace App 2405 or newer

> **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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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.
>
> - Starting with the Citrix Workspace app 2507 for Windows, Browser Content Redirection (BCR) is managed as a modular component but is still packaged with Citrix Workspace App. The BCR component is now installed by default on LTSR versions as well, ensuring consistency between CR and LTSR. Additionally, standalone BCR packages will be published for situations that require independent updates or interim patches outside the regular Citrix Workspace app release cycle For more details, see 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 newer
    For more details, please refer to Citrix Workspace App for Linux documentation

> **Note:**
>
> - Starting with Citrix Workspace app 2601 for Linux, Browser Content Redirection (BCR) is managed as a modular component. The BCR component continues to be packaged & installed by default with Citrix Workspace app for Linux, ensuring a consistent user experience. Additionally, standalone BCR packages will be published for situations that require independent updates or interim patches outside the regular Citrix Workspace app release cycle. For more details, see Citrix Workspace App Linux documentation.

ChromeOS

- Citrix Workspace App
  - Latest version from Chrome Web Store

MacOS

- Citrix Workspace App
  - Minimum Requirement - Citrix Workspace App for Mac 2411 or newer

> **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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

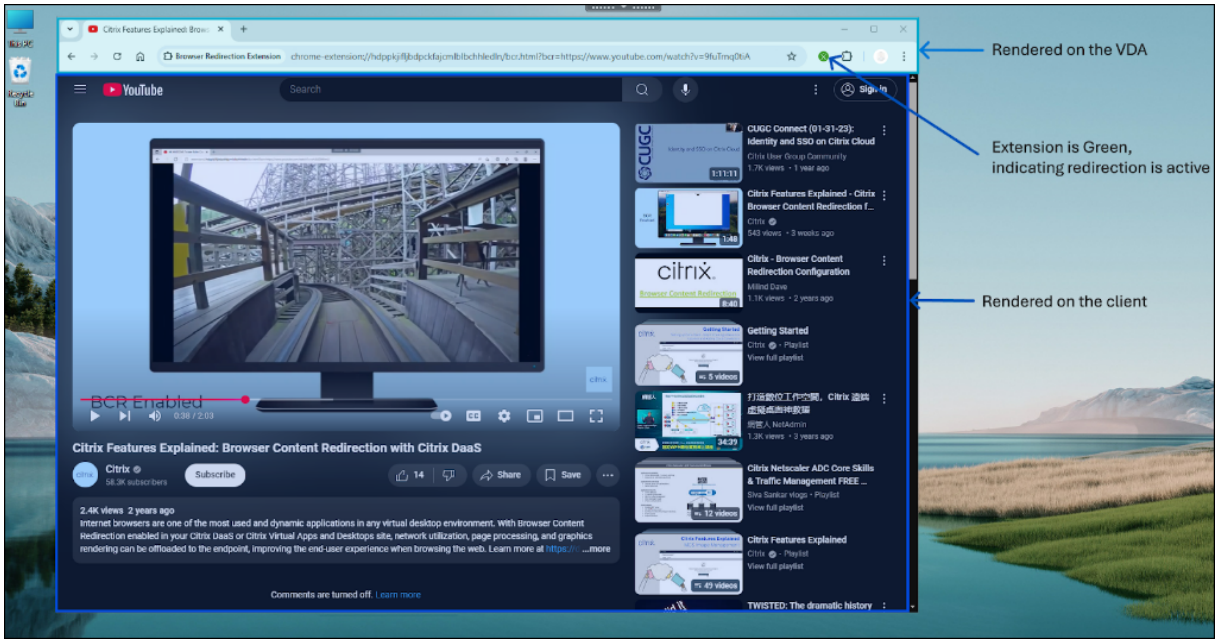
versions above the specified minimum version

- 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
- Starting with Citrix Workspace app 2511.1 for Mac, the Modular BCR component is installed by default but not packaged with Citrix Workspace App, eliminating the need to manually download and install the component from Citrix Downloads. Standalone BCR packages will be published for situations that require independent updates or interim patches outside the regular Citrix Workspace app release cycle. For more details see Citrix Workspace App Mac documentation.

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.

Features and 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

Policy configuration options

- Browser content redirection: Allowed

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

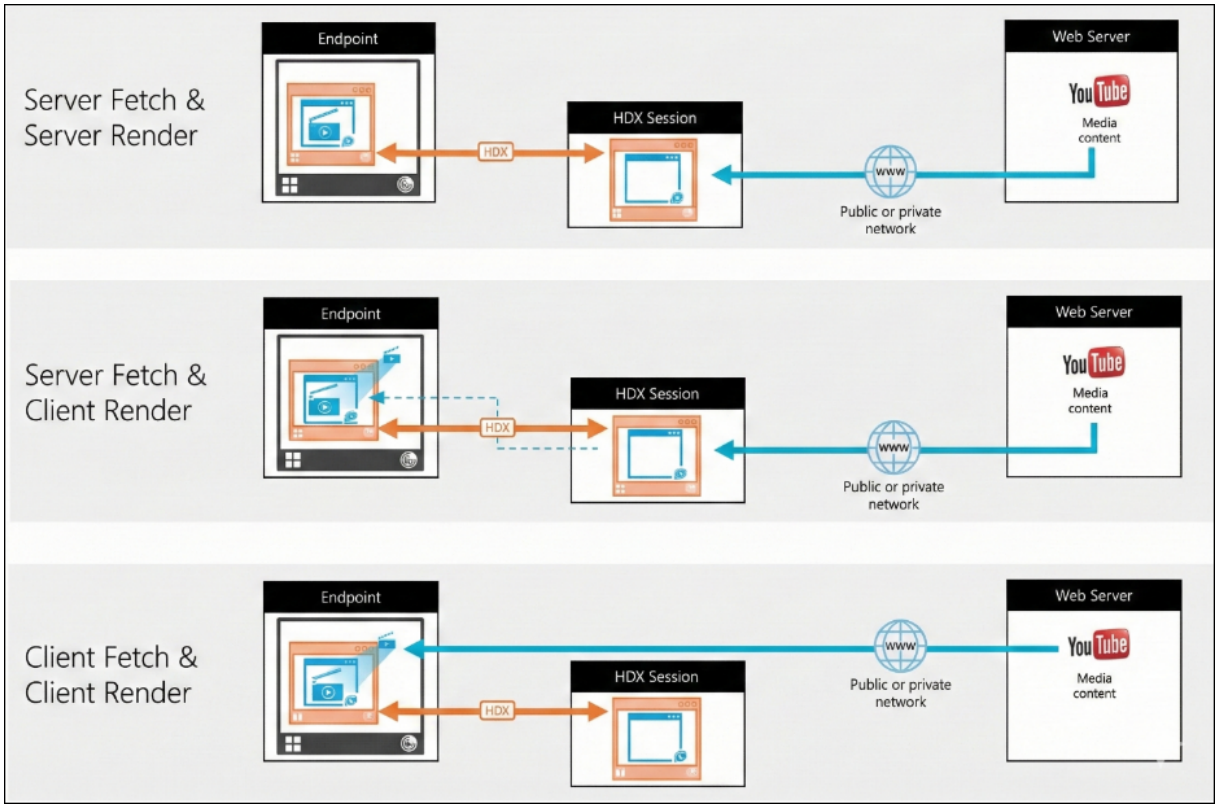
There are three modes of operation in this scenario. The term proxy refers to a proxy device that the VDA accesses to gain Internet access.

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.



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.
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Server-side certificate validation

Browser Content Redirection is further enhanced with certificate validation support. When accessing a redirected website from the client, the client overlay browser may not trust the certificate from the server or the MitM proxy. In such cases, BCR can now validate the Host or Proxy certificates against the VDAs certificate store.

Minimum requirements This feature is enabled by default, and no configuration is necessary once the below requirements are met:

- Citrix Virtual Apps and Desktops 2507
- Citrix Workspace App for Windows 2511
- Citrix Workspace App for Linux 2604
- Browser Redirection Extension (Chrome or Edge) 25.11 or later.

Single sign-on support

Browser Content Redirection now offers streamlined user experience with single sign-on support, enabling VDA-side authentication and cookie sharing. This enhancement eliminates redundant logins, boosting productivity by maintaining authentication and cookie persistence across BCR sessions, even after the BCR window is closed. This seamless experience further enhances security by ensuring authentication originates from the VDA, not the client.

For detailed information on the feature, see Single sign-on support section.

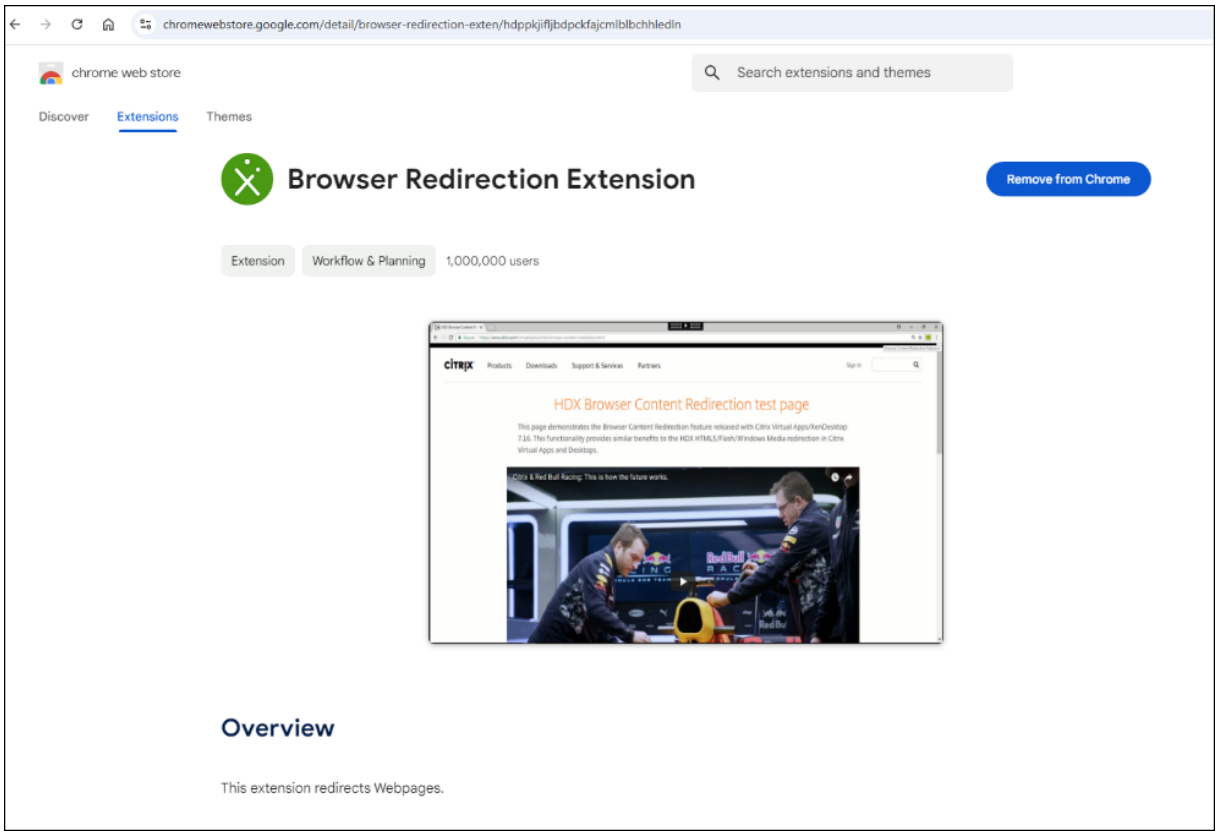
Use Cases

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Extension ID and Update URL:** The extension ID and update URL for the Citrix Browser Content Redirection extension.

Steps for Google Chrome

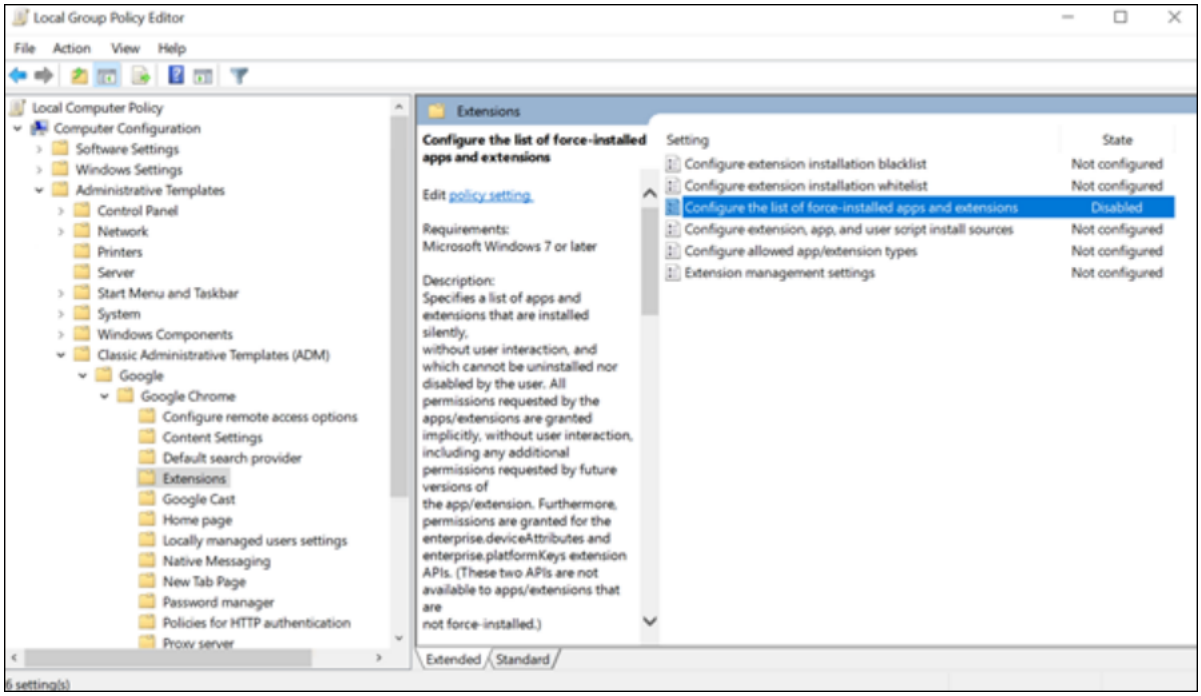
1. Import ADMX Files:
    - Copy the Chrome ADMX files to your central store for administrative templates. This is typically %SystemRoot%\PolicyDefinitions on your domain controller.
2. Open Group Policy Management:
    - Launch the Group Policy Management Console (gpmc.msc).
3. Create or Edit a GPO:
    - 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: ;
    - 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.

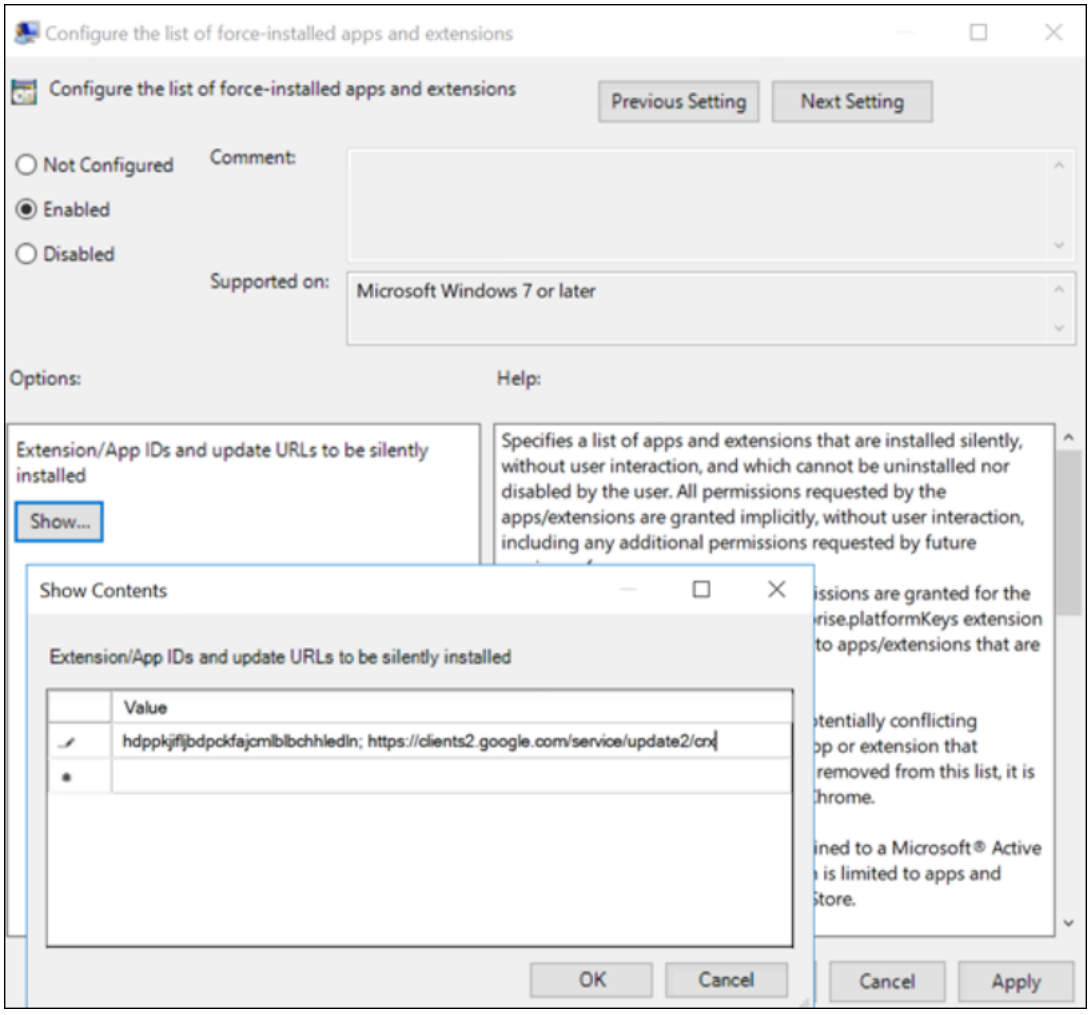
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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).
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: ;
    - 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.
- 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.
- When using Browser content redirection with Browser Profile Sharing, SSO persistence with multiple profiles is 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.

Single sign-on support

July 23, 2026

Introduction

Browser Content Redirection now offers streamlined user experience with single sign-on support, enabling VDA-side authentication and cookie sharing.

This enhancement eliminates redundant logins, boosting productivity by maintaining authentication and cookie persistence across BCR sessions, even after the BCR window is closed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This seamless experience further enhances security by ensuring authentication originates from the VDA, not the client.

Without Single sign-on

- Opening an authenticated page within BCR required users to re-enter their credentials each time, breaking SSO persistence.
- SSO was only maintained while the BCR window remained open; closing and reopening the window forced users to repeat the login process.
- The authentication flow happened from the client, forcing administrators to provide network access to secure authentication sites from the client device.

With Single sign-on

- Users are no longer prompted for credentials (when already authenticated on the VDA), as SSO is seamlessly preserved from the VDA browser.
- Authentication happens from the VDA, which improves security posture by limiting client-side network requirements and exposure, providing a significantly improved and uninterrupted experience.

Minimum requirements

- Citrix Virtual Apps and Desktops 2507
- Citrix Workspace App for Windows 2511
- Citrix Workspace App for Linux 2601
- Browser Redirection Extension (Chrome or Edge) 25.11 or later

Supported authentication sequences

There are two types of authentication sequences that are currently supported with BCR Single sign-on.

Redirection based authentication

In this standard method, the application uses an HTTP redirect to force the user to a dedicated page for authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, if a user attempts to reach https://my.intranet.app without the necessary session cookies, the web application will respond with an HTTP 302 Redirect to the authentication endpoint, like https://my.intranet.app/auth .

Once the user successfully authenticates on that page, the browser is redirected back to the original application URL, now including the required authentication cookies.

In-page forms-based authentication [Preview]

This method keeps the user on the intended application URL while dynamically presenting the login interface.

For example, if a user navigates to a protected page, such as https://my.intranet.app , the page loads the authentication form directly without triggering a redirection, because the necessary cookies are missing. This process may involve several internal exchanges between the page interface and the Identity Provider (IDP). These exchanges continue until a final, valid cookie is provided and utilized, granting the user access to the content on the original page.

> **Note:**
>
> In case your scenario is not covered by the mechanisms specified above and it's not possible to set up your webapp to use above mechanisms, reach out to Citrix Product team.

Configuration

Step 0: Introduction

There are two methods to configure Single sign-on with BCR. Choosing the method of configuration depends on the authentication mechanism for the desired BCR websites and the flexibility you need to configure multiple web applications for single sign on support.

Method 1: This method uses the existing BCR policies in Web Studio and uses them to achieve Single sign on support.

Before introduction of Single sign-on support, Browser content redirection authentication sites policy was used to specify the URLs used for authentication (or intermediary pages) to be redirected to the client to ensure there is no break in the flow.

With the introduction of Single sign-on support, BCR will leverage the authentication cookies on the VDA side browser and hence, the URLs in authentication sites policy now need to be configured in the Browser content redirection block list policy instead. This ensures that the authentication happens through the VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Method 2: This method operates on a similar logic as Method 1, but the URLs are configured via JSON (`bcrconfig.json`) instead and the hosted JSON URL is called in BCR ACL policy. The JSON configuration offers additional flexibility.

1. Enterprises use several web applications in their environment, and each application may use a different authentication mechanism based on its implementation. The new JSON method allows configuration to be more intuitive, robust and scalable.
2. When dealing with **In-page forms-based authentication**, the Method 1 does not offer a way to set specific authentication cookie as there are no existing policies to support such configuration. Hence, if your website requires **In-page forms-based authentication**, JSON is the only way to do it.

Looking towards the future, JSON offers a scalable way to introduce more robust features, and Citrix recommends trying the JSON based configuration.

Step 1: Determining authentication mechanism

To determine which Method to use for your configuration, first step is to determine what kind of authentication mechanism your application is using. To accurately determine the web application's authentication method, the best approach is to contact the web application administrator.

If that is not an option, you must inspect the request/response interactions in the browser's developer tools, under the Network tab, while performing the authentication flow **without** the BCR extension installed. The following results can help you determine the authentication type:

For Redirection based authentication: Look under the Status column for one or more 302 (Redirection) responses. The 302 responses should contain a location header pointing to the authentication page. This page URL must be set in the Browser Content Redirection block list policy if you are using Method 1 and `denyList` section of the app configuration in the `bcrconfig.json` file if you are using Method 2.

For In-page forms-based authentication: Look under the Method column for several POST requests. One of the later responses to a POST request should return a set-cookie header with the web-app specific authentication cookie. This cookie should be set in the cookies section of the app configuration in the `bcrconfig.json` file. As Method 1 doesn't support In-page forms-based authentication, Method 2 is the only configuration option for this scenario.

Example: Here's an example with github.com. This method can be used for any website that you want to redirect with BCR and ensure that you have the right configuration

1. Open **Chrome**, then press **CTRL+SHIFT+I** to bring up its developer tools.
2. Click on the **Network** tab.
3. Check the **Preserve log** setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click on the **Doc** filter to simplify the network logs.
5. Right click next to the **Name** and add the **URL** column.
6. Browser to **github.com** while the developer tools are still open.
7. Sign in to **github.com**
8. Note all the intermediate hops between github.com's initial page and its destination after logon has occurred.
9. Analyze the request/response headers to determine the authentication type as specified above.

Step 2: Choose a configuration method

1. If you're dealing with only Redirection based authentication and you don't have a need for redirecting multiple web applications with varying needs (e.g., one web application with Redirection based authentication and another web application with In-page forms based authentication), you can choose Method 1 to configure Single sign-on.
2. If you're dealing with In-page forms-based authentication (or) you are dealing with multiple web applications with different authentication mechanisms (or) simply want more flexibility even if you just have Redirection based authentication, you can choose Method 2.

Step 3: Configure

Method 1: Configure BCR Single sign-on with existing policies

1. Enable the feature in the VDA by creating the following registry value in the `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStream key: Dword BrowserProfileSharing value 1`
2. Configure the Browser content redirection ACL configuration policy with the websites to be redirected. No change in configuration on this front.
3. In case you have URLs configured in authentication sites policy already, copy them into the Browser content redirection block list policy and disable the authentication sites policy.
4. In case you haven't configured authentication / intermediary sites previously, then identify the intermediary URLs (from the request/response interactions in the browser's developer tools, under the Network tab, while performing the authentication flow **without** the BCR extension installed) and configure them in the block list.

Method 2: Configure BCR Single sign-on with JSON

Creating bcrconfig.json The `bcrconfig.json` can contain several web app configurations. BCR extension will try to match the requested URL to one of the `allowList` specified by one of the apps in the apps array and dynamically apply its related rules to decide how to handle page redirection and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

single sign on processing. The following keys can be utilized to control how a web app is treated by the BCR extension (please note that *boolean* values must be lower case as per JSON specifications - **true** or **false** only):

- **appName** [string value, mandatory]: This is mainly used internally by the extension and for logging purposes.
- **allowList** [string array, mandatory]: An app must contain at least one URL in `allowList`, which is the URL that is intended to be redirected so that the client should render the page, not the VDA. Multiple URLs can be defined, and wildcards are accepted. The wildcard rules are exactly the same as Browser Content Redirection ACL configuration. For example, to configure all Google apps to be redirected, utilize the following array:

  [“*.google.com/*”, “*.google.com*”, “.youtube.com”, “*.youtube.com/*”]
- **denyList** [string value, optional]: Define the URLs to which the web application redirects the user when authentication is required. This configuration is primarily essential for redirection-based authentication, but it can also be used to prevent specific redirects in some forms-based authentication flows. URLs listed in this key will not be redirected so that server-side authentication occurs. You can also use this when profile sharing is not needed to restrict specific sub-URLs of a domain to not get redirected to the client.
- **profileSharing** [boolean value, mandatory]: This is the key value that needs to be set to ensure Single sign-on authentication cookies and other cookies that store user preferences to be shared, ensuring consistent behavior between server-side and client-side rendered pages.
- **cookies** [string array, optional]: Define one or more authentication cookies necessary for the web application to load without prompting the user. The extension will then prevent client-side redirection until all cookies listed here are detected as set for the given web app URL. This setting is primarily used for In-page forms-based authentication, but it can also be utilized for redirection-based authentication in addition to specifying denyList in certain scenarios.
- **deleteClientCache**[boolean value, optional]: If `bcrconfig.json` configuration mechanism is used, then the BCR client deletes its browser cache by default for enhanced security. This process happens when the user closes all redirected tabs or starts a redirected page for the first time in a session. Set this key’s value to **false** to prevent this behavior. If client device is trusted, then setting this key to **false** can enhance user experience. If client device is not trusted, then not setting this key (or) setting this key to **true** can enhance security posture.
- **schemaVersion** [string value, mandatory]: This is mainly used internally by the extension and for logging purposes. At the time of this writing, it should have its value set to **2511**.

Example Configuration

```
{

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 "apps": [
   {

     "appName": "myWebApp1",
     "allowList": [
       "https://myWebApp1.com/*"
     ],
     "denyList": [],
     "requires": {

       "profileSharing": false,
       "cookies": []
      }

    }
,
   {

     "appName": "myWebApp2",
     "allowList": [
       "https://myWebApp2.com/*"
     ],
     "denyList": [
       "https://myWebApp2.com/authPortal/*"
     ],
     "requires": {

       "profileSharing": true,
       "cookies": []
      }

    }
,
   {

     "appName": "myWebApp3",
     "allowList": [
       "https://*.myWebApp3.com/"
     ],
     "denyList": [
       "https://myWebApp3.com/authPortal/*"
     ],
     "requires": {

       "profileSharing": true,
       "cookies": [
         "requiredAuthCookie1",
         "requiredAuthCookie2"
       ]
      }

    }

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  ],
  "preferences": {

    "deleteClientCache": true
   }
,
  "schemaVersion": "2511"
}
```

Here is a sample `bcrconfig.json` file. Its elements are explained in detail below:

The JSON structure above contains 3 apps with different configurations:

myWebApp1 scenario, no SSO:

- The `allowList` key's string array value specifies that all paths within https://myWebApp1.com should be redirected to the client, except for values listed in the `denyList` key, if any.
- The `denyList` key's string array value is empty, so no authentication sites will be prevented from redirection. So, authentication will not be kept strictly on the server side.
- The `profileSharing` key's boolean value is set to **false**, so no cookies pertaining to the `allowList` entries will be shared with the client.
- The cookies key's string array is empty, but it would have been ignored anyways since the `profileSharing` sharing key is set to **false**.

myWebApp2, redirection-based authentication scenario:

- The `allowList` key's string array value specifies that all paths within https://myWebApp2.com should be redirected to the client, except for values listed in the `denyList` key, if any.
- The `denyList` key's string array value specifies that paths that start with `/authPortal/` under the **myWebApp2.com** domain will be prevented from client-side redirection so that server-side authentication can be performed.
- The `profileSharing` key's boolean value is set to **true**, so cookies pertaining to the allowList entries will be shared with the client and single sign-on goes through.
- The cookies key's string array is empty, so the extension will not wait for a specific cookie to be set post server-side authentication before they are shared with the client.

myWebApp3, forms-based authentication scenario:

- The `allowList` key's string array value specifies that all paths within https://myWebApp3.com should be redirected to the client, except for values listed in the `denyList` key, if any.
- The `denyList` key's string array value specifies that paths that start with `/authPortal/` under the **myWebApp3.com** domain will be prevented from client-side redirection so that server-side authentication can be performed.
- The `profileSharing` key's boolean value is set to **true**, so cookies pertaining to the `allowList` entries will be shared with the client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The cookies key's string array contains a cookie name, so the extension will wait for this cookie to be set post server-side authentication. The cookie for the related URL in `allowList` will be shared with the client and client-side redirection will occur.

Preferences

- The `deleteClientCache` key is set to be **true**, so the BCR client deletes its browser cache by default for enhanced security. This is the default behavior even if the key is not set.

Configuring the BCR policy Once you have created the `bcrconfig.json`, follow the steps below to configure the Browser Content Redirection ACL configuration to use the content in the JSON file.

- Name the file with `.bcrconfig.json` extension, for example, `myrules.bcrconfig.json`
- Host the JSON file on a webserver accessible to the VDA and note the URL.

  > **Note:**
  >
  > The server must allow file downloads; Microsoft IIS sites permit JSON file downloads by default.

- In Citrix Studio, under the Policies, add the URL from the previous step to the Browser content redirection ACL configuration setting:

  > **Note:**
  >
  > Other entries in the Browser content redirection ACL configuration setting can remain. The BCR Extension prioritizes the `bcrconfig.json` settings if conflicts arise. Citrix recommends shifting the entire configuration to JSON for ease of management, application-level configuration and scalability.

- Save the policy and launch a session to test the policy configuration.

  > **Note:**
  >
  > After setting the policy, you can edit the hosted `bcrconfig.json` file anytime for tuning. The file reloads and applies changes only when the main browser process running the BCR extension launches or relaunches.

> **Note:**
>
> - In essence, from the policy perspective, you need to just enable Browser Content Redirection policy (which is enabled by default) and configure Browser Content Redirection ACL configuration policy with the URL which points to the JSON file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- JSON configuration currently applies to the following policies and makes them flexible, but the rest of the policies continue to do the same actions as before.
  - **Browser content redirection ACL configuration:** URLs in the ACL can now be configured via JSON through `allowList` key.
  - **Browser Content redirection block list configuration:** Blocklist can now be configured via JSON through `denyList` key.
  - **Browser Content redirection authentication sites:** Authentication sites can also be configured via JSON through `denyList` key.

HDX™ video conferencing and webcam video compression

September 6, 2025

> **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

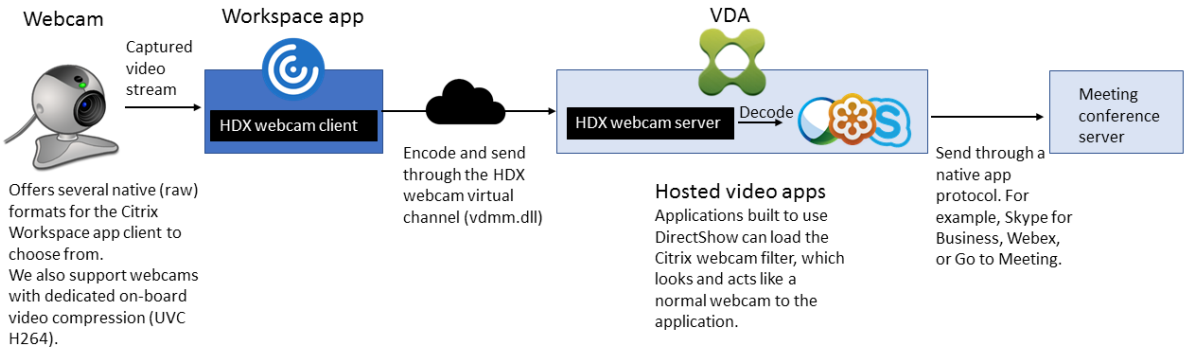
HDX webcam video compression is also called **Optimized** webcam mode. This type of webcam video compression sends the H.264 video directly to the video conferencing application running in the virtual session. To optimize VDA resources, HDX webcam compression doesn't encode, transcode, and decode webcam video. This feature is enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



The **Multimedia conferencing** policy must be enabled for HDX webcam video compression. This policy is enabled by default.

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:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Platform	Processor
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 both 32-bit and 64-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 10 or higher and Windows Server 2019 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
- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

server. Choose a webcam from the application. When the webcam and the video conferencing application support high-definition rendering then the application uses high-definition resolution. We support all webcam resolutions.

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 VGA resolution (640 x 480 pixels). 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. 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

September 6, 2025

HTML5 multimedia redirection extends the multimedia redirection features of HDX™ MediaStream to include HTML5 audio and video. Because of the growth in online distribution of multimedia content,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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, and newer browsers versions of Mozilla, Google, and Microsoft are moving to HTML5 making it the new standard.

HTML5-based multimedia have 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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 7 x86 and x64; 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 7 x86 and x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) and x64 (1607 RS1); Windows 7 x86 and x64; 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 and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA)
    Location: **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - For the end-entity (leaf): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and 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?

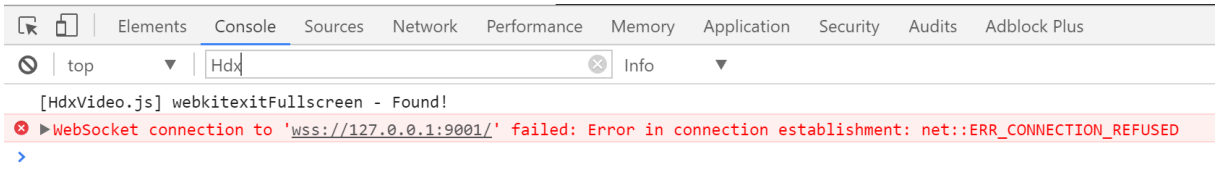
In this release, this feature is available for controlled webpages only. It requires the addition of the HdxVideo.js JavaScript (included in the Citrix Virtual Apps and Desktops Installation media) to the webpages where the HTML5 multimedia content is available. For example, videos on an internal training 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*.

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)

August 27, 2026

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

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). Media offloading is handled by `HdxRtcEngine` which resides in Citrix Workspace app. No additional components needed on the endpoint except installation of Citrix Workspace app. Available on endpoint platforms - Windows, macOS, Linux, and ChromeOS.	Optimization solution is owned and managed by Microsoft and uses virtual channels owned by Microsoft (MSTEAMS, MSTEAM1, and MSTEAM2). Media offloading is handled by the SlimCore media engine on Windows and Mac endpoints. 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 and Mac.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix HDX Optimization	New VDI solution for Teams
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.
- 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

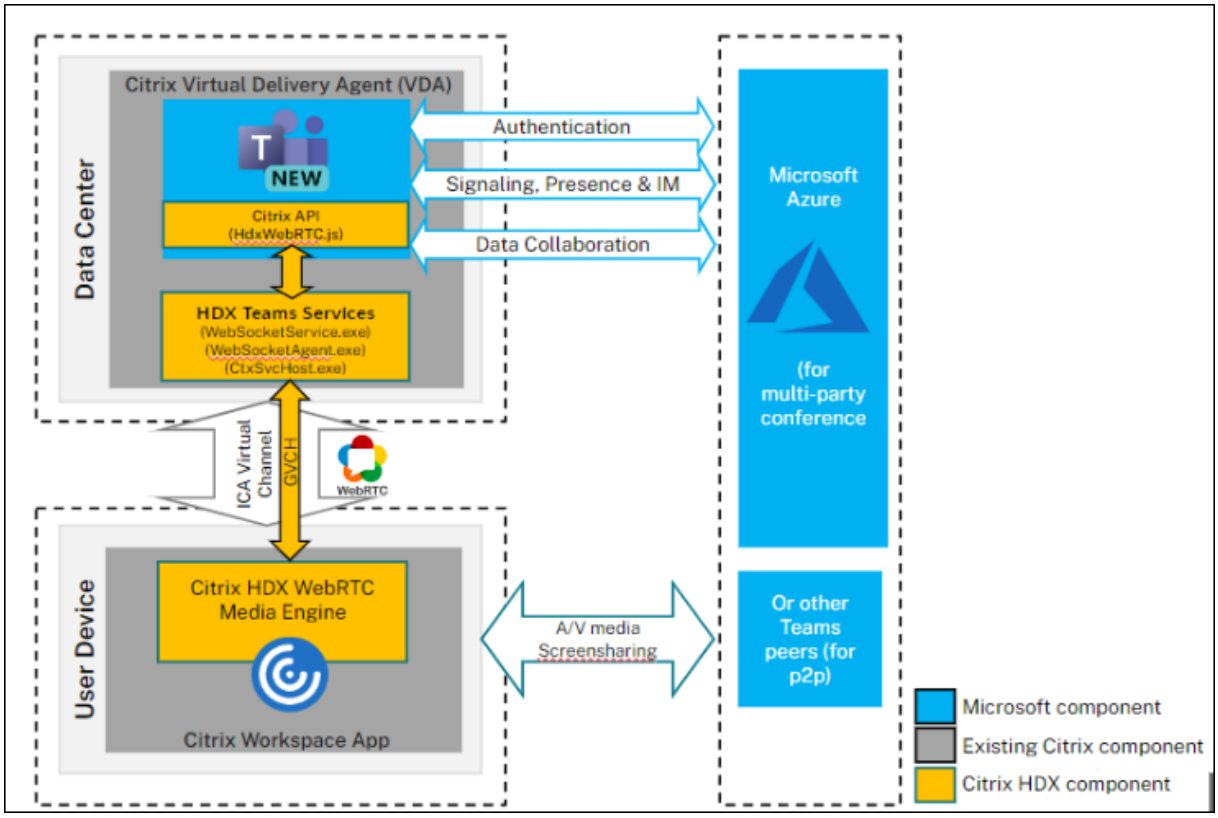
May 4, 2026

> **Note:**
>
> Microsoft has announced the deprecation of WebRTC-based 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: Microsoft has announced deprecation for HDX WebRTC

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Optimization for Windows endpoints. WebRTC-based optimization stops functioning. Citrix Studio policies for the legacy optimization no longer take effect.
>
> Customers are recommended to migrate to new VDI solution for Microsoft Teams (SlimCore). This change affects Windows endpoints only —macOS, Linux, ChromeOS, and HTML5 endpoints are not impacted. For more details, see Microsoft Blog.

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`

     > **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

> **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.

© 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)
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
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

© 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)
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
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
  - 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%.
- Microsoft Teams 2.1 supports redirection of only one webcam at a time. However, it does not support multiple webcam redirection or plug and play (PnP) webcam redirection on single-session VDAs.

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

August 31, 2026

> **Note:**
>
> The New VDI solution for Teams is currently generally available for Windows and Mac endpoints

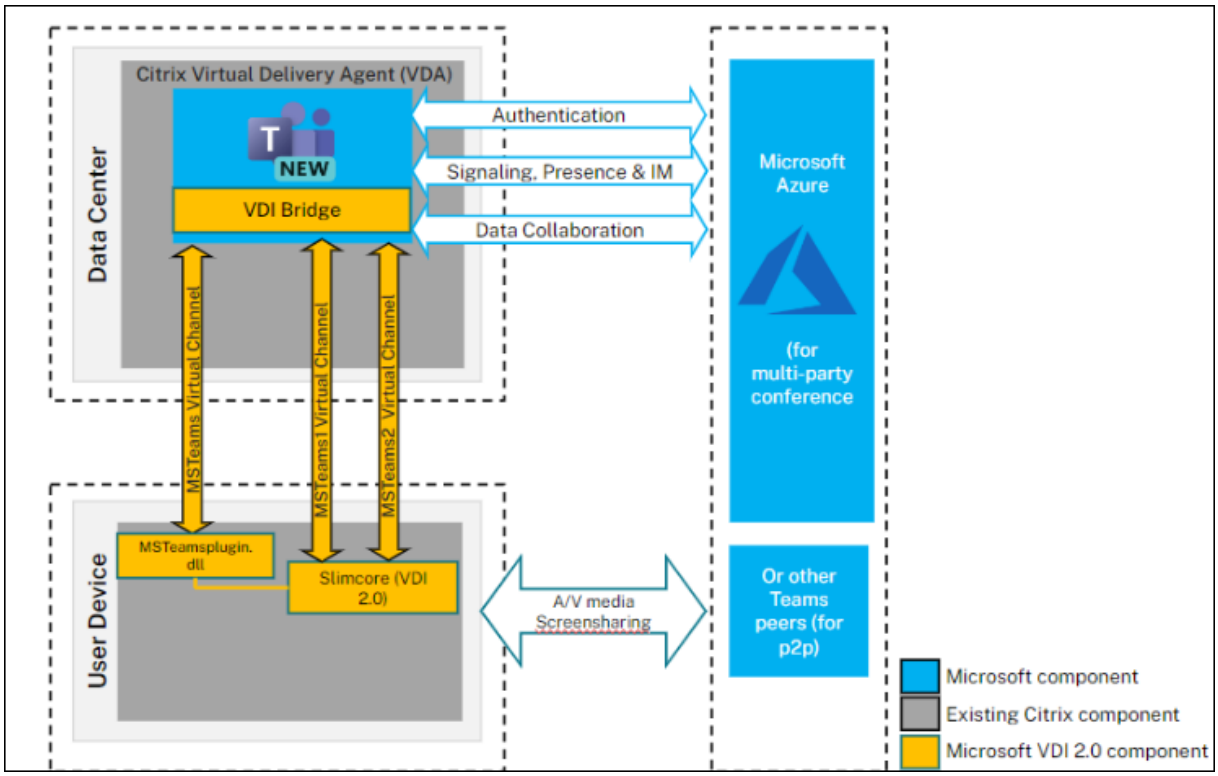
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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.
>
> 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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

   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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Options to install the Teams plug-in

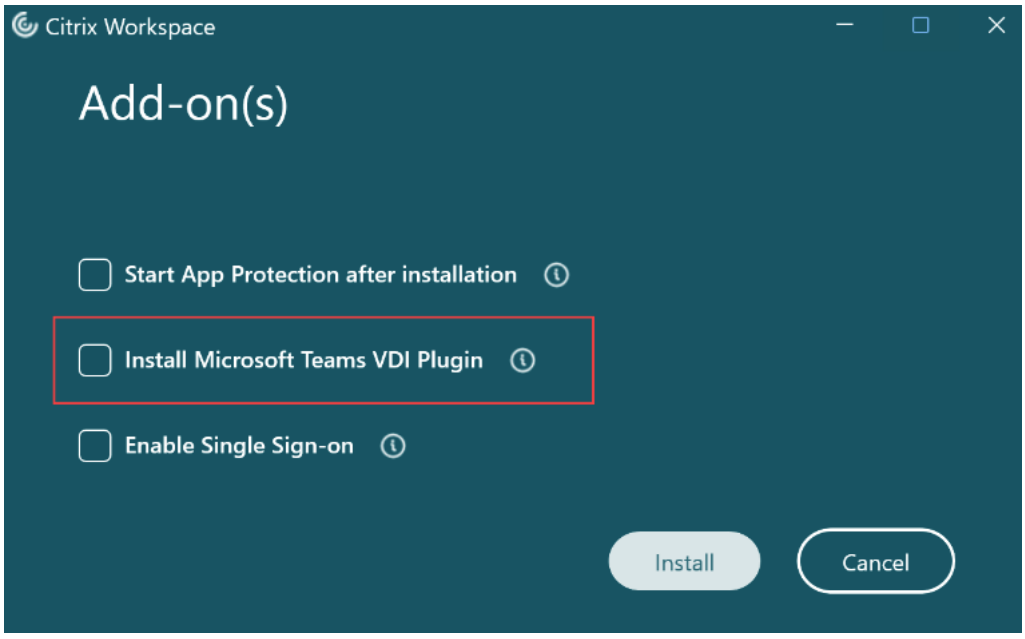
Regardless of the install method, the plug-in is placed in the Citrix Workspace app location on the endpoint:

- 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`

> **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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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)

September 13, 2025

> **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).
>
> Starting with Citrix Virtual Apps and Desktops 2402, you don't need to manually configure the `msedgewebview2.exe` registry entry as it's allow-listed by default.
>
> Published apps are now supported with the new Microsoft Teams.

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).

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

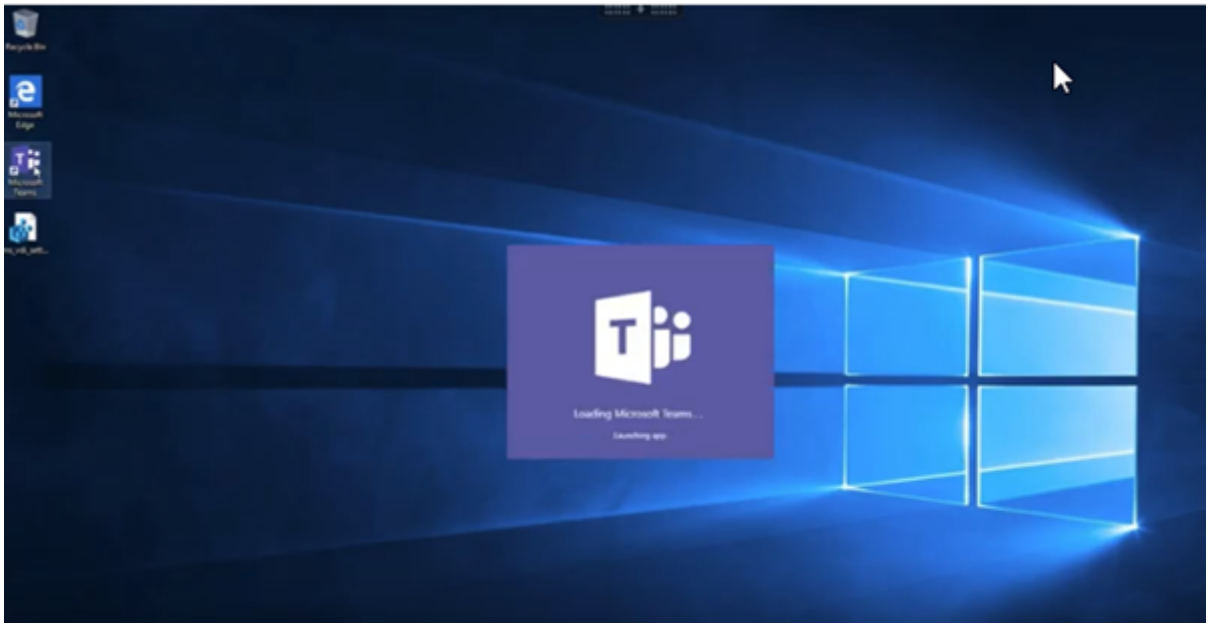
multimedia locally, moving the Citrix Workspace app window back into the hosted Microsoft Teams app.

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 demonstration 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 Microsoft Teams App (Desktop and Mac).

We recommend that you follow the Microsoft Teams machine-wide installation guidelines. Avoid using the .exe installer that installs Microsoft Teams in `AppData`. Instead, install in `C:\Program`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`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.

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 a Windows 10 dedicated persistent VDI environment. 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:**
>
> Citrix recommends 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

Citrix recommends 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 chats, or meeting reactions.

> **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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 Access 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 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.

Machine-wide installer

The following is an example of folders, desktop shortcuts, and registries created by installing a Microsoft Teams machine-wide installer on any Windows Server 64-bit VM:

Folder:

- `C:\Program Files (x86)\Microsoft\Teams`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

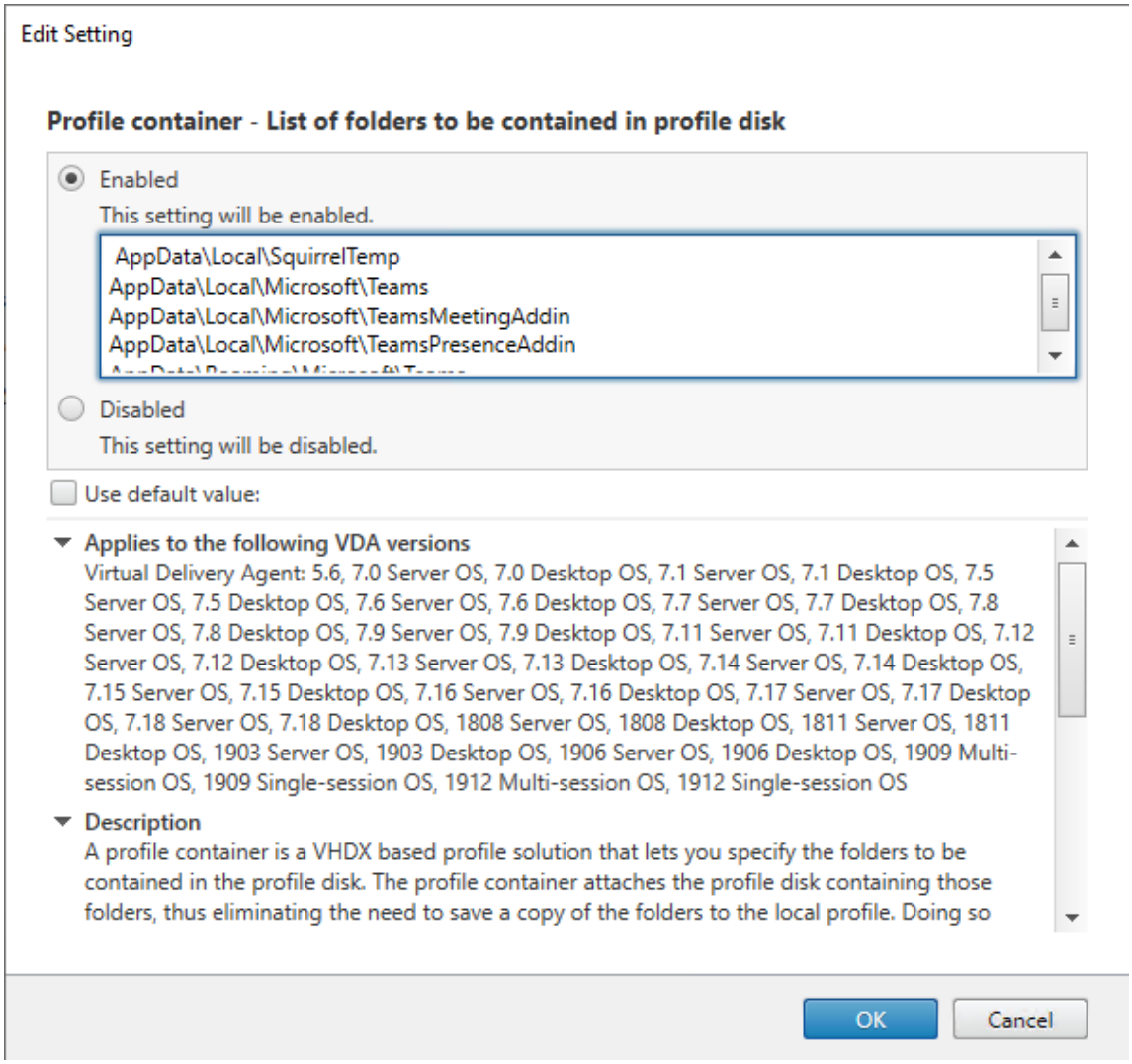
- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

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 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



List all the per-user directories in 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.
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 the 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.
- 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 of free disk space and 1 GB RAM.
- The Microsoft .NET Framework minimum requirement is version 4.8. Citrix Workspace app automatically downloads and installs the .NET Framework if it's not present in the system.

Administrators can enable/disable Microsoft Teams starting in optimized mode by changing the Microsoft Teams Optimization policy. Users starting in the optimized mode in the Citrix Workspace app can't disable Microsoft Teams.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Minimum version - Citrix Workspace app 2006 for Linux

For more information, see Optimization for Microsoft Teams in Citrix Workspace app for Linux documentation.

Software:

- `GStreamer` 1.0 or later or Cairo 2
- `libc++-9.0` or later
- `libgdk` 3.22 or later
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 or later

Authentication enhancement:

- Libsecret library
- libunwind-12 library. For more information, see Adding the libunwind-12 library dependency for llvm-12.

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 by 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 completed, restart the Session. (Root permission is required).

Minimum version - Citrix Workspace app 2012 for Mac

Supported operating systems:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 and later.
- macOS Monterey.

Features supported:

- Audio

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Video
- Screen sharing optimization (incoming and outgoing)

> **Note:**
>
> The 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 ChromeOS running on the latest version of ChromeOS

Hardware:

- Processors performing at par or better than the 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.

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. 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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.

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 are stopped or killed, before the 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 the chat window using keyboard shortcuts.
- Switch to the calendar window using keyboard shortcuts.
- Send the chat message to a specific user using keyboard shortcuts.
- Switch to the Microsoft Teams window using keyboard shortcuts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 the 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 an environment with slower storage.

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 ChromeOS (Minimum Version)
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

© 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 ChromeOS (Minimum Version)
iii. Multi-monitor	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
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

© 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 ChromeOS (Minimum Version)
MultiWindow	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
Meeting Transcrip-tions	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 is 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 only work if the 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 the 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.
> - Microsoft has deprecated support for Single Window mode in Microsoft Teams. To comply, you must upgrade your VDA to 1912 CU6+ LTSR and Citrix Workspace app 2203 CU2+ or greater, which supports the MultiWindow mode.

Enable optimization of Microsoft Teams

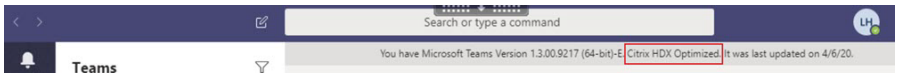
To enable optimization for Microsoft Teams, use the Manage policy described in the Microsoft Teams redirection policy. This policy is **ON** by default. In addition to this policy being enabled,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

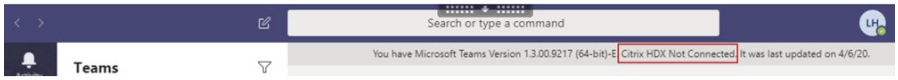
HDX checks to verify that the version of the Citrix Workspace app is at least the minimum required version. If you enabled the policy and the Citrix Workspace app version is supported, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** is set to **1** automatically on the VDA. Microsoft 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 the Manage console (Studio), your VDA can still be optimized. HDX optimization for Microsoft Teams is enabled by default in the VDA.

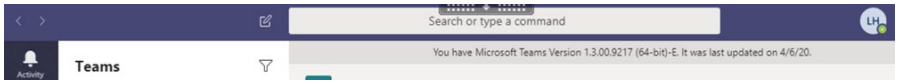
If you click **About > Version**, the **Citrix HDX Optimized** legend displays:



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 Manage policy isn't set to **Prohibited** and that the Citrix Workspace app version is supported.



> **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. Refer to Microsoft 365 network connectivity principles for detailed guidelines around network planning.

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.
- If you must use any of the following at the branch office, make sure that RTP/UDP traffic (handled by HdxRtcEngine.exe in the Citrix Workspace app) is unhindered.
    - 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 depends on the VPN product and machine platform used but most VPN solutions 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

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 supports constant and variable bitrate encoding from 6 kbps up to 510 kbps.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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)
  - 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 the 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 with the media establishment fails.
>
> - The location of the conference server is selected based on the first participant's virtual desktop location (and not the client).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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, 52.122.0.0/15	**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.

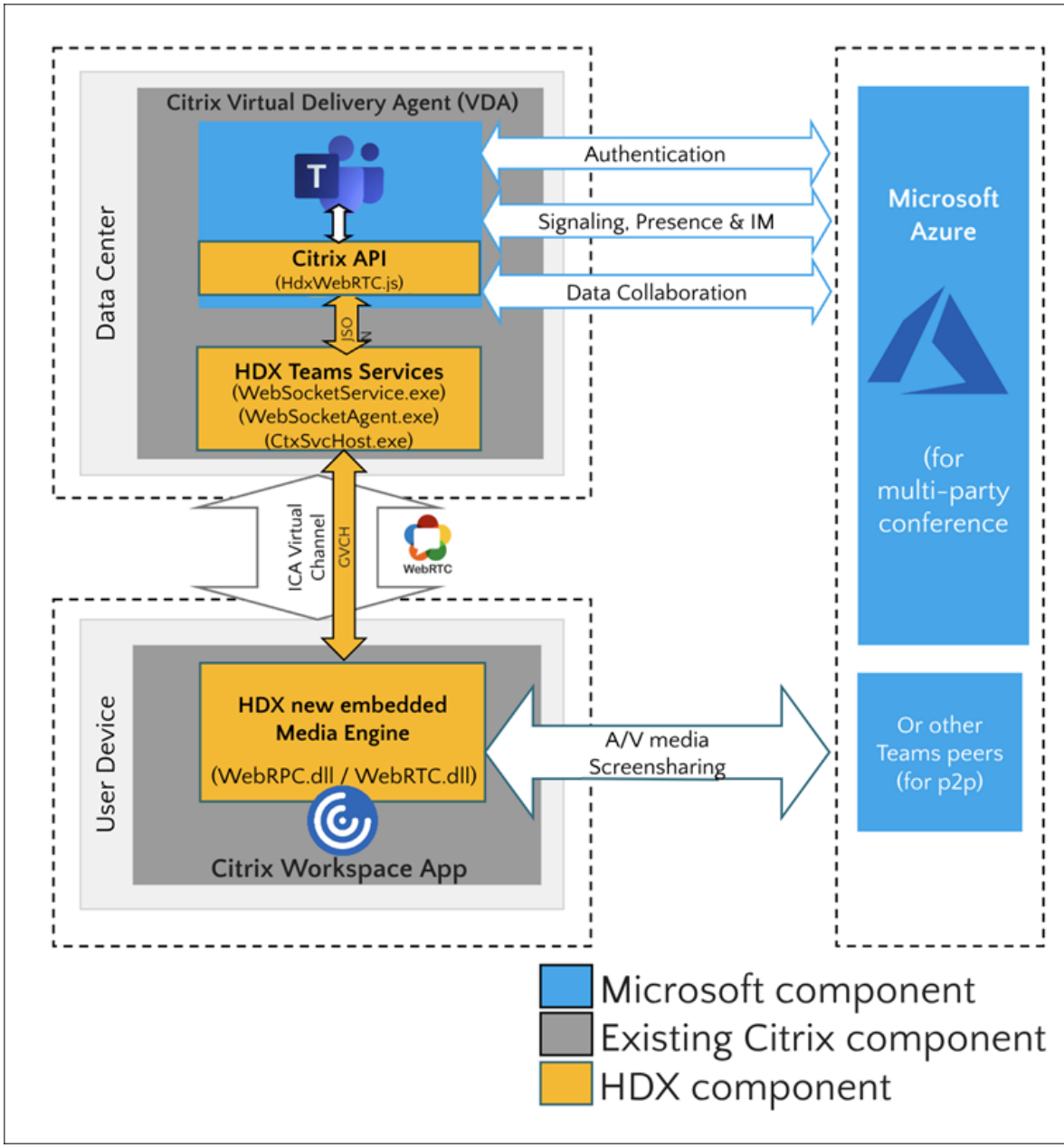
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

Call setup

Use this architecture diagram as a visual reference for the call flow sequence. The corresponding steps are indicated in the diagram.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.
5. WebSocketAgent.exe instantiates a generic virtual channel by calling into the Citrix HDX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.exe 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 can 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 the 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 ChromeOS version 2111.1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for dynamic e911

Starting with version 2112, the 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 the 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 ChromeOS 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 the Citrix Workspace app relays to Microsoft Teams are:

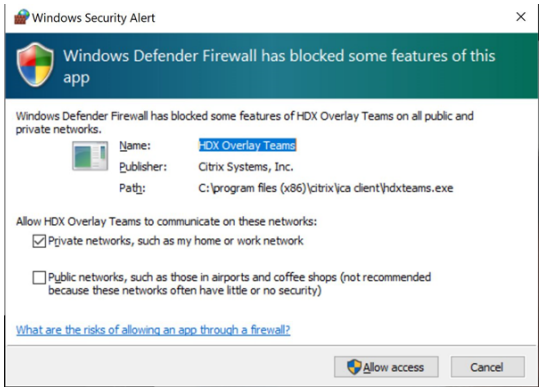
- Chassis ID / Port ID using Link Layer Discovery Protocol (LLDP) for Ethernet/Switch connections. Ethernet/Switch (LLDP) is supported on:
  - Windows versions 8.1 and 10
  - macOS, which requires LLDP enablement software. To download the LLDP enablement software, go to `www.microsoft.com` and search 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.
  - 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 the Citrix Workspace app is installed (permission is set to HDX RTC Engine)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

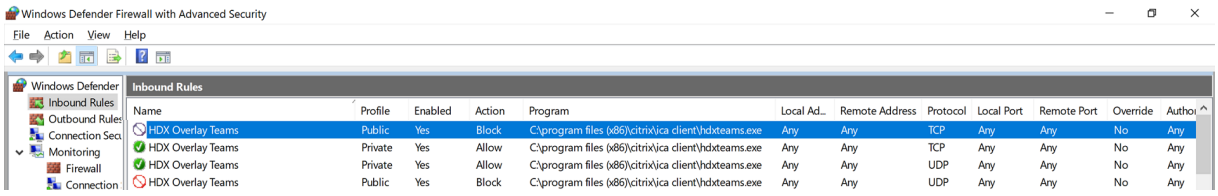
- Supported on all Workspace app platforms. However, for Citrix Workspace for Linux, you must include the `libgps` library in the OS distribution of the Thin Client (>sudo apt-get install libgps23 gpsd lldpd).

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.



Microsoft Teams and Skype for Business Coexistence

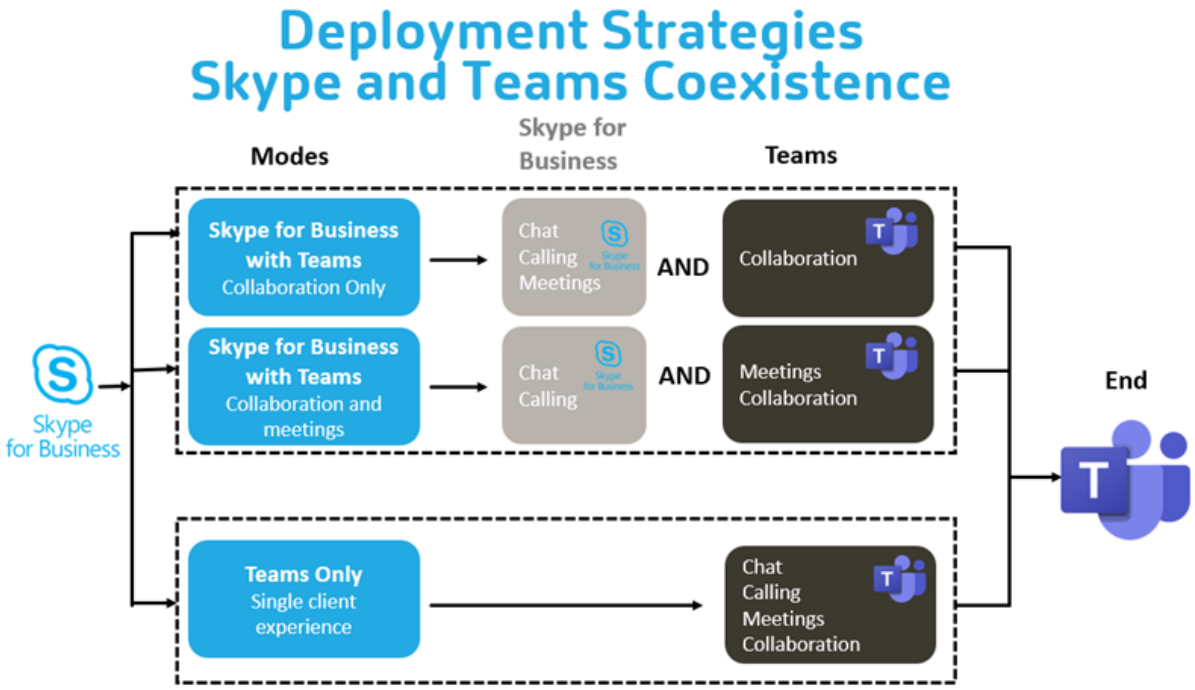
You can deploy Microsoft Teams and Skype for Business side by side as two separate solutions with overlapping capabilities.
For more information, see Understand Microsoft Teams and Skype for Business coexistence and interoperability.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Business broadband internet connections in many areas suffer from intermittent packet loss, periods of excessive jitter, and outages.

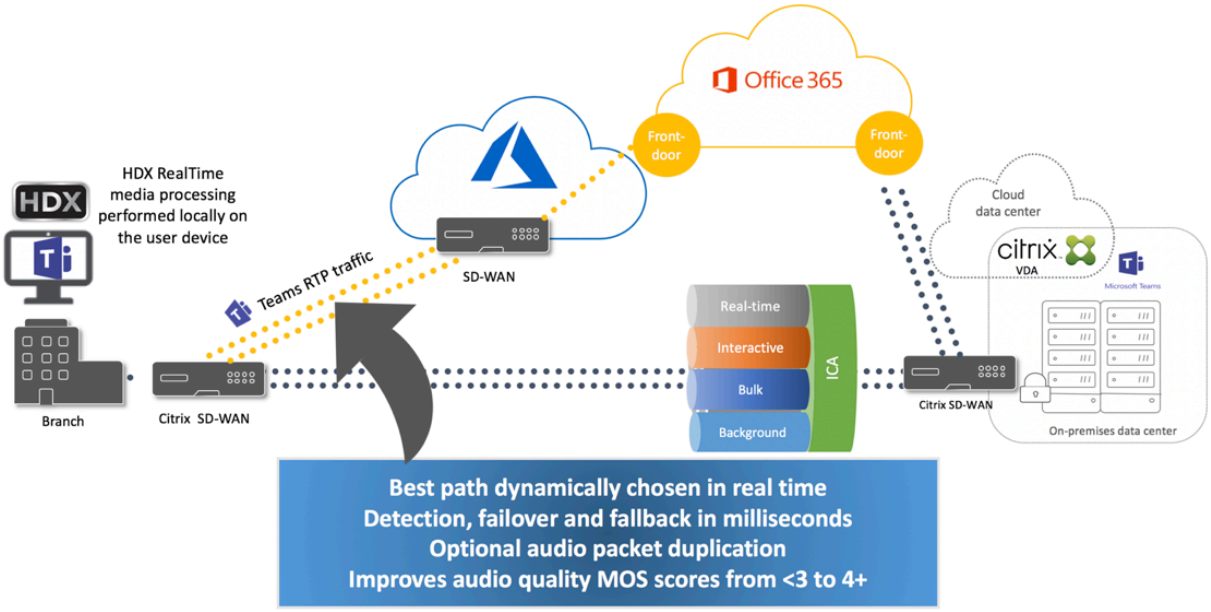
Citrix SD-WAN offers two solutions to preserve Microsoft Teams audio-video quality when network health is variable or degraded.

- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

> **Note:**
>
> This feature is supported with the 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.

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 pre-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> requisite 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 2307
- 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.

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)

A value set to 1 blurs the background. The end-user or the administrator can set this value.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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*

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 the 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

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.

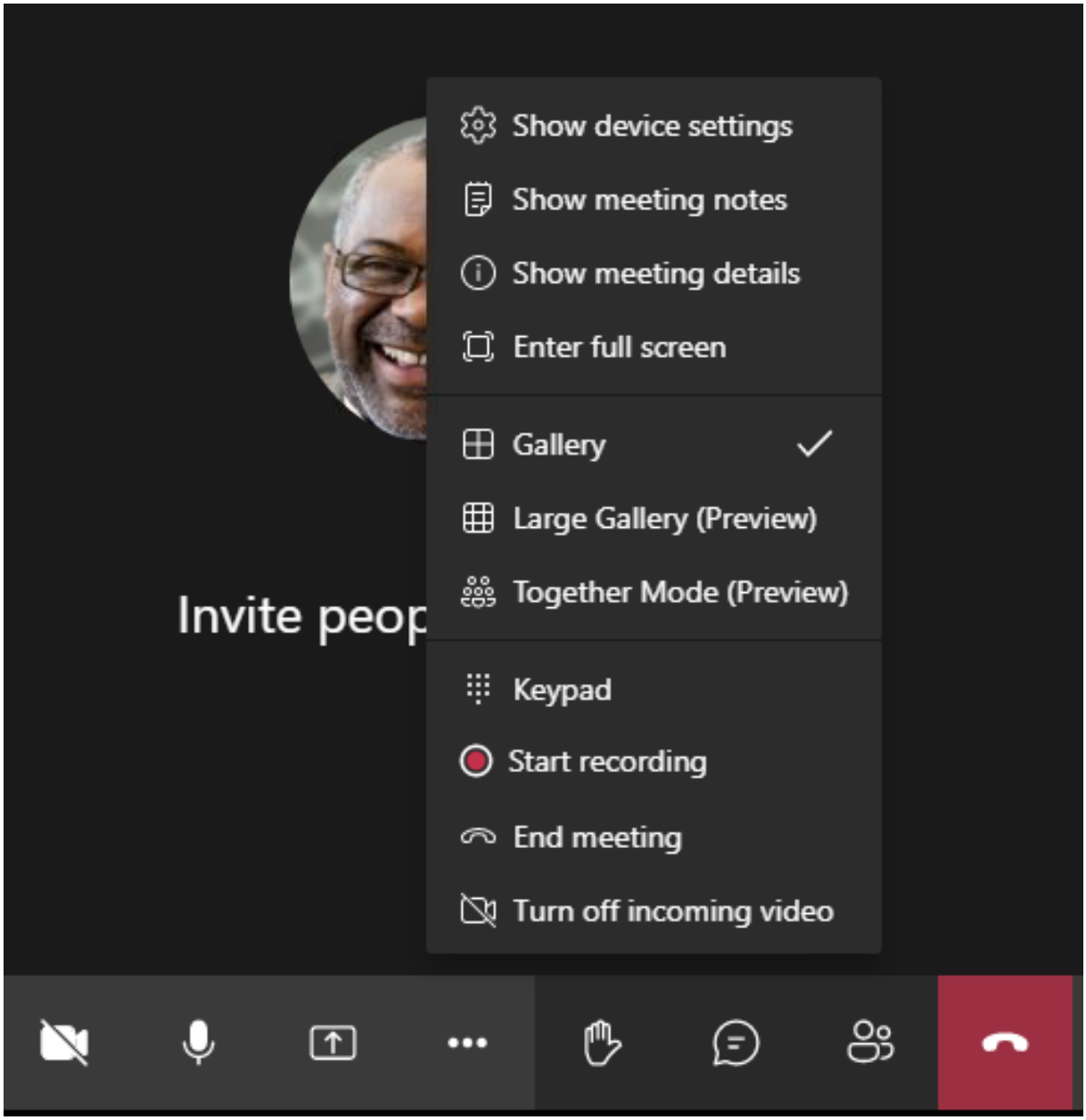
Microsoft Teams displays a 2x2 grid with video streams of four participants (known as **Gallery**). In this case, Microsoft Teams sends four video streams to the client device for decoding. When more than four participants share a video, only the last four most active speakers appear on the screen.

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 videos 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 (Citrix Workspace app for Windows 2102, Citrix Workspace app for Linux 2106, Citrix Workspace app 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	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.
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, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	Gallery view 2x2 (default)	Large Gallery view
'Slow-user'problem	Sender modifies each modality's (audio/video/screenshare) quality to the lowest common network quality among the 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.	Less susceptible to the lowest common network quality scenario. The conference server provides different qualities based on 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 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.

Outgoing screen sharing is also optimized and offloaded to Citrix Workspace app. In this case, the

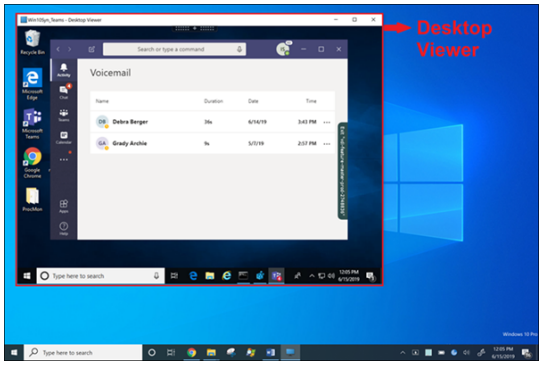
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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 peers 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 share a local application that runs in the client machine. This sharing is possible only if the local app is overlaid on top of the 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.
- It is not possible to Pin the Sharing Controls to a specific location in Optimized Microsoft Teams.
- When sharing a minimized app, the title bar of the app might also be shared.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App sharing

Starting with the Citrix Workspace app for Windows 2112.1 and VDA 2112, Microsoft Teams supports app sharing.

Starting with the 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. You can also share custom in-house applications, like Java, using the optimized Microsoft Teams. To share a specific app:

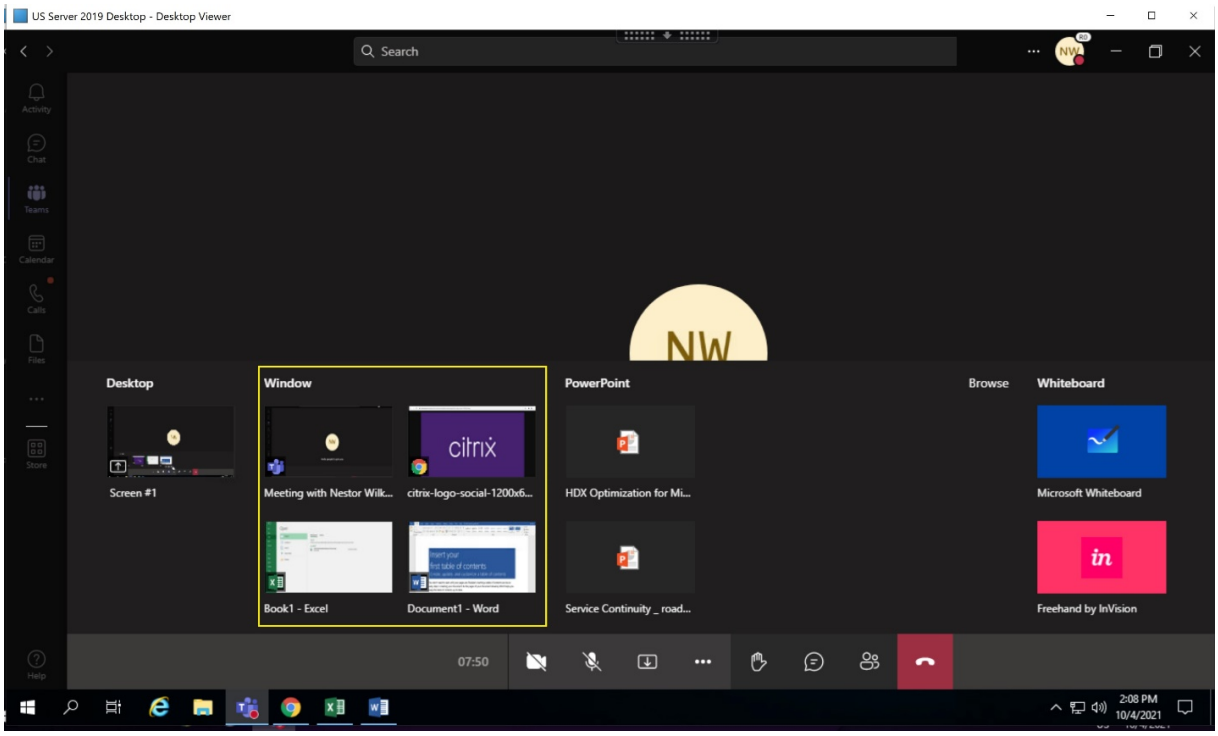
1. Navigate to the Microsoft Teams app within your remote session.
2. Click **Share content** in your Microsoft Teams UI.
3. Select an app to share in the meeting. The red border appears around an app that you selected and the peers on the call can see the shared app.

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

> **Note:**
>
> - 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 maximum rate is 30 frames per second. The Citrix Workspace app forwards the content to the peer or conference server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Known limitations with screen sharing of specific app:

- The 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 show 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.

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 if you are using the Citrix Workspace app for Windows 2202 or earlier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Give and Request control in Microsoft Teams This feature is supported in the following versions of the 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 or later
- Citrix Workspace app for Mac version 2203.1 or later
- Citrix Workspace app for Linux version 2203 or later
- Citrix Workspace app for ChromeOS version 2303 or 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 the **Request control** button in the Microsoft Teams UI. The meeting participant who's sharing the screen can either allow or deny your request.

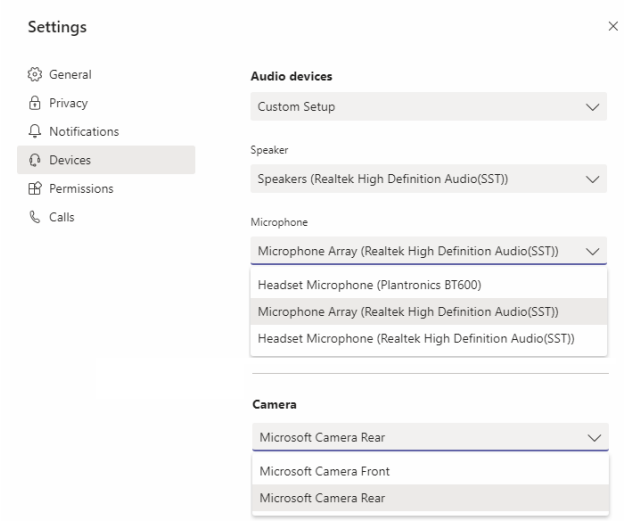
While you have control, you can make selections, edits, and other modifications to the shared screen. For these actions, you can use both a keyboard and a mouse. When you're done, click **Request control**.

> **Limitations:**
>
> - Give and Request controls 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.

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**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 are 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:

- Microsoft Teams certified headsets with built-in echo cancellation. In setups with extra peripherals, where the 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. For more information, go to `www.microsoft.com` and search for Microsoft Teams certified headsets.
- Microsoft Teams certified cameras, although Skype for Business certified peripherals are compatible with Microsoft Teams. For more information, go to and search for Microsoft Teams certified cameras and Skype for Business certified peripherals.
- 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 spe-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> cific 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

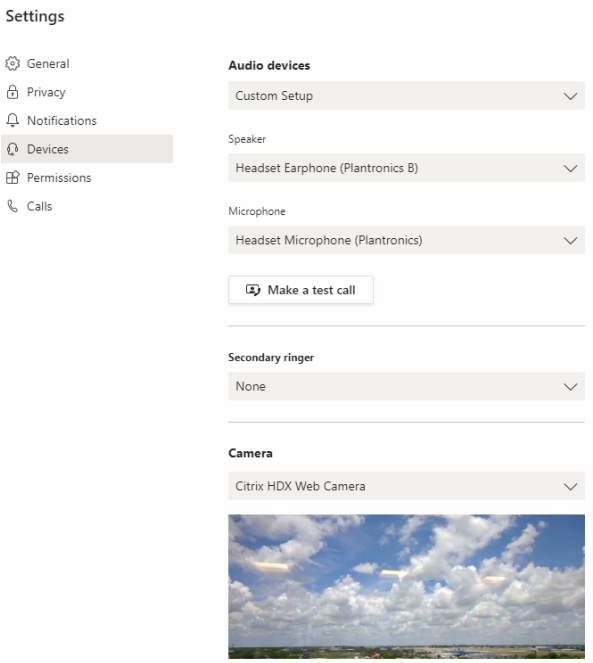
If Microsoft Teams fails to load in optimized VDI mode ("Citrix HDX Not Connected"in Microsoft Teams/About/Version), the VDA falls back to legacy HDX technologies. The legacy HDX technologies might be webcam redirection and client audio and microphone redirection. If you're using a Workspace app version/platform OS that does not support Microsoft Teams optimization, fallback 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 more 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 is 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:

- HID buttons - Answer and end calls aren't supported. Volume up and down are supported.
- QoS settings in the Admin Center for Microsoft Teams don't apply for VDI users.
- 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.

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 the 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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, go to https://www.microsoft.com/ 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.

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.
- 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 **include system audio** option isn't available.
- Simulcast isn't supported on ChromeOS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

> **Note:**
>
> Citrix recommends you 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, your calls, video calls, and screen sharing become unoptimized. This may result in call quality issues, increased latency, and increased load on the server.

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:

Component	Minimum version (1)	LTSR supported version (2)	Recommended version (3)
Microsoft Teams	1.5.00.11865	Not applicable	Latest
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
Citrix Workspace app for Windows	2112.1 CR	2203 CU2+ (4)	2309 CR+
Citrix Workspace app for Mac	2203 CR	Not applicable	2308 CR+
Citrix Workspace app for Linux	2202 CR	Not applicable	2308 CR+
Citrix Workspace app for ChromeOS or HTML5	2303 CR	Not applicable	2309 CR+

> **Notes:**
>
> 1. Minimum Version: This is the version where Multi-window was first introduced. Some minimum versions listed here can be end-of-life.
> 2. LTSR Supported Version: This is the LTSR version that is supported by Citrix for Multi-window. Older versions of these LTSR releases can work but support is no longer available for those versions once a new LTSR CU version is released. For more in-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> formation on LTSR support policies, see https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr.
> 3. Recommended Version: This is the version of software that Citrix recommends if the user/-customer chooses to upgrade their software. These are all CR versions.
> 4. Version 2203 LTSR for VDA and CWA base versions include the multi-window functionality. These versions have been superseded by the latest CU which is the officially supported version. Customers can continue to use these unsupported versions at their discretion. Citrix encourages customers on the LTSR release to upgrade to the latest CU.

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

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Additional information

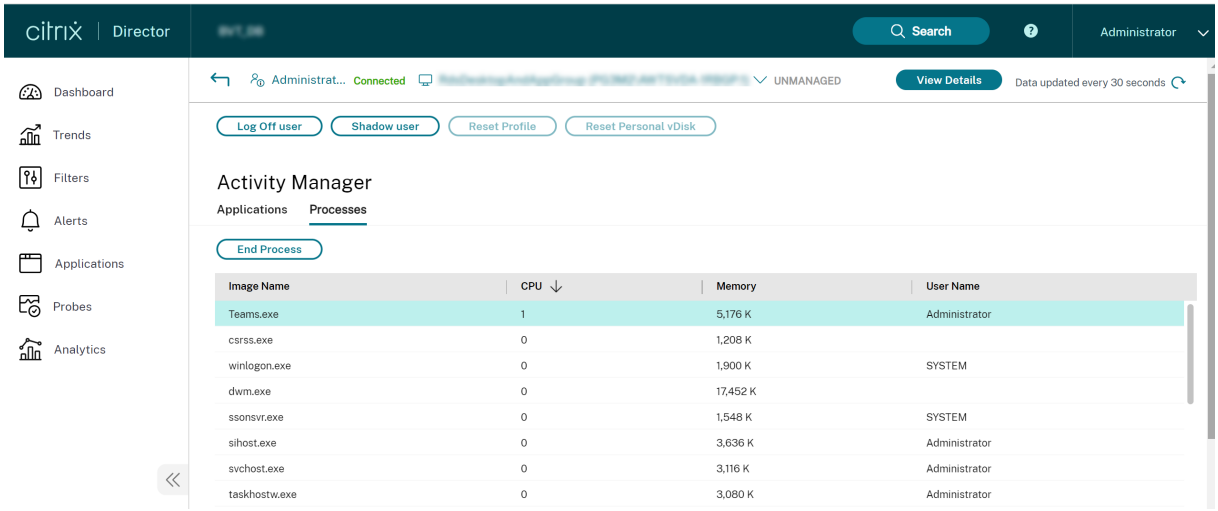
- Monitor, troubleshoot, and support Microsoft Teams
- Deploy the Microsoft Teams desktop app to the VM
- Install Microsoft Teams using MSI (VDI Installation section)
- Thin clients
- Skype for Business Network Assessment Tool
- Understand Microsoft Teams and Skype for Business coexistence and interoperability

Monitor, troubleshoot, and support Microsoft Teams

September 6, 2025

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.



Microsoft Teams Optimization status can be viewed in the Director > **User Details** page > **Session Details** panel > **MS Teams Optimization** field. Microsoft Teams being optimized is critical for better user experience such as clear audio and video. This feature is available for VDA version 2311 and later. Citrix Workspace™ app versions supported are listed in Optimization for Microsoft Teams. Director displays the status of the Microsoft Teams optimization only if Microsoft Teams is running as a published app

© 1997–2026 Citrix Systems, Inc. All rights reserved.

or inside a published desktop.
For more information, see Microsoft Teams optimization status.

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`.
With the VDA minimum version 1912, you can monitor active Microsoft 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`.

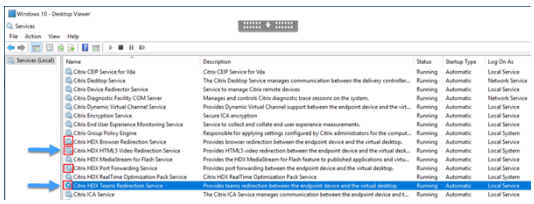
For more information, see *Monitoring* in the Knowledge Center article CTX253754.

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.
- **Citrix HDX HTML5 Video Redirection Service** runs as WebSocketService.exe listening on 127.0.0.1:9002 TCP. WebSocketService.exe performs two main functions:

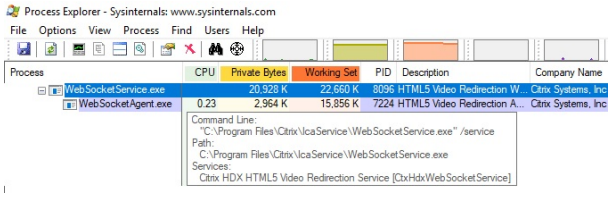
  i. **TLS termination for secure WebSockets** receives a secure WebSocket connection from vdiCitrixPeerConnection.js, which is a component inside the Microsoft Teams app. You can track it with the Process Monitor. For more information about certificates, see the section TLS and HTML5 video redirection, and browser content redirection.

  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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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\System32\CtxSvcHost.exe" -g PortFwdSvcs	This account (local Service)	Provides port forwarding between the endpoint device and the virtual 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 or HdxRtcEngine.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 or HdxRtcEngine.exe and the webrpc.dll binaries in the Workspace app installation path?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. If you validated step1, do the following to check if HdxTeams.exe or HdxRtcEngine.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 or HdxRtcEngine.exe being launched on the client endpoint, do the following:

    a) Restart the VDA.
    b) Restart the client endpoint.

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/HDX-Teams 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

   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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveLocalOffer

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
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveRemotelOffer
```

If there are multiple ICE candidates, the order of preference is:

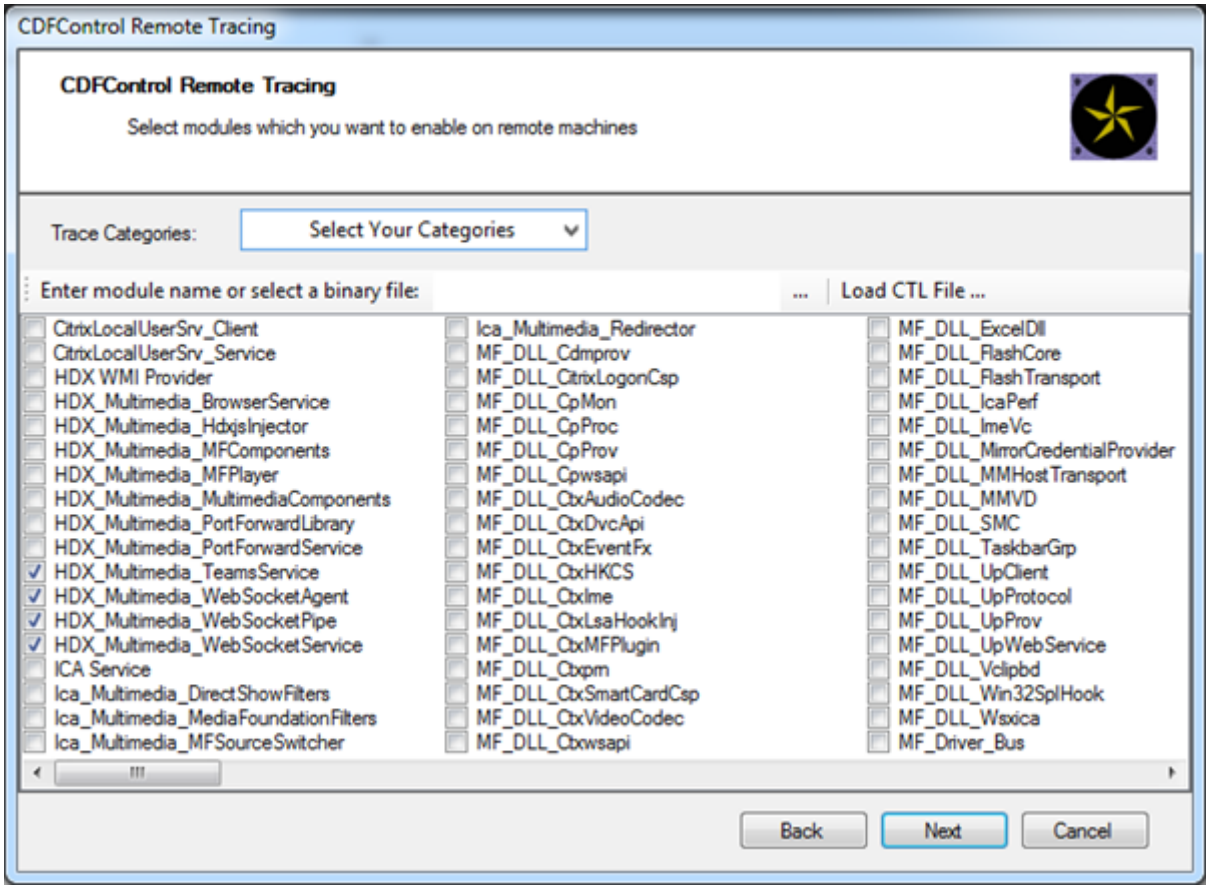
1. host
2. peer reflexive
3. server reflexive
4. transport relay

If you encounter an issue and can reproduce it consistently, we recommend that you click **Help > Report a problem** in Microsoft 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.

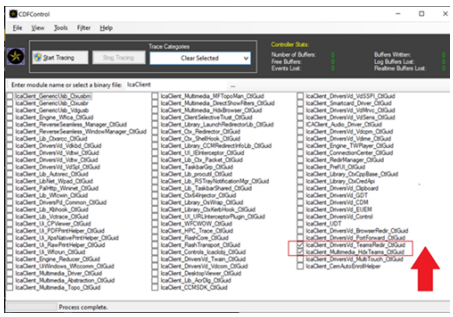
For recommendations for collecting CDF Traces, see the Knowledge Center article Recommendations for Collecting the CDF Traces.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA side CDF traces - Enable the following CDF trace providers:



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)

Windows Media redirection

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

Virtual Channel Plugin Manager

September 6, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 [New] 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
- DDC
  - Cloud 121 Release
  - 2407 CR
- Citrix Workspace™ App (Citrix Workspace App)
  - Citrix Workspace App for Windows 2409
- Citrix Workspace App Mac 2508

> **Note:**
>
> This feature is currently applicable to Windows endpoints.

Supported applications

- Currently supported applications are listed below:
  - Microsoft Teams - See new VDI solution for Teams

Virtual Channel Plugin Manager

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Virtual Channel Plugin Manager

September 6, 2025

Deployment

1. Check if the Microsoft Teams redirection policy is enabled: Refer Microsoft Teams redirection policy for more details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

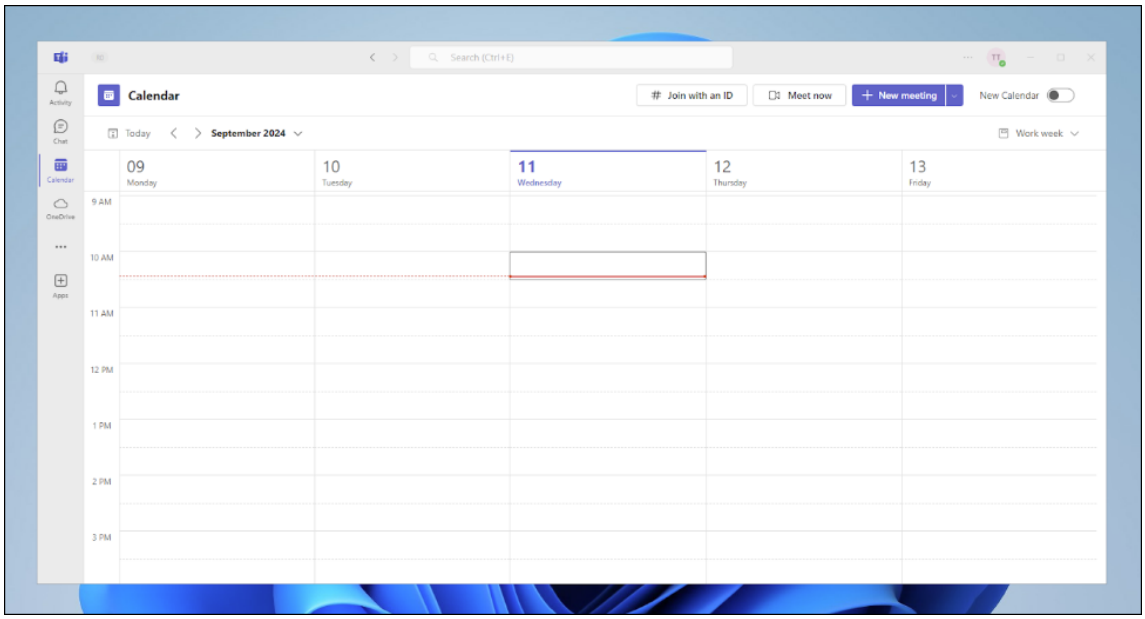
   This policy is available in the Multimedia Policy Settings on Citrix Studio. Enabling the policy allows you to specify the application name to be monitored For Example., "Microsoft Teams". This policy is disabled by default.

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.

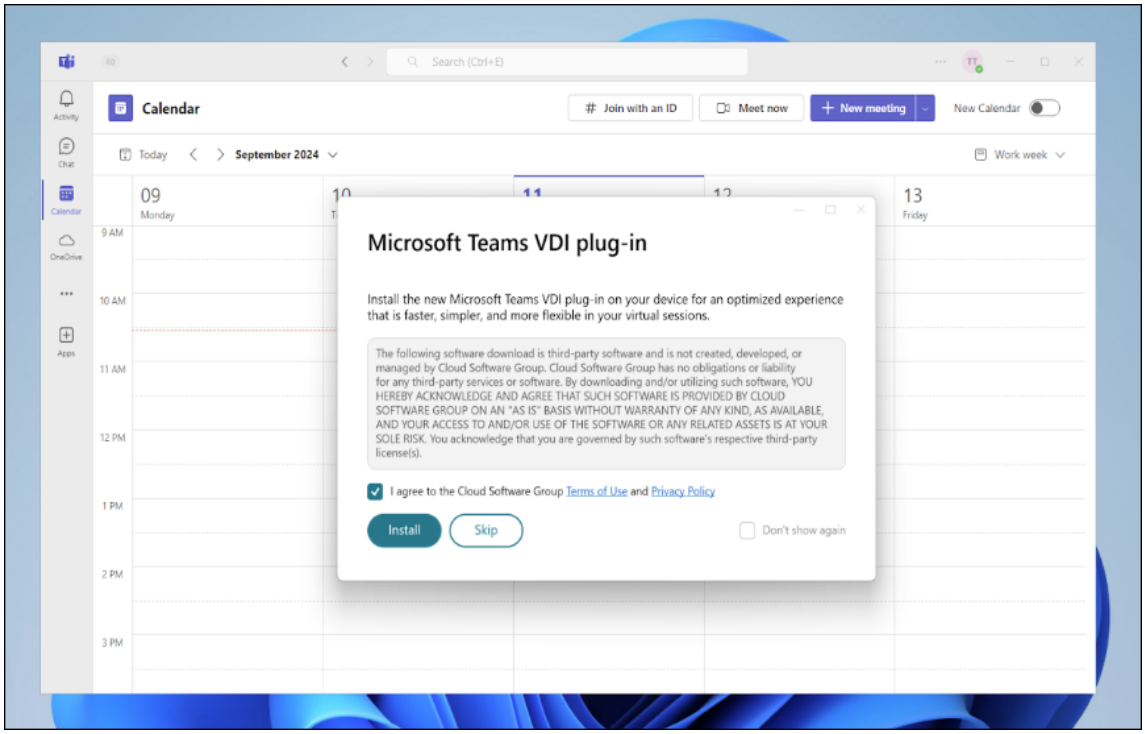
Procedure

1. User launches application on the Citrix session. For e.g., Microsoft Teams.

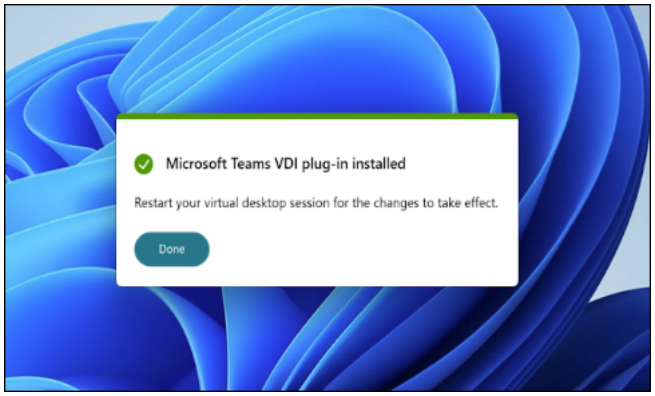


2. User receives a pop up to install the Teams VDI plugin on the endpoint for better experience. The pop up is above the session and not inside the session as the plugin will be installed on the endpoint.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unified Communications SDK Optimization

May 26, 2026

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 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,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Example: Pexip
- **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.
- 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 - 5.0.0 . For compatibility details for older versions of the SDK and specific feature requirements, see Versions and Feature Matrix table below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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 –5.0.0, fully compatible versions of Citrix components are as below:

- **Citrix Virtual Apps and Desktops:** 2603
- **Citrix Workspace App Windows:** 2603
- **Citrix Workspace App Mac:** To be released
- **Citrix Workspace App Linux:** 2603
- **Citrix Workspace App ChromeOS/HTML5:** To be released

> **Note:**
>
> UCSDK Optimization is supported on all endpoint platforms: Windows, Mac, Linux, ChromeOS, and HTML5. If the list above shows "To be released"for a specific endpoint platform, it simply means that a version fully compatible with the latest UCSDK features hasn't been released yet. Hence, customers can still use older versions of the Citrix Workspace app to continue using existing features, even with the newer UCSDK.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Starting with CVAD 2603, optimization for applications using the Citrix Unified Communications SDK (UCSDK) is no longer dependent on the "Microsoft Teams redirection"policy. Administrators can now disable Microsoft Teams optimization without affecting other UCSDK-integrated applications. Please note that to use this separation, the vendor application must utilize the Bootstrap method (first introduced in UCSDK 4.0) alongside CVAD 2603. For more detail, see Decoupled UCSDK and HDX Microsoft Teams Optimization

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.

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.

Feature Reference

Enhanced Call Connect times with Smart Sync

Introduced in UCSDK 5.0.0, the Smart Sync feature accelerates call connection times by streamlining communication between the VDA and the client endpoint. This enhancement delivers faster call setups across the board, providing the most significant performance improvements for high-latency network environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix recommends that customers reach out to their application vendors to upgrade to UCSDK 5.0.0 to take advantage of this feature.

> **Note:**
>
> This feature depends only on UCSDK 5.0.0 and the Citrix Workspace app. See the Versions and Feature Matrix for exact client versions. There is no VDA version dependency, so older supported VDAs can still be used.

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 ChromeOS/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 CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	N/A
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	UCSDK Version	VDA	CWA Windows	CWA Mac	CWA Linux	CWA ChromeOS/HTML5
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
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
Smart Sync	5.0.0	2203 LTSR latest CU / 2311 CR	2603	N/A	2604	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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

Vendor	Documentation
Sprinklr	Citrix Media Offloading for Voice Calls - Sprinklr
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
Zoom Web App	Configure WebRTC redirection for Zoom Web App

Troubleshooting

For troubleshooting information, see Troubleshooting Guidance for Apps Optimized with Citrix Unified Communications SDK.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known Issues & Limitations

This section will document the current known issues and limitations as they are recognized.

General content redirection

September 6, 2025

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.

Client folder redirection

September 6, 2025

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 redirection on the server. Then, on the client device, specify which folders to redirect. The application (CtxCFRUI.exe) you use to specify the client folder options is included with the Citrix Workspace app supplied with this release.

Requirements:

For servers:

- Windows Server 2022
- Windows Server 2019, Standard and Datacenter Editions

For Clients:

- Windows 10
- Windows 11

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 **(..\Citrix\ICA Client\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.

Client location redirection

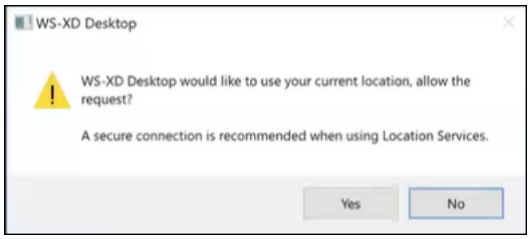
September 6, 2025

Client location redirection, when enabled, allows VDA-hosted apps and desktop sessions to seamlessly access the client's current location. On a multi-session operating system (TS VDA or Multi-Session WS VDA), each session has its own unique location provided by the connected client. Using this feature, applications on the VDA that depend on location have the accurate location of the client.

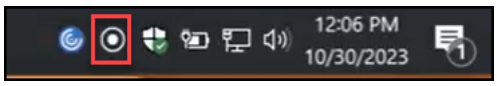
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see the Microsoft documentation.

After client location redirection is enabled and location access is allowed on both the server and client side, when you launch a location-accessing application or desktop, the client prompts you to share its current location with the following dialog box:



When you enable the client location redirection, the following icon appears in the client's taskbar if/when the VDA-hosted app or desktop queries current location information.



System requirements

For servers:

- Single-Session (Win10/11) or Multi-Session (Win 11 22H2 and Server 2022 23H2 or later) OS VDA
- Citrix Workspace™ app for Windows, iOS, or Android

Configuration

Client location redirection must be enabled using the Citrix® policy for the feature to work. Client location redirection is disabled by default.

To enable client location redirection, complete the following steps:

On the Windows VDA and Client side:

1. In **Settings > Privacy > Location**, enable the following options:
    - **Allow access to location on this device**
    - **Allow apps to access your location**
    - **Allow desktop apps to access your location**
2. For multi-session OS, enable the **Location Override** setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On the Controller/DDC side:

Enable the **Studio > Policies > Location > Settings > Allow application to use the physical location of the client device** policy.
For more information, see Client sensors policy settings.

Bidirectional content redirection

July 29, 2026

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 2311 or above
- Citrix Workspace™ app for Linux 2503 or above
- Citrix Workspace™ app for Mac 2607 or above

Browsers:

- Google Chrome with Citrix Browser Redirection Extension
  - Google Chrome Extension
- Microsoft Edge with Citrix Browser Redirection Extension
  - Microsoft Edge Extension

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration

Starting in Citrix Virtual Apps and Desktops™ version 2311, bidirectional content redirection is configured through Citrix Studio only. Prior releases had policy settings configured on both the client endpoint and Studio. Bidirectional content redirection is disabled by default.

For VDA configuration, see Bidirectional content redirection in the **ICA policy** settings.

For browser redirection to work, browser extensions must be registered on the originating browser (where the URL is redirected from) using the commands shown. Run the commands as needed on the VDA and client, based on the browser in use.

Browser	VDA	Client
Google Chrome	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
Microsoft Edge	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe"/regEdge
All Available Browsers	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe" /regall	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe"/regall

To unregister a browser extension:

Browser	VDA	Client
Google Chrome	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
Microsoft Edge	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
All Available Browsers	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe" /unregall	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe"/unregall

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note:

- Run these commands in a Command Prompt (CMD) window with administrator privileges.
- The register command causes Chrome and Edge browsers to prompt users to enable the Citrix Browser Redirection Extension during first launch.
- The registration command also links the Browser Redirection Extension to the native messaging host, which allows the extension to communicate with the native code. Without this, the browser blocks the communication.
- You can also install the browser extension manually from the Google Chrome Web Store. To use the Browser Redirection Extension from the Microsoft Edge Add-ons store, you need Virtual Delivery Agent (VDA) version 2503 or later. For older VDA versions, install the extension from the Google Chrome Web Store within your Microsoft Edge browser (see Add an extension to Microsoft Edge from the Chrome Web Store).
- The Citrix Workspace app versions listed in the system requirements are the minimum versions required to support both bidirectional content redirection and OAuth redirection.
- For Mac: due to macOS security requirements for notarized applications, custom OAuth callback URL schemes must be pre-registered with Citrix and cannot be changed dynamically post-installation. Only `citrix-oauth-redir` is supported by default. Please reach out to the Citrix Product team to register your URL scheme.

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.

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 Web Studio, set the custom protocol in **Bidirectional content redirection**.

Note:

- You must have administrator privileges to run these commands.
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - 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.
- 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.

Host to client redirection

September 6, 2025

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.
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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>

<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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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"/>

<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. The 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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
- 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 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.

Local App Access and URL redirection

September 13, 2025

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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 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.
    - 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. By default, Local App Access is prohibited.

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.
  - 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Install the 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. Sign in to Web Studio and click **Policies** in the left pane.
2. In the action bar, click **Create Policy**.
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 these steps:

1. Enable URL redirection when you install the 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`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For CitrixReceiverWeb.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

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.
> - 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/CitrixBase.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_clientHostedApps "-value "true"`.

To have access to **Add Local App Access Application** in a Cloud service deployment, use the Citrix DaaS Remote PowerShell SDK. For more information, see Citrix DaaS Remote PowerShell SDK.

1. Download the installer:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. Run these commands:

   a) `asnp citrix.*`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b) `Get-XdAuthentication`

3. Enter the following command: `set-configsitemetadata -name "studio_clientHostedApps "-value "true"`.

After you complete the applicable preceding steps, follow these steps to continue.

1. Sign in to Web Studio and 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 context menu. You can also click **Add Local App Access Application** in the action bar. To display the Add Local App Access Application option in the action bar, 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 is visible on the Start menu, the desktop, or both.
    - 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 the Citrix Workspace app from the command line using the /ALLOW_CLIENTHOSTEDAPPSURL=1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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 the 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.

- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

Overview

September 13, 2025

Effective print management is a cornerstone of productive and efficient IT operations within Citrix Virtual Apps and Desktops™ (CVAD) environments. Users require seamless and reliable access to printing resources, while administrators need robust tools to configure, manage, secure, and troubleshoot the printing infrastructure.

This document serves as a comprehensive, expert-level guide designed to revamp existing knowledge bases and provide IT administrators with a thorough understanding of all facets of CVAD printing.

Printing remains a fundamental requirement for many business workflows. Within Citrix Virtual Apps and Desktops (CVAD) environments, efficiently managing print requests from virtual sessions to physical devices presents unique challenges due to the separation between the user's session and the physical printer hardware.

CVAD provides a comprehensive suite of technologies and policies designed to bridge this gap, offering flexibility to accommodate diverse printer types, network conditions, and user requirements while aiming for optimal performance and administrative simplicity.

Citrix Universal™ Print Driver (UPD)

September 6, 2025

The Citrix Universal Print Driver (UPD) is not a single driver but a technology comprising components on both the server (VDA) and the client (endpoint with Workspace app).

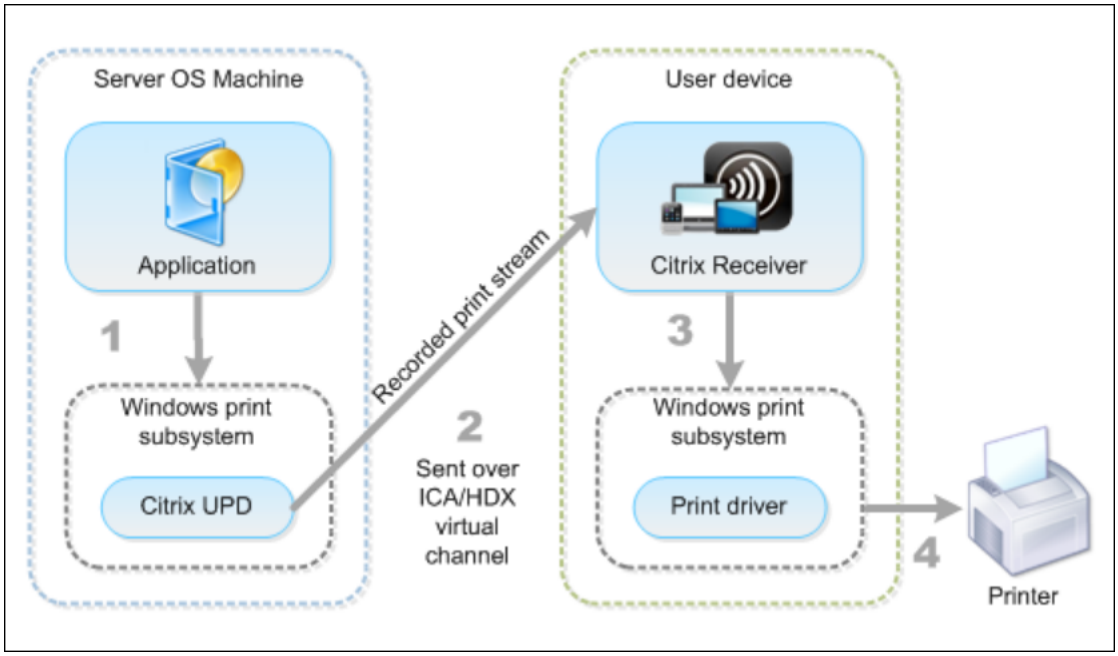
- **Server Component:** Installed with the VDA, this includes the actual generic print drivers, such as the "Citrix Universal Printer"(which uses the EMF format) and the "Citrix XPS Universal Printer"(which uses the XPS format), along with support for PDF and PS formats. Its role is to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

capture the print output generated by applications running on the VDA in a device-independent format.

- **Client Component:** Included within the Citrix Workspace™ app installation, this component receives the print stream sent from the VDA. It then interacts with the local Windows printing subsystem on the endpoint device to render the print job using the appropriate device-specific driver installed locally for the target printer.

The following illustration shows the Universal Print driver components and a typical workflow for a printer locally attached to a device -



The primary goal of the UPD is to simplify printer driver management within the Citrix® environment. By using a built-in driver on the VDA, administrators can avoid installing and maintaining potentially hundreds of different manufacturer-specific drivers, which are a common source of instability and conflicts. The UPD aims to be compatible with a wide range of printers, providing a universal interface between the virtual session and the client's printing capabilities.

Supported Formats

The UPD technology supports several print data formats, allowing flexibility in how print jobs are processed and rendered:

- **EMF (Enhanced Metafile Format):** The default format used by the "Citrix Universal Printer" driver. It's a 32-bit Windows-native vector format. Printing using EMF is generally efficient but typically requires a Windows-based client endpoint for rendering.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **XPS (XML Paper Specification):** Used by the "Citrix XPS Universal Printer" driver. XPS is an XML-based page description language developed by Microsoft, similar in concept to PDF, designed to be platform-independent.
- **PS (PostScript):** A page description language developed by Adobe, known for its capabilities in handling complex graphics and typography, often used in publishing and by various printers and multifunction peripherals. Linux clients often utilize PostScript printing with UPD.
- **PDF:** PDF is a widely used open standard for document exchange. It encapsulates a complete description of a fixed-layout flat document, including the text, fonts, graphics, and other information needed to display it. It is designed to be platform-independent and is ideal for preserving document fidelity across different systems and applications.

Using the UPD offers several potential advantages:

- **Reduced Driver Management:** Significantly decreases the number of drivers needed on VDA images, simplifying image creation and maintenance.
- **Improved Stability:** Fewer drivers mean fewer potential conflicts and a lower risk of driver-related spooler crashes or system instability.
- **Optimized Print Jobs:** Certain UPD formats, particularly EMF, can sometimes result in smaller print job sizes compared to native drivers.
- **Advanced Feature Support:** The EMF and XPS UPD components can support advanced printing features (like stapling, tray selection) if the native driver on the client exposes these capabilities through Microsoft's standard Print Capability technology.

Configuration

September 6, 2025

Choosing the most appropriate printing configuration options for your needs and environment can simplify administration.

The options you can choose from are:

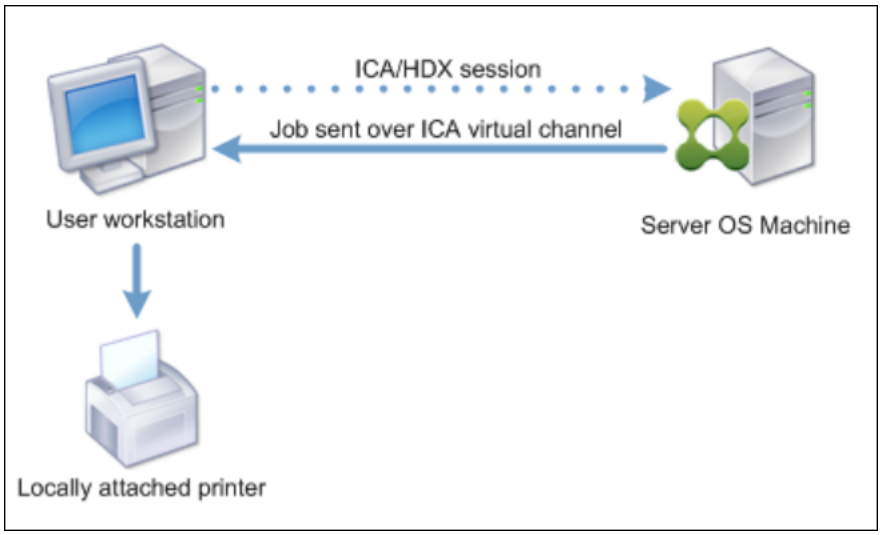
- Citrix Universal™ Print Servers
- Client Printer Redirection
- Network Printers

Client printer redirection

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This is often the default mechanism, where printers configured on the user's endpoint device are automatically mapped into the Citrix® session when the user logs on. This includes printers directly attached to the client (USB, LPT, etc.) as well as network printers that are mapped on the client machine. End users typically cannot manually select which local printers get redirected; this is controlled by administrative policy.



Steps to setup

This functionality is enabled by default. Related settings and configurations can be found in the "Client Printers"template. The policy settings in this template can be used to further customize and optimize the client print redirection experience.

Policies associated with client printer redirection can be found Client printers policy settings.

Considerations

The primary challenge is the potential for performance degradation and instability if a large number of printers are mapped on the client endpoint and redirected. Additionally, printer mapping failures can occur due to driver incompatibilities or client-side issues. The reliability depends heavily on the configuration and health of the client device. Some administrators prefer to avoid autocreation of client printers altogether due to the potential load and driver management complexities.

Use Case

Users needing access to printers directly connected to their local machine (USB, LPT, COM, network printers mapped only on the client).

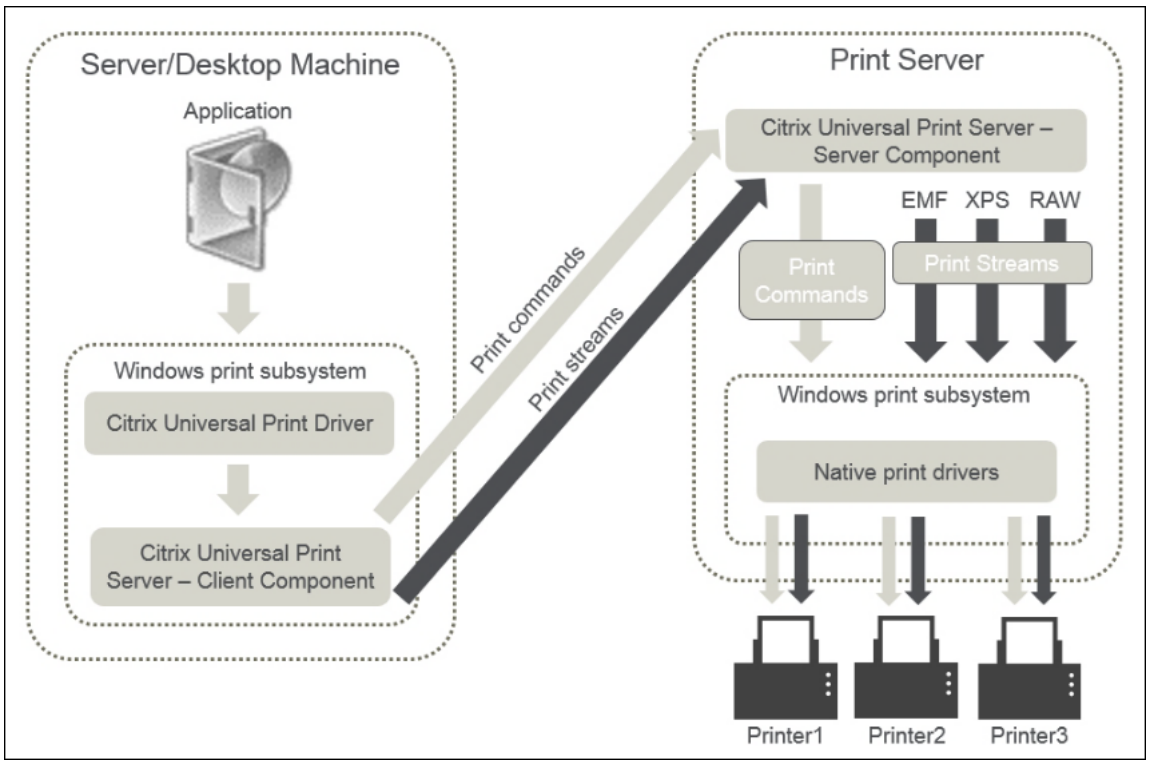
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Universal™ Print Server (UPS)

September 6, 2025

UPS is an optional Citrix® component designed to optimize and manage network printing. It consists of two parts:

- **UPServer** component is installed on one or more Windows Print Servers in the network.
- **UPClient** component, which is part of the VDA installation. When enabled via policy, VDAs communicate with the UPServer to establish connections to network printers, typically leveraging the Citrix Universal Print Driver (UPD).



UPS offers several advantages, particularly for network printing across WAN links or in large environments:

- Network Optimization: Print data sent between the VDA and UPServer is optimized and compressed, reducing bandwidth consumption, especially important over WAN connections.
- Centralized Driver Management: Allows leveraging the Citrix UPD for network printers, reducing the need to install and manage numerous native printer drivers on the VDAs.
- High Availability: Supports load balancing across multiple UPServers and automatic failover if a server becomes unavailable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements

- Microsoft Visual C++ 2015–2022 Redistributable
- Microsoft .NET Framework 4.8 (minimum)
- OS requirement for UPServer
    - Windows Server 2025
    - Windows Server 2022
    - Windows Server 2019

Configuration/ Steps to setup

This functionality is disabled by default. Related settings and configurations can be found in the "Universal Print Server"template. The policy settings in this template can be used to further customize and optimize the Universal Print server experience.

Beyond the enable setting, several policy settings fine-tune UPS behavior:

- Port configuration for communication (HTTP/SOAP, CGP, and their SSL/TLS equivalents).
- Input bandwidth limits for print streams.
- List of UPServers for load balancing.
  Out-of-service threshold for failover detection.
- Web service connection timeouts.
- SSL/TLS configuration settings for secure communication.

For more information, see Citrix UPS policy settings.

Best practices

- Use UPS for network printing across WAN links to optimize performance.
- Utilize the Citrix Universal Print Driver (UPD) to reduce driver management on VDAs.
- Configure load balancing across multiple UPServers for high availability.

Use cases

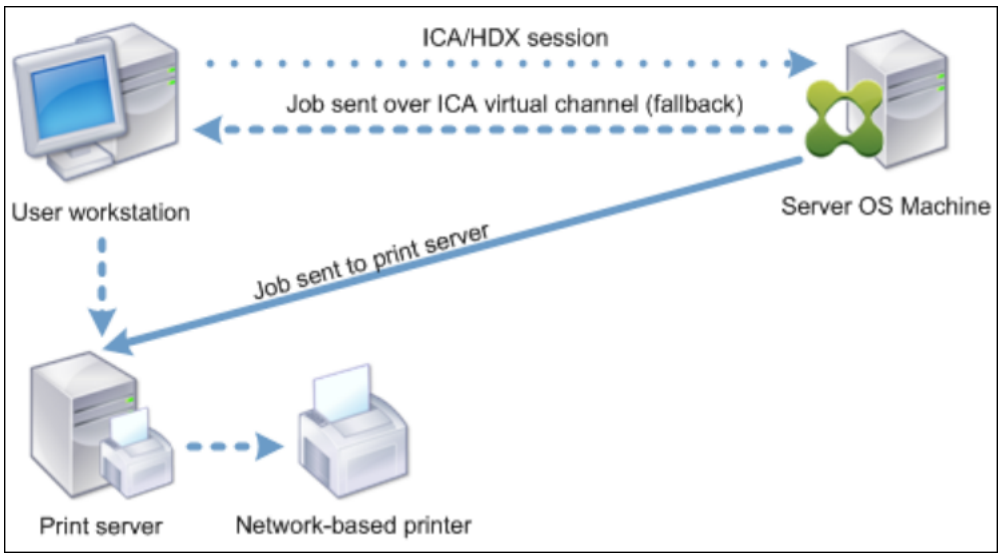
Citrix explicitly recommends UPS for remote print server scenarios involving WAN links.It's also ideal for environments seeking to minimize VDA driver footprint, improve network printing performance, provide high availability for network printing, or implement proximity printing based on network location. Thin clients that cannot directly connect to network printers can leverage UPS via the VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network Printers (on the VDA)

September 6, 2025

Here, the print job is sent directly from the VDA across the network to a network print server (either a standard Windows Print Server or a Citrix Universal™ Print Server). This pathway is generally faster for printers located on the same Local Area Network (LAN) as the VDA. This is the default pathway for network printers when direct connections are enabled. Print jobs fall back to being routed over the ICA connection if the published application or desktop cannot access the print server or if the native printer driver is not installed on the multi-session OS machine.



Requirements

- The necessary printer driver depends on the type of print server hosting the network printer:
  - If the printer is hosted on a standard Windows Print Server, the corresponding native printer driver must be installed on the VDA.
  - If the printer is hosted on a Citrix Universal Print Server (UPS), the connection can use either the native driver or the Citrix UPD.
- Network connectivity from the VDA to the print server.
- Appropriate permissions for the logged in user.

Guidance on connecting and configuring network printers (Policy settings)

- Connect printers via UNC paths (ex. “\PrintServer\PrinterName”)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Session printers:** The primary policy for this method. Administrators add printers by typing the UNC path or browsing the network. Filters can be applied to the policy to target specific users, groups, client IPs, etc.
- **Printer assignments:** An alternative policy, useful for assigning a large group of printers to multiple users or devices simultaneously. It allows setting both the session printers and the default printer for those assignments.

Best practices (Allow direct connections to N/W printers)

- Consider the "Direct connections to network printers"policy for routing (direct VDA-to-server or via client/ICA).
    - When enabled (default setting), printing performance will be optimal over LAN. The print traffic in this scenario is uncompressed.
    - Disable this policy setting if the VDA and the print server are not in the same network (WAN scenario). This would force the print traffic to flow through the client endpoint and leverage ICA® compression but will introduce latency.

Enabling direct connections favors LAN performance but uses uncompressed network traffic between the VDA and print server. Disabling it forces traffic through the client pathway, leveraging ICA compression, which is beneficial for WAN scenarios but adds latency.

Use case

Accessing shared departmental or office printers directly from the virtual session. Requires native drivers to be installed on the VDA.

Limitations

Printing performance will be poor in adverse network conditions (WAN). Additionally, driver management is a huge overhead for IT admins.

Troubleshooting

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Systematic Approach

Troubleshooting printing problems in a complex Citrix Virtual Apps and Desktops™ (CVAD) environment requires a methodical approach rather than random guessing. A recommended process involves:

1. **Identify Symptoms:** Clearly define the problem (e.g., printer not appearing, job stuck, wrong output, slow printing).
2. **Isolate Scope:** Determine who is affected (one user, multiple users, specific application), which printers are involved, and from which VDAs or client devices the issue occurs.
3. **Check Basics:** Verify network connectivity (VDA to print server, client to VDA), ensure the printer is online and functional outside Citrix®, check local printing from the client (for redirection issues).
4. **Review Policies:** Examine relevant Citrix policy settings applied to the affected user/session using tools like Citrix Group Policy Modeling wizard or by checking applied policy settings on the VDA. Ensure policy settings are configured as intended and that there are no obvious conflicts.
5. **Examine Logs:** Check Windows Event Logs (Application and System logs, PrintService logs) on the VDA, client device, and print server (if applicable). Check Citrix-specific logs if enabled.3
6. **Test Components:** Attempt to isolate the issue to a specific component –try printing from a different application, try a different printer, test with a generic driver (like UPD or Microsoft XPS Document Writer), check the status of the Print Spooler and Citrix Print Manager services.
7. **Consult Resources:** Leverage product documentation, support articles, and community forums for known issues and solutions.

Common Issues and Solutions

Some of the common printing issues reported in the field and recommended troubleshooting steps are documented below:

- **Failure to Auto-Create Printers / Printers Not Appearing in Session:**
    - **Potential Causes:** Client printer redirection policy disabled; Auto-create client printers policy set to 'None'or incorrectly filtered; Client device print spooler issue; Workspace app problem; Network connectivity issue between client and VDA; Citrix Print Manager Service (CpSvc.exe) not running or crashed on VDA; Required printer driver missing on VDA (if native driver needed); Citrix policy not applying correctly to the session.
    - **Troubleshooting Steps:**
        1. Verify Client printer redirection policy is 'Allowed'and Auto-create client printers is configured correctly for the user/session.
        2. Check CpSvc.exe service status on VDA; restart if necessary.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Check Windows Print Spooler service status on both VDA and client; restart if necessary.
4. Verify basic network connectivity.
5. Test printing locally on the client device.
6. Ensure a compatible Workspace app version is installed.
7. Check VDA event logs for errors related to CpSvc or printer creation.
8. Force policy update on VDA (gpupdate /force).
9. Check applied policies on VDA to confirm expected settings are present.
10. If native drivers are expected, verify they are installed on the VDA.
11. Check RDS/Terminal Server printer redirection settings in local/group policy on VDA.
12. Look for and clean up orphaned printer entries in the VDA registry.

- **Print Spooler Crashes / Service Unresponsive (on VDA or Print Server):**
  - **Potential Causes:** Faulty or incompatible printer driver (often third-party); Corrupted print job in the queue; Driver conflicts; Insufficient system resources.
  - **Troubleshooting Steps:**
    1. Identify the faulting process/module using Windows Event Logs (Application log often shows spooler crashes).
    2. Attempt to restart the Print Spooler service.
    3. If restarting fails or the issue repeats, try to clear the print queue manually (Stop Spooler service, delete files in C:\Windows\System32\spool\PRINTERS, Start Spooler service).
    4. Identify and remove the problematic printer driver. Clean removal may require registry edits.
    5. Test with the Citrix UPD or a generic Microsoft driver.
    6. Check for and clean up orphaned print processors in the registry.
- **Policy Conflicts / Settings Ignored:**
  - **Potential Causes:** GPO settings overriding Citrix policies; Conflicting Citrix policy priorities or filters; Errors during policy processing.
  - **Troubleshooting Steps:**
    1. Use Citrix Group Policy Modeling wizard to simulate policy application for the affected user/VDA.
    2. Verify policy filters (user groups, client IPs, etc.) are correct.
    3. Check policy priorities in Studio/Web Studio.
    4. Temporarily block GPO inheritance on the VDA's OU to isolate Citrix policy issues.
    5. Examine policy processing results on the VDA (e.g., using gpresult /h report.html).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Simplify the policy set applied to the user/VDA and add policies back incrementally to find the conflict.

- **Driver Issues (General - Compatibility, Corruption, Mapping):**
  - **Potential Causes:** Driver not compatible with VDA OS or Citrix version; Corrupted driver installation; Driver required by policy is missing on VDA; Conflict between multiple drivers; Incorrect configuration of Printer driver mapping policy.
  - **Troubleshooting Steps:**
    1. Try printing with Citrix UPD (configure Universal print driver usage policy).
    2. Verify the correct driver (native or UPD) is being selected based on applied policies.
    3. Ensure required native drivers are installed correctly on the VDA (if used).
    4. Check vendor documentation for driver compatibility with CVAD and the VDA OS version.
    5. Perform a clean reinstall of the problematic driver (uninstall, reboot, install).
    6. Review and test Printer driver mapping policy rules carefully.
    7. Minimize the number of installed drivers on the VDA.
- **Slow Printing / Performance Issues:**
  - **Potential Causes:** Network congestion or high latency (especially WAN); Large, complex print jobs (e.g., high-resolution graphics); Inefficient printer driver; Print optimizations (compression, caching) disabled or misconfigured; Inefficient routing (e.g., direct connection over slow WAN).
  - **Troubleshooting Steps:**
    1. Analyze network path and performance between VDA, client, and print server.
    2. Configure Citrix bandwidth limiting policies for printing.
    3. Enable and configure UPD optimizations (image compression, font/image caching) via Universal Printing policies.
    4. For WAN links, disable Direct connections to print servers policy to force traffic over compressed ICA® channel.
    5. If using UPS, ensure it's optimally configured for the network.
    6. Analyze the print job itself –reduce resolution or complexity if possible.
    7. Test with a different driver (e.g., UPD vs. native).
- **Incorrect Output (Missing Characters, Formatting Errors, Wrong Orientation):**
  - **Potential Causes:** Missing fonts on VDA required by the document/application; Incorrect font substitution; Printer driver incompatibility; Issue with specific UPD format (e.g., EMF vs. XPS); Application bug; Conflict with advanced printing features enabled on the local client printer.
  - **Troubleshooting Steps:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Ensure all necessary fonts are installed on the VDA.
2. Try changing the Universal driver preference policy order (e.g., try XPS before EMF).
3. Test printing the same document from a different application.
4. Test printing to a different physical printer or a virtual printer (e.g., Microsoft XPS Document Writer).
5. Try using a different printer driver (UPD vs. native, or different native version).
6. Check the application's print settings and page setup.
7. Disable "Advanced Printing Features"in the local printer properties on the client device.
8. Verify print orientation settings in user preferences and policies.

- **Citrix Print Manager Service (CpSvc.exe) Crashes/Hangs:**
  - **Potential Causes:** Unresponsive printer drivers leaving orphaned objects in the registry; Corrupted Citrix policy data related to printing; System resource contention.
  - **Troubleshooting Steps:**
    1. Follow steps to clean orphaned printer and print processor entries from the VDA registry. Requires stopping Print Spooler and CpSvc services first.
    2. Identify and remove the offending printer driver(s).
    3. Consider cleaning the Citrix policy cache folders/registry keys on the VDA and forcing a policy refresh.
    4. Monitor VDA resource usage (CPU, Memory).
    5. Restart CpSvc and Print Spooler services.
- **PDF Printer Issues:**
  - **Potential Causes:** Auto-create PDF Universal Printer policy disabled; Incompatible VDA or Workspace app version; No PDF viewer installed on the client endpoint; Unsupported browser used (e.g., Edge) or HTML5 configuration error (CSP headers, config.js).
  - **Troubleshooting Steps:**
    1. Verify the Auto-create PDF Universal Printer policy is enabled and applied.
    2. Confirm VDA and Workspace app meet minimum version requirements.
    3. Ensure a supported PDF viewer (e.g., Adobe Reader, Chrome) is installed and set as default on the client.
    4. If using HTML5 Workspace app, verify browser compatibility and check configuration.js and CSP header settings.
    5. Restart the Citrix session after policy changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Basic End user troubleshooting

If permitted by organizational policy, users experiencing simple printing issues can sometimes resolve them with basic steps before escalating to IT -

- Log off completely from the HDX™ session and log back in.
- Check the status of the local printer on the endpoint device (ensure it's online, not paused, no errors).
- Restart the local endpoint device.

Best practices

September 6, 2025

- **Utilize Universal Print Server (UPS):** Recommended, especially for network printing across WANs, due to optimization and centralized management benefits.
- **Employ Universal Print Driver (UPD):** Use UPD as the primary driver strategy to minimize driver count and conflicts.
- **Use Vetted Native Drivers Selectively:** If native drivers are required for specific printer features, ensure they are thoroughly tested.
- **Minimize Driver Footprint:** Install the fewest possible number of printer drivers on VDA images.
- **Leverage Driver Mapping:** Use the Printer driver mapping and compatibility policy to substitute problematic drivers or enforce UPD usage.
- **Test Rigorously:** Never deploy untested drivers into production.
- **Manage Driver Updates Carefully:** Avoid in-place updates; prefer a clean uninstall, reboot, and reinstall process.
- **Clean Up Unused Drivers:** Regularly remove drivers that are no longer needed.
- **Optimize Routing:** Ensure print jobs take the most efficient path (e.g., direct VDA-to-print server on LAN via Direct connections to print servers enabled; route via ICA/client for WAN by disabling direct connections).
- **Consider Distributed Print Servers:** For large, geographically dispersed organizations without UPS, placing print servers at each physical location can aid management and load distribution (though UPS with load balancing offers a more integrated Citrix® solution).
- **Purge Old Print Jobs:** Periodically clear stuck or old jobs from print queues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Design Considerations

- **Tailor Provisioning:** Choose provisioning methods (Autocreation, Session Printers, UPS, PDF Printer) based on user requirements (e.g., roaming users benefit from proximity printing or PDF printing; static workstations might use Session Printers).
- **Plan Routing:** Design print job routing based on the network locations of endpoints, VDAs, and print servers.
- **Ensure Redundancy:** Implement print server redundancy, particularly when using UPS, via load balancing policies.

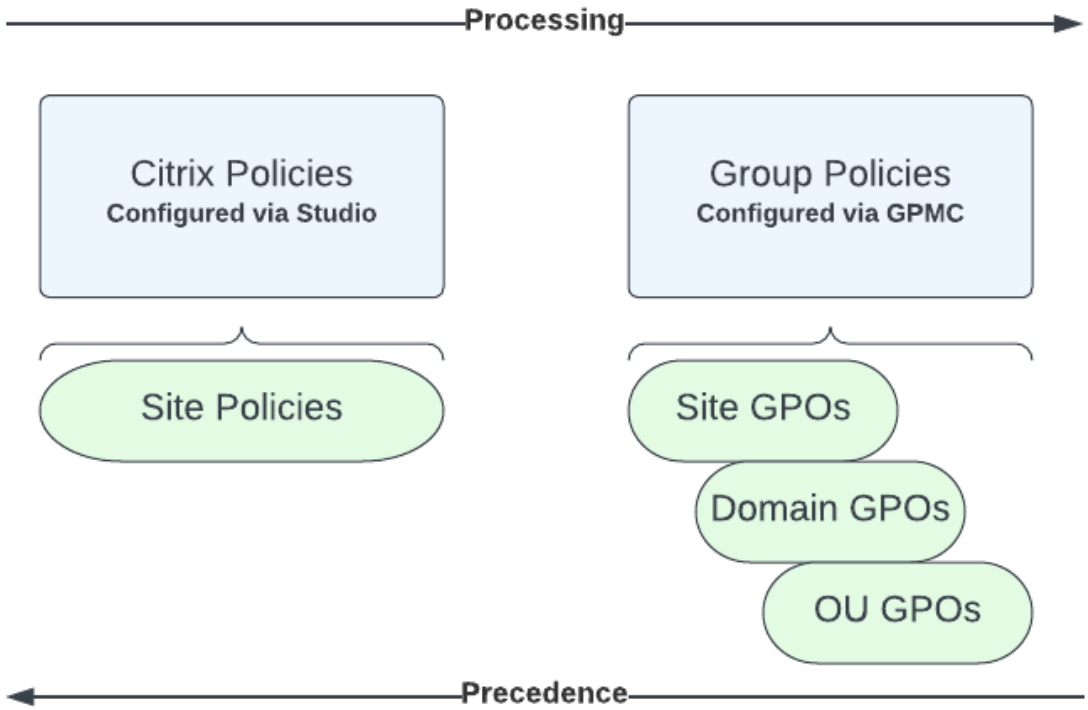
Policies

September 6, 2025

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 physical and virtual machines or to users. You can apply settings to individual users at the local level or in security groups in an Active Directory. The configurations define specific criteria and rules. If you don't specifically assign the policies, the settings are applied to all connections.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 Local 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.

Studio uses a Modeling Wizard to help administrators compare configuration settings within templates and policies to help eliminate conflicting and redundant settings. Administrators can set GPOs using the GPMC to configure settings. Also, apply them to a target set of users at different levels of the network.

These GPOs are saved in the Active Directory. Access to the management of these settings is restricted for most of the IT personnel for security.

Settings are merged according to priority and their condition. Any disabled setting overrides a lower-ranked enabled setting. Unconfigured policy settings are ignored and don't override lower-ranked settings.

Local policies can also have conflicts with group policies in the Active Directory, which might override

© 1997–2026 Citrix Systems, Inc. All rights reserved.

each other depending on the situation.

All policies are processed in the following order:

1. The end user logs on to a machine using domain credentials.
2. Credentials are sent to the domain controller.
3. Active Directory applies all policies (end user, endpoint, organizational unit, and domain).
4. The end user logs on to Citrix Workspace™ app and accesses an application or desktop.
5. Citrix and Microsoft policies are processed for the end user and machine hosting the resource.
6. Active Directory determines precedence for policy settings. It then applies them to the registries of the endpoint device and to the machine hosting the resource.
7. The end user logs off from the resource. Citrix policies for the end user and endpoint device are no longer active.
8. The end user logs off the user device, which releases the GPO user policies.
9. The end user turns off the device, which releases the GPO machine policies.

When creating policies for groups of users, devices, and machines, some members might have different requirements and would need exceptions to some policy settings. Exceptions are made by way of filters in the Studio and the GPMC that determine who or what the policy affects.

> **Note:**
>
> We do not support mixing Windows and Citrix policies in the same GPO.

Work with policies

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Configure Citrix policies to control user access and session environments. Citrix policies are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types. Each policy can contain multiple settings.

Tools for working with Citrix policies

You can use the following tools with Citrix policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web Studio.** If you are a Citrix administrator without permission to manage group policy, use Web Studio to create policies for your site. Policies that are created using Web Studio are stored in the site database, and the updates are pushed to the VDA either when that VDA registers with the broker or when a user connects to that VDA.
- **Local Group Policy Editor** (Microsoft Management Console snap-in). If your network environment uses Active Directory and you have permission to manage group policy, you can use the Local Group Policy Editor to create policies for your site. The settings you configure affect the Group Policy Objects (GPOs) you specify in the Group Policy Management Console.

> **Important:**
>
> We recommend using the Local Group Policy Editor to configure some policy settings. Examples include settings related to registering VDAs with a controller and settings related to Microsoft App-V servers.
> Additional policy validations are added. As a result, doing an in-place upgrade might lead to loss of policy data if invalid policy settings are present. If you create or edit the policies using a method other than Web Studio, Citrix recommends you to use the latest version of the SDK and snap-in.

Policy processing order and precedence

Group policy settings are processed in the following order:

1. Local GPO
2. Virtual Apps and Desktops site GPO (stored in the Site database)
3. Site-level GPOs
4. Domain-level GPOs
5. Organizational Units

However, if a conflict occurs, policy settings processed last overwrite the settings processed earlier. The order of precedence for policy settings is as follows:

1. Organizational Units
2. Domain-level GPOs
3. Site-level GPOs
4. Virtual Apps and Desktops site GPO (stored in the Site database)
5. Local GPO

For example, a Citrix administrator uses Web Studio to create a policy (Policy A) that enables client file redirection for the company's sales employees. Meanwhile, another administrator uses the Group Policy Editor to create a policy (Policy B) that disables client file redirection for sales employees. When the sales employees log on to the virtual desktops, Policy B is applied and Policy A is ignored. The

© 1997–2026 Citrix Systems, Inc. All rights reserved.

reason is Policy B was processed at the domain level and Policy A was processed at the Virtual Apps and Desktops site GPO level.

However, when a user launches an ICA® or Remote Desktop Protocol (RDP) session, Citrix session settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This setting includes settings that are related to typical RDP client connection settings. The examples for the RDP client connection settings are Desktop wallpaper, menu animation, and View window contents while dragging.

When using multiple policies, you can prioritize policies that contain conflicting settings. For more information, see Compare, prioritize, model, and troubleshoot policies.

Workflow for Citrix policies

The process for configuring policies is as follows:

1. Create the policy.
2. Configure policy settings.
3. Assign the policy to machine and user objects.
4. Prioritize the policy.
5. Verify the effective policy by running the Citrix Group Policy Modeling wizard.

> **Note:**
>
> You open the Citrix Group Policy Modeling wizard by navigating to the **Policies > Modeling** tab and then clicking **Launch Modeling Wizard** in the action bar. The **Modeling** tab is available in Web Studio per customer request.

Navigate Citrix policies and settings

In the Local Group Policy Editor, policies and settings appear in two categories: Computer Configuration and User Configuration. Each category has a Citrix Policies node. See the Microsoft documentation for details about navigating and using this snap-in.

In Web Studio, policy settings are sorted into categories based on the functionality or feature they affect. For example, the **Profile Management** section includes policy settings for Profile Management.

- Computer settings (policy settings applying to machines) define the behavior of virtual desktops and are applied when a virtual desktop starts. These settings apply even when there are no active user sessions on the virtual desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- User settings define the user experience when connecting using ICA. User policies are applied when a user connects or reconnects using ICA. User policies aren't applied if a user connects using RDP or logs on directly to the console.

  To access policies, settings, or templates, select **Policies** in the Web Studio left pane.

  - The **Policies** tab lists all policies. When you select a policy, tabs to the bottom display:
    - Overview - Lists name, priority, enabled/disabled status, and description
    - Settings - Lists all configured settings
    - Assigned To - Lists user and machine objects to which the policy is assigned.

    For more information, see Create policies.
  - The **Templates** tab lists Citrix-provided and custom templates that you created. When you select a template, tabs to the bottom display:
    - Description (why you might want to use the template)
    - Settings (list of configured settings). For more information, see Policy templates.
  - The **Comparison** tab enables you to compare the settings in a policy or template with those settings in other policies or templates. For example, you might want to verify setting values to ensure compliance with best practices. For more information, see Compare, prioritize, model, and troubleshoot policies.

  To search for a setting in a policy or template:

  1. Select the policy or template.
  2. Select **Edit policy** or **Edit Template** in the action bar.
  3. On the **Settings** page, type the name of the setting in the **search** field:

     You can refine your search by selecting:

     - A specific product version
     - A category (for example, Bandwidth)
     - Keywords in the setting name
     - The **View selected only** check box
     - To search only the settings that have been added to the selected policy.

  For an unfiltered search, select **All Settings**.

- To search for a setting within a policy:

  1. Select the policy.
  2. Select the **Settings** tab and type the name of the setting.

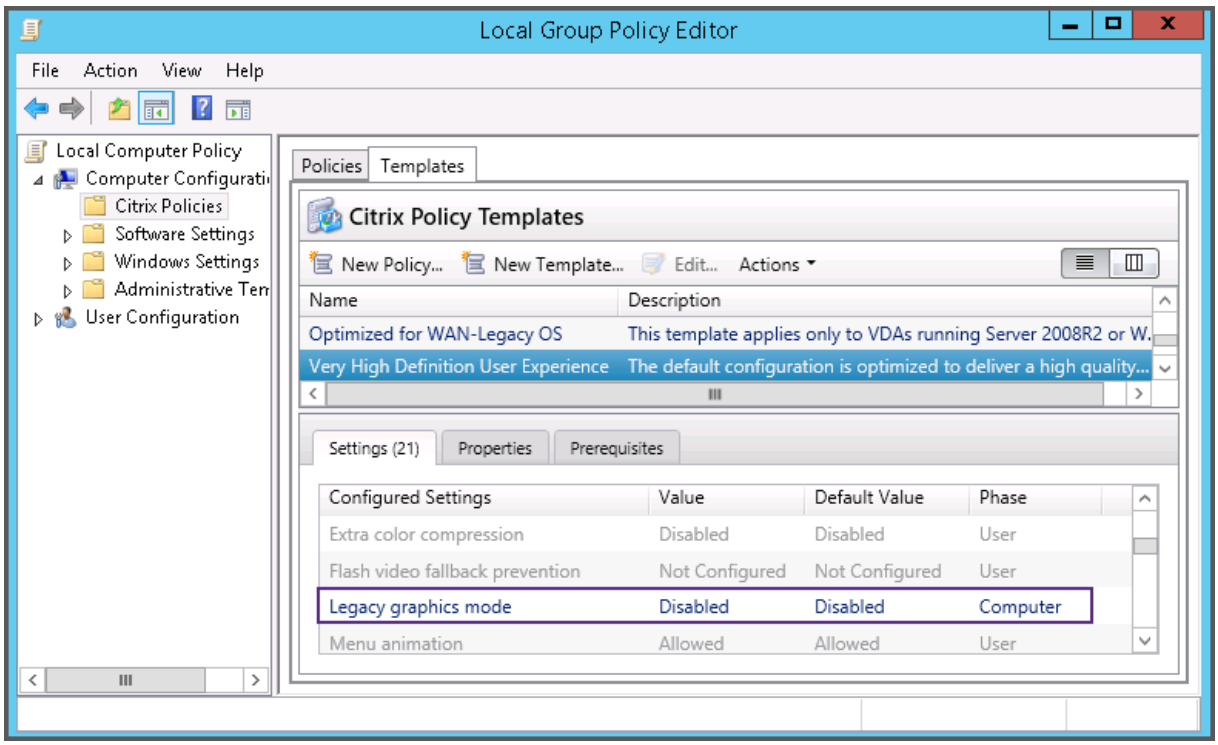
You can refine your search by selecting a specific product version or by selecting a category. For an unfiltered search, select **All Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A policy, once created, is independent of the template used. You can use the **Description** field on a new policy to track the source template used.

In the Group Policy Editor, computer and user settings must be applied separately, even if created from a template that includes both types of settings. In this example choosing to use Very High Definition User Experience in Computer Configuration:

- Legacy Graphics mode is a Computer setting that is used in a policy created from this template.
- The User settings, grayed out, is not used in a policy created from this template.



Policy templates

September 13, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Templates are collections of settings that are recommended to be used in creating policies for achieving some specific results. For example, to create policies for delivering high definition user experience

© 1997–2026 Citrix Systems, Inc. All rights reserved.

to end users, the settings defined in the template Very High Definition User Experience can be used as a reference and starting point for creating such policies.

Templates are not policies. Templates are supplemental documentation for Citrix policy settings. They demonstrate the collective functionalities of certain user related settings.

Using templates is optional. Administrators may create policies without using templates. Templates are useful for administrators who have a high-level idea about how a site should be configured but are not sure which settings to use to achieve the desired configuration.

Administrators can create the templates using either an existing template or an existing policy or from scratch.

ADMX/ADML

The Citrix group policy templates described here have nothing to do with the Windows policy templates. The templates described here and the Windows policy templates are two different concepts. The Citrix group policy templates are not ADMX files.

Built-in Citrix templates

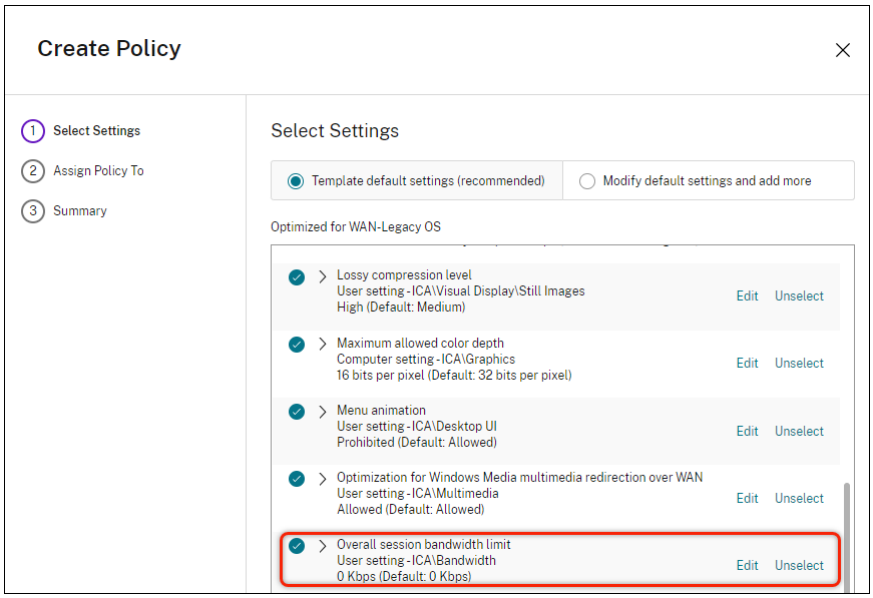
The following policy templates are available:

- **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.
- **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 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 is intended for task workers in branch offices using a shared WAN connection or remote locations with low bandwidth connections accessing 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Optimized for WAN-Legacy OS**. This *Optimized for WAN* 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 Virtual Apps and Desktops. This template includes settings that disable access to printing, clipboard, peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices. Applying this template might use more bandwidth and reduce user density per server.

While we recommend using the built-in Citrix templates with their default settings, there are settings that do not have a specific recommended value. For example, **Overall session bandwidth limit**, included in the Optimized for WAN templates. In this case, the template exposes the setting so the administrator understands this setting is likely to apply to the scenario.



If you are working with a deployment (policy management and VDAs) earlier than XenApp and XenDesktop 7.6 FP3, and require High Server Scalability and Optimized for WAN templates, use the Legacy OS versions of these templates when they apply.

> **Note:**
>
> Citrix creates and updates built-in templates. You cannot modify or delete these templates.

Create and manage templates using Web Studio

To create a template based on a template:

1. Sign in to Web Studio and select **Policies** in the left pane.
2. Select the **Templates** tab and then select the template from which you will create the template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select the **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. Sign in to Web Studio and select **Policies** in the left pane.
2. Select the **Policies** tab and then select the policy from which you create the template.
3. Click the **More** tab.
4. Select **Save as Template**. The **Select Settings** screen appears.
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**.

Templates and delegated administration

Templates in Web Studio are stored in the site database, unlike the templates in Citrix Studio, which are stored as files in the current administrator's user profile folder with a `.gpt` extension. Citrix Studio Templates created by one administrator are not visible to other administrators or to the same administrator on a different machine. Web Studio templates are visible to all the administrators subject to permissions and delegated administration.

Create policies

January 26, 2026

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Before creating a policy, decide which group of users or devices it might affect. You might want to create a policy that is based on user job function, connection type, user device, or geographic location. You can also use the same criteria that you use for Windows Active Directory group policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you already created a policy that applies to a group, consider editing that policy instead of creating another policy. After editing the policy, configure the appropriate settings. Avoid creating a policy solely to enable a specific setting or to exclude the policy from applying to certain users.

When you create a policy, you can base it on settings in a policy template and customize settings as needed. You can also create it without using a template and add all the settings you need.

In Web Studio, new policies created are set to Disabled unless the **Enable policy** check box is explicitly checked.

During policy creation and 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 applicable to all VDA versions
- Current settings only - View settings specific to the current VDA version
- Legacy settings only - View settings applicable only to the deprecated VDA versions

To view the settings while configuring the settings:

1. Sign in to Web Studio and select **Policies** in the left pane.
2. In the **Policies** tab, click **Create Policy**.
3. In the **Select Settings** table, click the drop-down next to **Settings**.
4. Select one of the following options from the drop-down:

- 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

1. The **Settings** table lists the settings available based on the previous step.

Policy settings

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.

The policy settings are enhanced to provide clarity between dependent policies. This feature ensures that the parent policy is configured first for the child policy settings to take effect when configured.

To configure the policy settings:

1. On the **Create Policy** page, under **Select Settings**, search for "overall".
   All the policies (parent and children) related to **Overall session bandwidth limit** are listed.
2. When you hover over a child policy, a tool tip instructs you that the child policy cannot be configured until the **Overall session bandwidth limit** parent policy is configured.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Configure the parent policy settings and then configure the child policy settings and click **Save**.
4. The **Settings** and **Current Value** columns show the values configured in the **Create/Edit policy** table. The table shows the **Edit** option for you to modify the configured settings.

> **Note:**
>
> - The child policies cannot be selected until the parent policy is configured.
> - If the parent policy is unchecked, a pop-up message instructs that the child policies associated will also get unchecked or unselected.

The following table provides the list of parent policies along with the corresponding dependent or child policies.

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
	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

Some policy settings can be in one of the following states:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 setting is set to Allowed, users can control menu animations in their client environment.
- Enabled or Disabled turns the setting on or off. If you disable a setting, it is not enabled in lower-ranked policies.

In addition, some settings control the effectiveness of dependent settings. For example, Client drive redirection controls whether users are allowed to access the drives on their devices. Both this setting and the **Client network drives** setting must be added to the policy to allow users to access their network drives. If the **Client drive redirection** setting is disabled, users can't access their network drives, even if the **Client network drives** setting is enabled.

In general, policy setting changes that impact machines go into effect either when the virtual desktop restarts or when a user logs on. Policy setting changes that impact users go into effect the next time users log on. If you're using Active Directory, policy settings are updated when Active Directory reevaluates policies at 90-minute intervals. And the policy settings are applied either when the virtual desktop restarts or when a user logs on.

For some policy settings, you can enter or select a value when you add the setting to a policy. You can limit the configuration of the setting by selecting Use default value. This selection disables the configuration of the setting and allows only the setting's default value to be used when the policy is applied. This selection is regardless of the value that was entered before selecting Use default value.

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
- Secure default setting takes the second priority
- Default setting takes the least priority

To see the secure default setting for a policy:

1. Log in to Web Studio.
2. In the left navigation, click **Policies**.
3. In the **Policies** tab, click **Create Policy**.
4. 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.

As 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.
- Do not enable conflicting or overlapping settings in Remote Desktop Session Host Configuration. Sometimes, Remote Desktop Session Host Configuration provides similar functionality to Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

policy settings. When possible, keep all settings consistent (enabled or disabled) for ease of troubleshooting.

- Disable unused policies. Policies with no settings added create unnecessary processing.

Policy assignments

When creating a policy, you assign it to certain users and machine objects. That policy is applied to connections according to specific criteria or rules. In general, you can add as many assignments as you want to a policy, based on a combination of criteria.

If you do not specify any assignments, or specify assignments but disable them, the policy is applied to **all** connections.

> **Note:**
>
> Policy assignments are also known as policy filters. For additional information, see the following topics:
>
> - Create, modify, or delete a filter for a policy
> - How do filters get applied?

The following table lists the available assignments:

Assignment name	Applies a policy based on
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 SD-WAN	Whether a user session is launched through NetScaler SD-WAN. **Note:** You can add only one NetScaler SD-WAN assignment to a policy.
Client IP Address	IP address from which a client is connecting, which varies based on how the client connects to the session: Direct internal network connection: The IP address will be the client's private IP address. NetScaler Gateway connection: The IP address will be the NetScaler's subnet IP address. Gateway Service connection. If Rendezvous is disabled, the IP address will be one of the Cloud Connectors' IP addresses. If Rendezvous is enabled, the IP address will be a Gateway Service public IP address. IPv4 examples: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6 examples:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assignment name	Applies a policy based on
Client Name	Name of the user device. Exact match: ClientABCName. Using wildcard: Client*Name.
Delivery Group	Delivery Group membership.
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 type	Type of desktop or application: private desktop, shared desktop, private application, or shared application. **Note:** Private desktop and shared desktop filter options are available only for Citrix Virtual Apps and Desktops 7.x. For more information, see CTX219153.
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.

When a user logs on, all policies that match the assignments for the connection are identified. Those policies are sorted into priority order and multiple instances of any setting are compared. Each setting is applied according to the priority ranking of the policy. Any policy setting that is disabled takes precedence over a lower-ranked setting that is enabled. Policy settings that are not configured are ignored.

> **Important:**
>
> When configuring both Active Directory and Citrix policies using the Group Policy Management Console, assignments and settings might not be applied as expected. For more information, see CTX127461
>
> To set the Client IP policy filter to always use the client's private IP address, configure the following registry setting on the session host:
>
> - Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy`
> - Value type: `DWORD`
> - Value name: `UseClientDeviceIpForPolicyFilter`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> • Value data: 1

A policy named "Unfiltered" is provided by default.

- If you use Web Studio to manage Citrix policies, the settings you add to the Unfiltered policy are applied to all servers, desktops, and connections in a Site.
- If you use the Local Group Policy Editor to manage Citrix policies, the settings you add to the Unfiltered policy are applied to all Sites and connections. The Sites and connections must be within the scope of the Group Policy Objects (GPOs) that includes the policy. For example, the Sales OU includes a GPO called Sales-US that includes all members of the US sales team. The Sales-US GPO is configured with an Unfiltered policy that includes several user policy settings. When the US Sales manager logs on to the Site, the settings in the Unfiltered policy are automatically applied to the session. This configuration is because the user is a member of the Sales-US GPO.

An assignment's mode determines if the policy is applied only to connections that match all the assignment criteria. If the mode is set to Allow (the default), the policy is applied only to connections that match the assignment criteria. If the mode is set to Deny, the policy is applied if the connection does not match the assignment criteria. The following examples illustrate how assignment modes affect Citrix policies when multiple assignments are present.

- **Example: Assignments of like type with differing modes** - In policies with two assignments of the same type, one set to Allow and one set to Deny, the assignment set to Deny takes precedence, provided the connection satisfies both assignments. For example:

  Policy 1 includes the following assignments:

  - Assignment A specifies the Sales group. The mode is set to Allow.
  - Assignment B specifies the Sales manager's account. The mode is set to Deny.

  Because the mode for Assignment B is set to Deny, the policy isn't applied when the Sales manager logs on to the Site, even though the user is a member of the Sales group.

- **Example: Assignments of differing type with like modes** - In policies with two or more assignments of differing types, set to Allow, the connection must satisfy at least one assignment of each type for the policy to be applied. For example:

  Policy 2 includes the following assignments:

  - Assignment C is a User assignment that specifies the Sales group. The mode is set to Allow.
  - Assignment D is a Client IP Address assignment that specifies 10.8.169.* (the corporate network). The mode is set to Allow.

  When the Sales manager logs on to the Site from the office, the policy is applied because the connection satisfies both assignments.

  Policy 3 includes the following assignments:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Assignment E is a User assignment that specifies the Sales group. The mode is set to Allow.
- Assignment F is an Access Control assignment that specifies NetScaler Gateway connection conditions. The mode is set to Allow.

When the Sales manager logs on to the Site from the office, the policy isn't applied because the connection does not satisfy Assignment F.

Create a policy based on a template, using Web Studio

1. Sign in to Web Studio and select **Policies** in the left pane.
2. Select the **Templates** tab and select a template.
3. Select **Create Policy from Template** in the action bar.
4. By default, the new policy uses all the default settings in the template. In this case, the **Template default settings (recommended)** is selected. If you want to change settings, select the **Modify default settings and add more**, and then add or remove settings.
5. Specify how to apply the policy by selecting one of the following:

   - **Selected user and machine objects**. To apply the policy to selected user and machine objects, and then click **Assign** to select the user and machine objects to which the policy must be applied.
   - **All objects in the site**. To apply the policy to all user and machine objects in the site.

6. Enter a name for the policy. Consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.

   The policy is disabled by default; you can enable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you must prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create a policy using Web Studio

1. Sign in to Web Studio and select **Policies** in the left pane.
2. Select the **Policies** tab.
3. Select **Create Policy** in the action bar.
4. Add and configure policy settings.
5. Specify how to apply the policy by choosing one of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Assign to selected user and machine objects and then select the user and machine objects to which the policy must be applied.
- Assign to all objects in a site to apply the policy to all user and machine objects in the Site.

6. Enter a name for the policy or accept the default. Consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.

   The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you must prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

Create and manage policies using the Group Policy Editor

From the Group Policy Editor, expand **Computer Configuration or User Configuration**. Expand the **Policies** node and then select **Citrix Policies**. Choose the appropriate action:

Task	Instruction
Create a policy	On the **Policies** tab, click **New**.
Edit an existing policy	On the **Policies** tab, select the policy and then click **Edit**.
Change the priority of an existing policy	On the **Policies** tab, select the policy and then click either **Higher** or **Lower**.
View summary information about a policy	On the **Policies** tab, select the policy and then click the **Summary** tab.
View and amend policy settings	On the **Policies** tab, select the policy and then click the **Settings** tab.
View and amend policy filters	On the **Policies** tab, select the policy and then click the **Filters** tab. When you add more than one filter to a policy, all the filter conditions must be met for the policy to be applied.
Enable or disable a policy	On the **Policies** tab, select the policy and then select either **Actions > Enable** or **Actions > Disable**.
Create a policy from an existing template	On the **Templates** tab, select the template and then click **New Policy**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy sets

September 6, 2025

Policy sets are objects in Citrix Virtual Apps and Desktops™ which aggregates policies to allow for simplified, role-based access, and easy management. 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. 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.

> **Note:**
>
> Before enabling the policy sets, Citrix® recommends that you make note of the following:
>
> - Additional policy validations are added. As a result, doing an in-place upgrade might lead to loss of policy data if invalid policy settings are present.
> - To detect the invalid data, use the GPO scanner tool and make necessary edits before upgrading. For more information, see CTX676686.
> - For all future upgrades, Citrix recommends you to use the latest SDK. Using an older SDK for updating policies might allow adding invalid data to the policy settings which might lead to the risk of losing policy data.

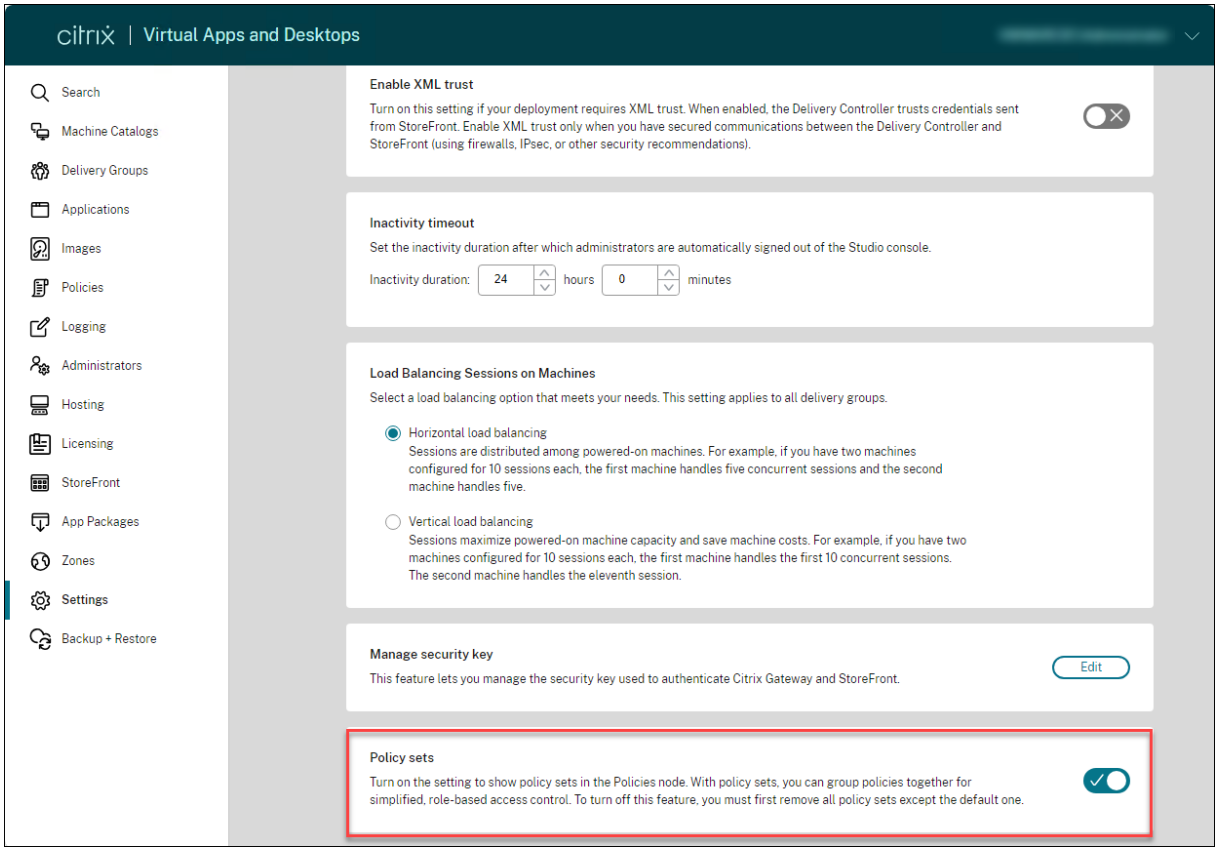
Benefits

- Role-based access control for distributed administrator teams
- Simplified mergers, acquisitions, and consolidations
- Limited fault domain
- Multitenant support for policies

Enable policy sets

From the **Manage** tab of Virtual Apps and Desktops, navigate to **Settings** and turn on the **Policy sets** setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> You must enable policy sets before creating a policy set.

Feature comparison

Before applying policy sets	After applying policy sets
Policies, settings, filters, and policy priorities for the entire site are configured in one place within Citrix Studio.	Policies, settings, filters, and policy priorities are configured separately for each policy set.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How does policy sets work?

General overview

- Policy sets are assigned to delivery groups
- Policy sets have one or multiple scopes
- Delivery groups with no policy set assigned receive the default policy set
- A delivery group can have only one policy set assigned to it
- Multiple delivery groups can use the same policy set
- Even though policy sets are assigned to delivery groups, the policies maintain their filters

For more information, see How do filters get applied?. There is no change in the way that policy assignments or policy filters work for policy sets. That is, they work the same way as they do for policies.

Default policy set

- When the policy set setting is turned on, all existing policies are grouped within the default policy set
- Every delivery group receives the default policy set unless the administrator team creates a policy set and assigns that to a delivery group.
- Once a delivery group has a different policy set assigned to it, it will no longer get policies from the default policy set

Policy set creation

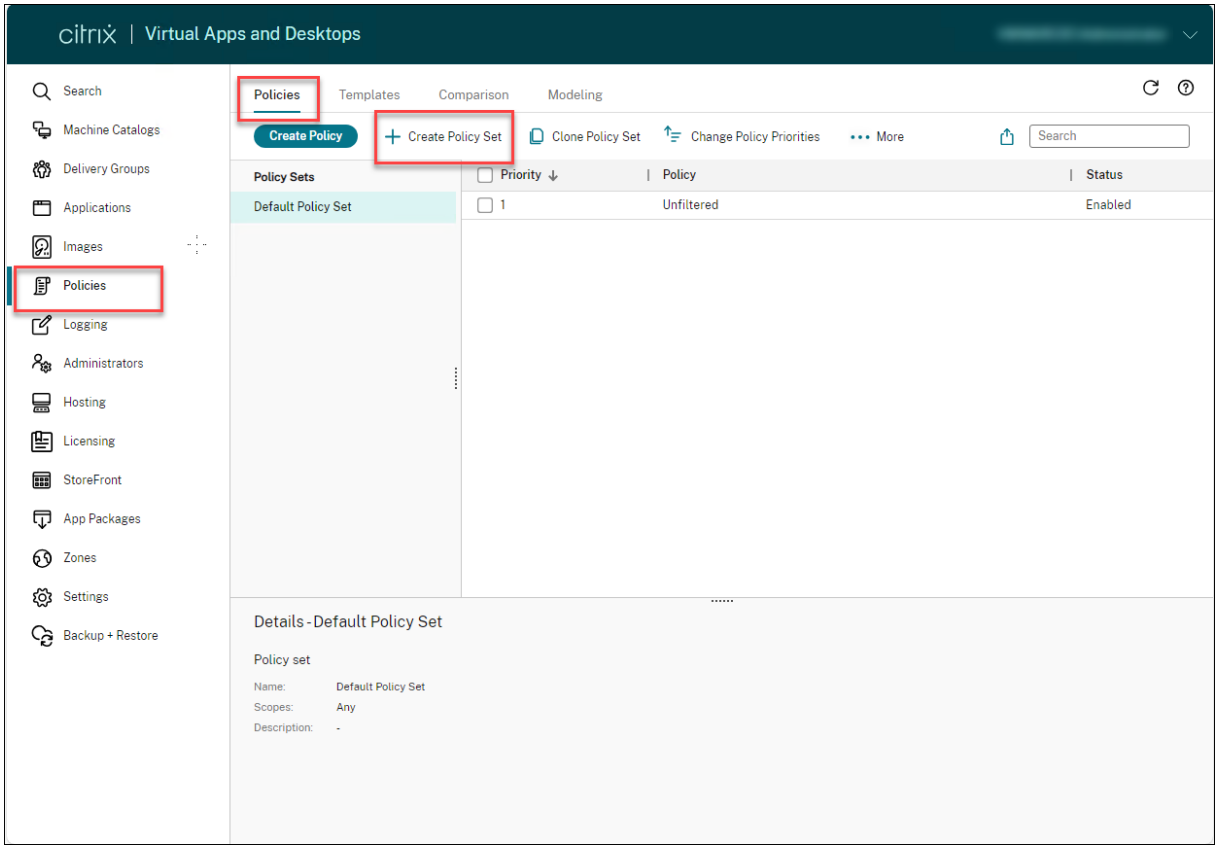
Policy sets can be created in the following two ways:

- Create policy set - this action creates an empty policy set
- Clone policy set - this action creates a policy set based on an existing policy set

Create policy sets

1. Sign in to Web Studio and select **Policies** in the left pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Select **Create Policy Set**. The **Introduction** tab appears.
2. Click **Next** or click **Name and Description** tab.
3. Enter the name and description of the policy set.
4. Click **Next** or click the **Assignments** tab.
5. Select one or more delivery groups to which you want to assign the policy set.
6. Click **Next** or click **Scopes** tab.
7. Select the scopes of the policy set.
8. Click **Create**. The policy set is created with the defined assignment and scope.

Clone policy sets

1. Sign in to Web Studio and select **Policies** in the left pane.
2. Select **Clone Policy Set**.
3. Modify the name of the policy set.
4. Modify or create assignments for the policy set and click **Next**.
5. Select or deselect policies to include in the cloned policy set.
6. Modify the scope of the policy.
7. Click **Create**. The policy set is created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Edit policy sets

1. Sign in to Web Studio and select **Policies** in the left pane.
2. Select **Edit Policy Set**.
3. Modify the name of the policy set and click **Next**.
4. Modify or create assignments for the policy set and click **Next**.
5. Modify the scope of the policy.
6. Click **Create**.

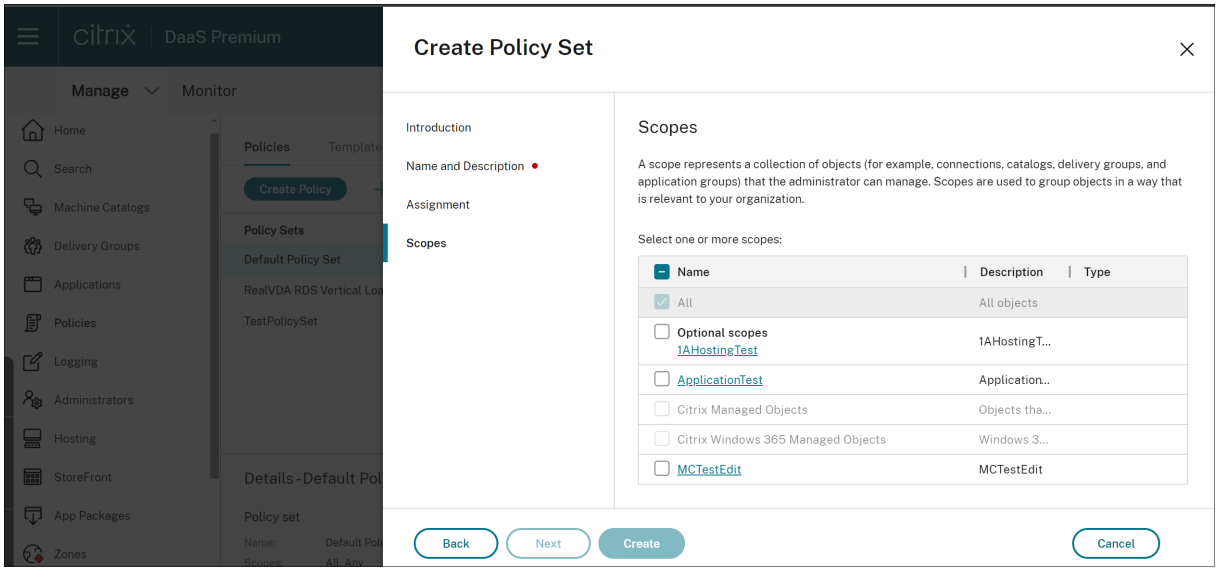
Policy set assignment

Policy sets are assigned to delivery groups. You can configure assignments when the policy set is created or edited. You can also configure assignments when delivery groups are created or edited.

Policy set scopes

Administrators can define the scope of the policy set so that only authorized administrators can view or edit it. You can configure scopes when the policy set is created or edited.

With the introduction of Policy Sets, you can also create and manage Citrix Policy using API. For more information, see How to create a policy set in Citrix DaaS.



Compare, prioritize, and troubleshoot policies

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

You can use multiple policies to customize your environment to meet users' needs based on their job functions, geographic locations, or connection types. For example, for enhanced security, place restrictions on user groups who regularly interact with sensitive data.

You can also create a policy that prevents users from saving sensitive files on their local client drives. However, if some users in the user group do need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one takes precedence. When using multiple policies, you must determine:

- How to prioritize the policies
- How to create exceptions
- How to view the effective policy when policies conflict.

In general, policies override similar settings configured for the entire Site, for specific Delivery Controllers, or on the user device. The exception to this principle is security. The highest encryption setting in your environment, always overrides other settings and policies. The highest encryption setting includes the operating system and the most restrictive shadowing settings.

Citrix policies interact with policies that you set in your operating system. In a Citrix environment, Citrix settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This setting includes settings that are related to typical Remote Desktop Protocol (RDP) client connection settings. The typical RDP settings include settings such as desktop wallpaper, menu animation, and view window contents while dragging.

Some policy settings, such as Secure ICA®, must match the settings in the operating system. If a higher priority encryption level is set elsewhere, the **Secure ICA policy** settings that you specify in the policy or when you're delivering application and desktops can be overridden.

For example, the encryption settings that you specify when creating Delivery Groups must be at the same level as the encryption settings you specified throughout your environment.

> **Note:**
>
> In the second hop of double-hop scenarios, consider that a Single-session OS VDA connects to Multi-session OS VDA. In this case, Citrix policies act on the Single-session OS VDA as if it were the user device. For example, consider policies are set to cache images on the user device. In

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> this example, the images cached for the second hop in a double-hop scenario are cached on the Single-session OS VDA machine.

Use the policy modeling wizard

Policy modeling helps you simulate enabled policies with filters for planning and testing purposes. Only enabled policies with filters are modeled. Disabled policies are never applied and enabled policies without filters are always applied.

Perform the following steps to open the **Policy Modeling** wizard:

1. Select **Policies** from the left navigation.
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 browse for containers or specific users or computers. Click **Next**.
6. Choose your filter evidence. You can optionally get more granular with your simulation by entering additional details, such as **Delivery group**, **Tags**, **Client IP address**, and so on. Click **Next**.
7. Review the summary of your selections and click **Run**.

After you click **Run**, the wizard generates a report of the modeling results. While viewing this report, you can:

- Select if you would like to view **All settings**, **Computer settings**, or **User settings** in the drop-down menu.
- Use the search bar to look for specific settings.
- Click a specific setting to view details of that setting. For example, if all user settings were not applied for a specific policy, the **Details** pane shows you the reason why the settings were not applied.
- Click **Export** to export the modeling results in JSON format, HTML format, or both.

After running policy modeling, more options become available to you. You can:

- **View Modeling Report**: This opens the same modeling report from above so you can view it again or export it.
- **Rerun Policy Modeling**: This allows you to rerun policy modeling with the same set of criteria selected previously and generate new modeling results. This is useful if some policies have changed and you would like to see how those changes affect your current model.
- **Delete Modeling Report**: This deletes the current modeling report.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compare policies and templates

You can compare the settings in a policy or template with the settings of the other policies or templates. For example, you might need to verify setting values to maintain compliance with best practices. You might also want to compare settings in a policy or template with the default settings that are provided by Citrix.

1. Sign in to Web Studio and select **Policies** in the left pane.
2. Click the **Comparison** tab and then click **Select**.
3. Choose the policies or templates to compare. To include default values in the comparison, select the **Compare to default settings** check box.
4. After you click **Compare**, the configured settings are displayed in columns.
5. To see all settings, select **Show All Settings**. To return to the default view, select **Show Common Settings**.

Prioritize policies

Prioritizing policies allows you to define the precedence of policies when they contain conflicting settings. When a user logs on, all policies that match the assignments for the connection are identified. Those policies are sorted into priority order and multiple instances of any setting are compared. Each setting is applied according to the priority ranking of the policy.

You prioritize policies by giving them different priority numbers. By default, new policies are given the lowest priority. If policy settings conflict, a policy with a higher priority (a priority number of 1 is the highest) overrides a policy with a lower priority. Settings are merged according to priority and the setting's condition. For example, whether the setting is disabled or enabled. Any disabled setting overrides a lower-ranked setting that is enabled. Policy settings that are not configured are ignored and do not override the settings of lower-ranked settings.

1. Select **Policies** in the left pane. Make sure that you select the **Policies** tab.
2. On the **Policies** tab, select **Change Policy Priorities** in the action bar. The **Change Policy Priorities** page appears.
3. In the priority list, use one of the following ways to change the priority for a policy:
   - Drag the policy to a desired position.
   - To move it up or down by one position, click the Up or Down arrow icon respectively.
   - To move it to the top or bottom of the list, click the Top or Bottom arrow icon respectively.
   - To change the priority number, click the **Edit** icon, enter a number as needed, and then click **Save**.
4. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exceptions

When you create policies for groups of users, user devices, or machines, you might find that some members of the group require exceptions to some policy settings. You can create exceptions by:

- Creating a policy only for those group members who need the exceptions and then ranking the policy higher than the policy for the entire group
- Using the Deny mode for an assignment added to the policy

An assignment with the mode set to Deny applies a policy only to connections that do not match the assignment criteria. For example, a policy includes the following assignments:

- Assignment A is a client IP address assignment that specifies the range 208.77.88.*. The mode is set to Allow
- Assignment B is a user assignment that specifies a particular user account. The mode is set to Deny.

The policy is applied to all users who log on to the Site with IP addresses in the range that is specified in Assignment A. However, the policy isn't applied to the user logging on to the Site with the user account specified in Assignment B.

Determine which policies apply to a connection

A connection might not respond as expected because multiple policies apply. If a higher priority policy applies to a connection, it can override the settings you configure in the original policy. You can calculate the Resultant Set of Policy and determine how final policy settings are merged for a connection.

You can calculate the Resultant Set of Policy in the following ways:

- Use the **Citrix Group Policy Modeling** Wizard to simulate a connection scenario and discern how Citrix policies might be applied. You can specify conditions for a connection scenario such as:
    - Domain controller
    - Users
    - Citrix policy assignment evidence values
    - Simulated environment settings such as slow network connection

      The report that the wizard produces lists the Citrix policies that take effect in the scenario. Because you log on to the Controller as a domain user, the wizard calculates the results using both site policy settings and Active Directory Group Policy Objects (GPOs).
- Use **Group Policy Results** to produce a report describing the Citrix policies in effect for a given user and controller. The Group Policy Results tool helps you evaluate the current state of GPOs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

in your environment and generates a report. The generated report describes how these objects, including Citrix policies, are currently being applied to a particular user and controller.

You can launch the Citrix Group Policy Modeling Wizard in Web Studio. Or, you can launch the Group Policy Results tool through the Group Policy Management Console in Windows.

Site policy settings created using Web Studio aren't included in the Resultant Set of Policy in the following cases:

- If you run the Citrix Group Policy Modeling Wizard from the Group Policy Management Console
- If you run the Group Policy Results tool from the Group Policy Management Console

To verify that you obtain the most comprehensive Resultant Set of Policy, Citrix recommends launching the Citrix Group Policy Modeling wizard from Web Studio, unless you create policies using only the Group Policy Management Console.

Troubleshoot policies

Users, IP addresses, and other assigned objects can have multiple policies that apply simultaneously. This scenario can result in conflicts where a policy might not behave as expected. When you run the Citrix Group Policy Modeling Wizard or the Group Policy Results tool, you might discover that no policies are applied to user connections. In such a scenario, policy settings are not applied to the users who connect to their applications and desktops under conditions that match the policy evaluation criteria. This situation occurs when:

- No policies have assignments that match the policy evaluation criteria.
- Policies that match the assignment do not have any settings configured.
- Policies that match the assignment are disabled.

If you want to apply policy settings to the connections that meet the specified criteria, make sure:

- The policies you want to apply to those connections are enabled.
- The policies you want to apply have the appropriate settings configured.

Default policy settings

September 6, 2025

The following tables list policy settings, their default, and the Virtual Delivery Agent (VDA) versions to which they apply.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ICA®

Name	Default setting	VDA
Adaptive transport	Off. Use when preferred	VDA 7.13–7.15; VDA 7.16 through current
Client clipboard redirection	Allowed	All VDA versions
Client clipboard write allowed formats	No formats are specified	VDA 7.6 through current
Desktop launches	Prohibited	VDA for Multi-session OS 7 through current
ICA listener port number	1494	All VDA version
Launching of non-published programs during client connection	Prohibited	VDA for Multi-session OS 7 through current
Limit clipboard client to session transfer size	Disabled	VDA 2009
Limit clipboard session to client transfer size	Disabled	VDA 2009
Loss tolerant mode	Allowed	VDA 2003. Note: Loss tolerance mode isn't yet available. This version of the VDA supports it when it becomes available.
Loss tolerant thresholds	When loss tolerant mode is available: Packet loss: 5%, Latency: 300 ms (RTT)	VDA 2003 through current
Rendezvous protocol	Disabled	Applies only to HDX sessions established through Citrix Cloud.
Restrict client clipboard write	Prohibited	VDA 7.6 through current
Restrict session clipboard write	Prohibited	VDA 7.6 through current
Session clipboard write allowed formats	No formats are specified	VDA 7.6 through current
Tablet mode toggle	Enabled	VDA 7.16 through current; for VDA 7.14 and 7.15 LTSR, configure this setting using the registry.
Virtual channel allow list	Enabled	VDA 2109 through current

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Session metric collection	Allowed	7.42 through current

ICA/Adobe Flash delivery/Flash redirection

Name	Default setting	VDA
Flash video fallback prevention	Not configured	VDA 7.6 FP3 through current
Flash video fallback prevention error *.swf		VDA 7.6 FP3 through current

ICA/Audio

Name	Default setting	VDA
Adaptive Audio	Enabled	Applies to both single-session OS and multi-session OS sessions of VDAs using Citrix Virtual Apps and Desktops™ 2109 or later.
Audio over UDP real-time transport	Allowed	All VDA versions
Audio Plug N Play	Allowed	VDA for Multi-session OS 7 through current
Audio quality	High - high definition audio	All VDA versions
Client audio redirection	Allowed	All VDA versions
Client microphone redirection	Allowed	All VDA versions
Loss tolerant mode for audio	Prohibited	VDA versions 2411 and earlier

ICA/Auto client reconnect

Name	Default setting	VDA
Auto client reconnect	Allowed	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Auto client reconnect authentication	Do not require authentication	All VDA versions
Auto client reconnect logging	Do not log auto-reconnect events	All VDA versions
Auto client reconnect timeout	120 seconds	VDA 7.13 through current
Reconnect UI transparency level	80%	VDA 7.13 through current

ICA/Bandwidth

Name	Default setting	VDA
Audio redirection bandwidth limit	0 Kbps	All VDA versions
Audio redirection bandwidth limit percent	0	All VDA versions
Client USB device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Client USB device redirection bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Clipboard redirection bandwidth limit	0 Kbps	All VDA versions
Clipboard redirection bandwidth limit percent	0	All VDA versions
COM port redirection bandwidth limit	0 Kbps	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
COM port redirection bandwidth limit percent	0	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
File redirection bandwidth limit	0 Kbps	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
File redirection bandwidth limit percent	0	All VDA versions
HDX MediaStream Multimedia Acceleration bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 and VDA for Single-session OS 7 through current VDA for Multi-session OS and VDA for Single-session OS
HDX MediaStream Multimedia Acceleration bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
LPT port redirection bandwidth limit	0 Kbps	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
LPT port redirection bandwidth limit percent	0	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
Overall session bandwidth limit	0 Kbps	All VDA versions
Printer redirection bandwidth limit	0 Kbps	All VDA versions
Printer redirection bandwidth limit percent	0	All VDA versions
TWAIN device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
TWAIN device redirection bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Bidirectional content redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Allow bidirectional content redirection	Prohibited	VDA 7.13 through current
Allowed URLs to be redirected to client	empty	VDA 7.13 through current
Allowed URLs to be redirected to VDA	empty	VDA 7.13 through current
Bidirectional content redirection configuration	Disabled	VDA 2311 through current

ICA/Browser content redirection

Name	Default setting	VDA
Browser content redirection	Allowed	VDA 7.16 through current
Browser content redirection ACL configuration	`https://www.youtube.com/*`	VDA 7.16 through current
Browser content redirection Integrated Windows Authentication support	Prohibited	VDA 2106 through current
Browser content redirection proxy configuration	empty	VDA 7.16 through current
Browser content redirection server fetch web proxy authentication	Prohibited	VDA 2012 through current

ICA/Client sensors

Name	Default setting	VDA
Allow applications to use the physical location of the client device	Prohibited	VDA 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ICA/Desktop UI

Name	Default setting	VDA
Desktop Composition Redirection	Disabled (7.6 FP3 through current); Enabled (5.6 through 7.6 FP2)	VDA 5.6, VDA for Single-session OS 7 through 7.15
Desktop Composition Redirection graphics quality	Medium	VDA 5.6, VDA for Single-session OS 7 through 7.15
Desktop wallpaper	Allowed	All VDA versions
Menu animation	Allowed	All VDA versions
View window contents while dragging	Allowed	All VDA versions

ICA/End user monitoring

Name	Default setting	VDA
ICA round trip calculation	Enabled	All VDA versions
ICA round trip calculation interval	15 seconds	All VDA versions
ICA round trip calculations for idle connections	Disabled	All VDA versions

ICA/Enhanced desktop experience

Name	Default setting	VDA
Enhanced Desktop Experience	Allowed	VDA for Multi-session OS 7 through current

ICA/File redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Auto connect client drives	Allowed	All VDA versions
Client drive redirection	Allowed	All VDA versions
Client fixed drives	Allowed	All VDA versions
Client floppy drives	Allowed	All VDA versions
Client network drives	Allowed	All VDA versions
Client optical drives	Allowed	All VDA versions
Client removable drives	Allowed	All VDA versions
Host to client redirection	Disabled	VDA for Multi-session OS 7 through current
Preserve client drive letters	Disabled	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Read-only client drive access	Disabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Special folder redirection	Allowed	Web Interface deployments only; VDA for Multi-session OS 7 through current
Use asynchronous writes	Disabled	All VDA versions

ICA/Graphics

Name	Default setting	VDA
Allow visually lossless compression	Disabled	VDA 7.6 through current
Display memory limit	65,536 Kb	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Display mode degrade preference	Degrade color depth first	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Dynamic windows preview	Enabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Graphics status indicator	Disabled	VDA 7.16 through current
Image caching	Enabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Legacy graphics mode	Disabled	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Maximum allowed color depth	32 bits per pixel	All VDA versions
Notify user when display mode is degraded	Disabled	VDA for Multi-session OS 7 through current
Optimize for 3D graphics workload	Disabled	VDA 7.17 through current
Queuing and tossing	Enabled	All VDA versions
Screen sharing	Disabled	VDA 2112
Use video codec for compression	Use video codec when preferred	VDA 7.6 FP3 through current
Use hardware encoding for video codec	Enabled	VDA 7.11 through current

ICA/Graphics/Caching

Name	Default setting	VDA
Persistent cache threshold	3,000,000 bps	VDA for Multi-session OS 7 through current

ICA/Graphics/Framehawk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Framehawk display channel	Disabled	VDA 7.6 FP2 through current
Framehawk display channel port range	3224,3324	VDA 7.6 FP2 through current

ICA/Keep alive

Name	Default setting	VDA
ICA keep alive timeout	60 seconds	All VDA versions
ICA keep alives	Do not send ICA keep alive messages	All VDA versions

ICA/Keyboard and IME

Name	Default setting	VDA
Client Keyboard Layout Sync and IME Improvement	Disabled	Applies only to 1912 LTSR CU2 and later.
Unicode Keyboard Layout Mapping	Allowed (2407, 2411, 2503); Prohibited (earlier versions, 2507)	Applies only to 1912 LTSR CU2 and later.
Hide Keyboard Layout Switch Pop-up Message Box	Prohibited	Applies only to 1912 LTSR CU2 and later.

ICA/Local App Access

Name	Default setting	VDA
Allow Local App Access	Prohibited	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
URL redirection block list	No sites are specified	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
URL redirection allow list	No sites are specified	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Mobile experience

Name	Default setting	VDA
Automatic keyboard display	Prohibited	VDA 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Launch touch-optimized desktop	Allowed	VDA 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current. This setting is disabled and not available for Windows 10 and Windows Server 2016 machines.
Remote the combo box	Prohibited	VDA 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Multimedia

Name	Default setting	VDA
HTML5 video redirection	Prohibited	VDA 7.12 through current

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Limit video quality	Not configured	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Microsoft Teams redirection	Allowed	VDA for Multi-session OS 1906 through current, VDA for Single-session OS 1906 through current.
Multimedia conferencing	Allowed	All VDA versions
Optimization for Windows Media multimedia redirection over WAN	Allowed	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Use GPU for optimizing Windows Media multimedia redirection over WAN	Prohibited	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Windows Media fallback prevention	Not configured	VDA 7.6 FP3 through current
Windows Media client-side content fetching	Allowed	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Windows Media redirection	Allowed	All VDA versions
Windows Media redirection buffer size	5 seconds	VDA 5, 5.5, 5.6 FP1 through current
Windows Media redirection buffer size use	Disabled	VDA 5, 5.5, 5.6 FP1 through current

ICA/Multi-Stream Connections

Name	Default setting	VDA
Audio over UDP	Allowed	VDA for Multi-session OS 7 through current

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Audio UDP port range	16500, 16509	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Multi-Port policy	Primary port (2598) has High Priority	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Multi-Stream computer setting	Disabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Multi-Stream user setting	Disabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Multi-Stream virtual channel stream assignment setting	See Multi-Stream virtual channel assignment setting for default stream assignments	VDA 2003

ICA/Port Redirection

Name	Default setting	VDA
Auto connect client COM ports	Disabled	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
Auto connect client LPT ports	Disabled	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
Client COM port redirection	Prohibited	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry
Client LPT port redirection	Prohibited	All VDA versions; for VDA 7.0 through 7.8, configure this setting using the registry

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ICA/Printing

Name	Default setting	VDA
Client printer redirection	Allowed	All VDA versions
Default printer	Set default printer to the client's main printer	All VDA versions
Printer assignments	User's current printer is used as the default printer for the session	All VDA versions
Printer auto-creation event log preference	Log errors and warnings	All VDA versions
Session printers	No printers are specified	All VDA versions
Wait for printers to be created (desktop)	Disabled	All VDA versions

ICA/Printing/Client Printers

Name	Default setting	VDA
Auto-create client printers	Auto-create all client printers	All VDA versions
Auto-create generic universal printer	Disabled	All VDA versions
Client printer names	Standard printer names	VDA 5.6
Direct connections to print servers	Enabled	All VDA versions
Printer driver mapping and compatibility	No rules are specified	All VDA versions
Printer properties retention	Held in profile only if not saved on client	All VDA versions
Retained and restored client printers	Allowed	VDA 5, 5,5, 5.6 FP1

ICA/Printing/Drivers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Automatic installation of in-box printer drivers	Enabled	All VDA versions
Universal driver preference	EMF; XPS; PCL5c; PCL4; PS	All VDA versions
Universal print driver usage	Use universal printing only if requested driver is unavailable	All VDA versions

ICA/Printing/Universal Print Server

Name	Default setting	VDA
Universal Print Server enable	Disabled	All VDA versions
Universal Print Server print data stream (CGP) port	7229	All VDA version
Universal Print Server print stream input bandwidth limit (kbps)	0	All VDA versions
Universal Print Server web service (HTTP/SOAP) port	8080	All VDA versions
Universal Print Servers for load balancing		VDA versions 7.9 through current
Universal Print Server out-of-service threshold	180 (seconds)	VDA versions 7.9 through current

ICA/Printing/Universal Printing

Name	Default setting	VDA
Universal printing EMF processing mode	Spool directly to printer	All VDA versions
Universal printing image compression limit	Best quality (lossless compression)	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Universal printing optimization defaults	Image Compression: Desired image quality = Standard quality, Enable heavyweight compression = False; Image and Font Caching: Allow caching of embedded images = True; Allow non-administrators to modify these settings = False;	All VDA versions
Universal printing preview preference	Do not use print preview for auto-created or generic universal printers	All VDA versions
Universal printing print quality limit	No limit	All VDA versions

ICA/Security

Name	Default setting	VDA
SecureICA minimum encryption level	Basic	VDA for Multi-session OS 7 through current

ICA/Server Limits

Name	Default setting	VDA
Server idle timer interval	0 milliseconds	VDA for Multi-session OS 7 through current

ICA/Session Limits

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Disconnected session timer	Disabled	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Remote PC Access disconnected session timer	Disabled	VDA for Single-session OS 7 through current
Disconnected session timer interval	1,440 minutes	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Session connection timer	Disabled	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Session connection timer interval	1,440 minutes	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Session idle timer	Enabled	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current
Session idle timer interval	1,440 minutes	VDA 5, 5.5, 5.6 FP1, VDA for Single-session OS 7 through current

ICA/Session Reliability

Name	Default setting	VDA
Session reliability connections	Allowed	All VDA versions
Session reliability port number	2598	All VDA versions
Session reliability timeout	180 seconds	All VDA versions

ICA/Time Zone Control

Name	Default setting	VDA
Estimate local time for legacy clients	Enabled	VDA for Multi-session OS 7 through current

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Restore Single-session OS time zone on session disconnect or logoff	Enabled	Current VDA version
Use local time of client	Use server time zone	All VDA versions

ICA/TWAIN Devices

Name	Default setting	VDA
Client TWAIN device redirection	Allowed	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
TWAIN compression level	Medium	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/USB Devices

Name	Default setting	VDA
Client USB device optimization rules	Enabled (VDA 7.6 FP3 through current); Disabled (VDA 7.11 through current); By default, no rules are specified	VDA 7.6 FP3 through current
Client USB device redirection	Prohibited	All VDA versions
Client USB device redirection rules	No rules are specified	All VDA versions
Client USB Plug and Play device redirection	Allowed	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ICA/Visual Display

Name	Default setting	VDA
Preferred color depth for simple graphics	24 bits per pixel	VDA 7.6 FP3 through current
Target frame rate	30 fps	All VDA versions
Visual quality	Medium	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

ICA/Visual Display/Moving Images

Name	Default setting	VDA
Minimum image quality	Normal	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Moving image compression	Enabled	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Progressive compression level	None	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Progressive compression threshold value	2,147,483,647 Kbps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Target minimum frame rate	10 fps	VDA 5.5, 5.6 FP1, VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The **Target minimum frame rate** policy has been deprecated.

ICA/Visual Display/Still Images

Name	Default setting	VDA
Extra color compression	Disabled	All VDA versions
Extra color compression threshold	8,192 Kbps	All VDA versions
Heavyweight compression	Disabled	All VDA versions
Lossy compression level	Medium	All VDA versions
Lossy compression threshold value	2,147,483,647 Kbps	All VDA versions

ICA/WebSockets

Name	Default setting	VDA
WebSockets connections	Prohibited	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
WebSockets port number	8008	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
WebSockets trusted origin server list	The wildcard, *, is used to trust all Receiver for Web URLs	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

Load Management

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Concurrent logon tolerance	2	VDA for Multi-session OS 7 through current
CPU usage	Disabled	VDA for Multi-session OS 7 through current
CPU usage excluded process priority	Below Normal or Low	VDA for Multi-session OS 7 through current
Disk usage	Disabled	VDA for Multi-session OS 7 through current
Maximum number of sessions	250	VDA for Multi-session OS 7 through current
Memory usage	Disabled	VDA for Multi-session OS 7 through current
Memory usage base load	Zero load: 768 MB	VDA for Multi-session OS 7 through current

Profile Management/Advanced settings

Name	Default setting	VDA
Disable automatic configuration	Disabled	All VDA versions
Log off user if a problem is encountered	Disabled	All VDA versions
Number of retries when accessing locked files	5	All VDA versions
Process Internet cookie files on logoff	Disabled	All VDA versions

Profile Management/Basic settings

Name	Default setting	VDA
Active write back	Disabled	All VDA versions
Enable Profile Management	Disabled	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Excluded groups	Disabled. Members of all user groups are processed.	All VDA versions
Offline profile support	Disabled	All VDA versions
Path to user store	Windows	All VDA versions
Process logons of local administrators	Disabled	All VDA versions
Processed groups	Disabled. Members of all user groups are processed.	All VDA versions

Profile Management/Cross-Platform Settings

Name	Default setting	VDA
Cross-platform settings user groups	Disabled. All user groups specified in Processed groups are processed	All VDA versions
Enable cross-platform settings	Disabled	All VDA versions
Path to cross-platform definitions	Disabled. No path is specified.	All VDA versions
Path to cross-platform settings store	Disabled. Windows\PM_CM is used.	All VDA versions
Source for creating cross-platform settings	Disabled	All VDA versions

Profile Management/File System/Exclusions

Name	Default setting	VDA
Exclusion list - directories	Disabled. All folders in the user profile are synchronized.	All VDA versions
Exclusion list - files	Disabled. All files in the user profile are synchronized.	All VDA versions

Profile Management/File System/Synchronization

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Directories to synchronize	Disabled. Only non-excluded folders are synchronized.	All VDA versions
Files to synchronize	Disabled. Only non-excluded files are synchronized.	All VDA versions
Folders to mirror	Disabled. No folders are mirrored.	All VDA versions

Profile Management/Folder Redirection

Name	Default setting	VDA
Grant administrator access	Disabled	All VDA versions
Include domain name	Disabled	All VDA versions

Profile Management/Folder Redirection/AppData(Roaming)

Name	Default setting	VDA
AppData(Roaming) path	Disabled. No location is specified.	All VDA versions
Redirection settings for AppData(Roaming)	Contents are redirected to the UNC path specified in the AppData(Roaming) path policy settings	All VDA versions

Profile Management/Folder Redirection/Contacts

Name	Default setting	VDA
Contacts path	Disabled. No location is specified.	All VDA versions
Redirection settings for Contacts	Contents are redirected to the UNC path specified in the **Contacts path policy** settings	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management/Folder Redirection/Desktop

Name	Default setting	VDA
Desktop path	Disabled. No location is specified.	All VDA versions
Redirection settings for Desktop	Contents are redirected to the UNC path specified in the **Desktop path policy** settings	All VDA versions

Profile Management/Folder Redirection/Documents

Name	Default setting	VDA
Documents path	Disabled. No location is specified.	All VDA versions
Redirection settings for Documents	Contents are redirected to the UNC path specified in the **Documents path policy** settings	All VDA versions

Profile Management/Folder Redirection/Downloads

Name	Default setting	VDA
Downloads path	Disabled. No location is specified.	All VDA versions
Redirection settings for Downloads	Contents are redirected to the UNC path specified in the **Downloads path policy** settings	All VDA versions

Profile Management/Folder Redirection/Favorites

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Favorites path	Disabled. No location is specified.	All VDA versions
Redirection settings for Favorites	Contents are redirected to the UNC path specified in the **Favorites path policy** settings	All VDA versions

Profile Management/Folder Redirection/Links

Name	Default setting	VDA
Links path	Disabled. No location is specified.	All VDA versions
Redirection settings for Links	Contents are redirected to the UNC path specified in the **Links path policy** settings	All VDA versions

Profile Management/Folder Redirection/Music

Name	Default setting	VDA
Music path	Disabled. No location is specified.	All VDA versions
Redirection settings for Music	Contents are redirected to the UNC path specified in the **Music path policy** settings	All VDA versions

Profile Management/Folder Redirection/Pictures

Name	Default setting	VDA
Pictures path	Disabled. No location is specified.	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Redirection settings for Pictures	Contents are redirected to the UNC path specified in the **Pictures path policy** settings	All VDA versions

Profile Management/Folder Redirection/Saved Games

Name	Default setting	VDA
Saved Games path	Disabled. No location is specified.	All VDA versions
Redirection settings for Saved Games	Contents are redirected to the UNC path specified in the **Saved Games path policy** settings	All VDA versions

Profile Management/Folder Redirection/Searches

Name	Default setting	VDA
Searches path	Disabled. No location is specified.	All VDA versions
Redirection settings for Searches	Contents are redirected to the UNC path specified in the **Searches path policy** settings	All VDA versions

Profile Management/Folder Redirection/Start Menu

Name	Default setting	VDA
Start Menu path	Disabled. No location is specified.	All VDA versions
Redirection settings for Start Menu	Contents are redirected to the UNC path specified in the Start Menu path policy settings	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management/Folder Redirection/Video

Name	Default setting	VDA
Video path	Disabled. No location is specified.	All VDA versions
Redirection settings for Video	Contents are redirected to the UNC path specified in the **Video path policy** settings	All VDA versions

Profile Management/Log settings

Name	Default setting	VDA
Active Directory actions	Disabled	All VDA versions
Common information	Disabled	All VDA versions
Common warnings	Disabled	All VDA versions
Enable logging	Disabled	All VDA versions
File system actions	Disabled	All VDA versions
File system notifications	Disabled	All VDA versions
Logoff	Disabled	All VDA versions
Logon	Disabled	All VDA versions
Maximum size of the log file	1048576	All VDA versions
Path to log file	Disabled. Log files are saved in the default location; %SystemRoot%\System32\Logfiles\UserProfileManager.	All VDA versions
Personalized user information	Disabled	All VDA versions
Policy values at logon and logoff	Disabled	All VDA versions
Registry actions	Disabled	All VDA versions
Registry differences at logoff	Disabled	All VDA versions

Profile Management/Profile handling

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Delay before deleting cached profiles	0	All VDA versions
Delete locally cached profiles on logoff	Disabled	All VDA versions
Local profile conflict handling	Use local profile	All VDA versions
Migration of existing profiles	Local and roaming	All VDA versions
Path to the template profile	Disabled. New user profiles are created from the default user profile on the device where a user first logs on.	All VDA versions
Template profile overrides local profile	Disabled	All VDA versions
Template profile overrides roaming profile	Disabled	All VDA versions
Template profile used as a Citrix® mandatory profile for all logons	Disabled	All VDA versions

Profile Management/Registry

Name	Default setting	VDA
Exclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions
Inclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions

Profile Management/Streamed user profiles

Name	Default setting	VDA
Always cache	Disabled	All VDA versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Always cache size	0 Mb	All VDA versions
Profile streaming	Disabled	All VDA versions
Streamed user profile groups	Disabled. All user profiles within an OU are processed normally.	All VDA versions
Timeout for pending area lock files (days)	1 day	All VDA versions

Receiver

Name	Default setting	VDA
StoreFront™ accounts list	No stores are specified	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current

User personalization layer

Name	Default setting	VDA
User Layer Repository Path	Disabled. No path specified.	VDA 19.12 and later versions
User Layer Size in GB	10 GB. A user layer is a thin-provisioned disk that expands to the set size. User layers never decrease in size.	VDA 19.12 or later versions

Virtual Delivery Agent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Controller registration IPv6 netmask	No netmask is specified	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Controller registration port	80	All VDA versions
Controller SIDs	No SIDs are specified	All VDA versions
Controllers	No controllers are specified	All VDA versions
Enable auto update of controllers	Enabled	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Only use IPv6 controller registration	Disabled	VDA for Multi-session OS 7 through current, VDA for Single-session OS 7 through current
Site GUID	No GUID is specified	All VDA versions

Virtual Delivery Agent/HDX 3D Pro

Name	Default setting	VDA
Enable lossless	Enabled	VDA 5.5, 5.6 FP1
HDX 3D Pro quality settings		VDA 5.5, 5.6 FP1

Virtual Delivery Agent/Monitoring

Name	Default setting	VDA
Enable process monitoring	Disabled	VDA 7.11 through current
Enable resource monitoring	Enabled	VDA 7.11 through current

Virtual IP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Default setting	VDA
Virtual IP loopback support	Disabled	VDA 7.6 through current
Virtual IP virtual loopback programs list	None	VDA 7.6 through current

Policy settings reference

September 6, 2025

Policies include settings that are applied when the policy is enforced. Descriptions in this section also indicate if more settings are required to enable a feature or are similar to a setting.

Quick reference

The following tables list the settings that you can configure within a policy. Find the task that you want to complete in the left column, then locate its corresponding setting in the right column.

A full listing of all policy settings is available in .CHM (Compiled HTML) format and .CSV format. These files are available in the `\program files\citrix\grouppolicy` folder on the server where the broker (delivery controller) is installed. You can also download the latest version of the policy settings by clicking here.

Audio

For this task	Use this policy setting
Control whether to allow the use of multiple audio devices	Audio Plug N Play
Control whether to allow audio input from microphones on the user device	Client microphone redirection
Control audio quality on the user device	Audio quality
Control audio mapping to speakers on the user device	Client audio redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bandwidth for user devices

To limit bandwidth used for	Use this policy setting
Client audio mapping	Audio redirection bandwidth limit or Audio redirection bandwidth limit percent
Cut-and-paste using a local clipboard	Clipboard redirection bandwidth limit or Clipboard redirection bandwidth limit percent
Access in a session to local client drives	File redirection bandwidth limit or File redirection bandwidth limit percent
HDX™ MediaStream Multimedia Acceleration	HDX MediaStream Multimedia Acceleration bandwidth limit or HDX MediaStream Multimedia Acceleration bandwidth limit percent
Client session	Overall session bandwidth limit
Printing	Printer redirection bandwidth limit or Printer redirection bandwidth limit percent
TWAIN devices (such as a camera or scanner)	TWAIN device redirection bandwidth limit or TWAIN device redirection bandwidth limit percent
USB devices	Client USB device redirection bandwidth limit or Client USB device redirection bandwidth limit percent

Redirection of client drives and user devices

For this task	Use this policy setting
Control whether drives on the user device are connected when users log on to the server or not	Auto connect client drives
Control cut-and-paste data transfer between the server and the local clipboard	Client clipboard redirection
Control how drives map from the user device	Client drive redirection
Control whether users' local hard drives are available in a session	Client fixed drives and Client drive redirection
Control whether users' local floppy drives are available in a session	Client floppy drives and Client drive redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For this task	Use this policy setting
Control whether users' network drives are available in a session	Client network drives and Client drive redirection
Control whether users' local CD, DVD, or Blu-ray drives are available in a session	Client optical drives and Client drive redirection
Control whether users' local removable drives are available in a session	Client removable drives and Client drive redirection
Control whether users' TWAIN devices, such as scanners and cameras, are available in a session and control compression of image data transfers	Client TWAIN device redirection; TWAIN compression redirection
Control whether USB devices are available in a session	Client USB device redirection and Client USB device redirection rules
Improve the speed of writing and copying files to a client disk over a WAN	Use asynchronous writes

Content redirection

For this task	Use this policy setting
Control whether to use content redirection from the server to the user device	Host to client redirection

Desktop UI

For this task	Use this policy setting
Control whether Desktop wallpaper is used in users' sessions or not	Desktop wallpaper
View window contents while a window is dragged	View window contents while dragging

Graphics and multimedia

> **Important:**
>
> The Flash policy remains only to allow customers with older VDAs to use newer controllers (for example, version 1912 controllers) and still use Flash. This VDA version does not support Flash.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For this task	Use this policy setting
Control the maximum number of frames per second sent to user devices from virtual desktops	Target frame rate
Control the visual quality of images displayed on the user device	Visual quality
Control whether websites can display Flash content when accessed in sessions	Flash server-side content fetching URL list; Flash URL compatibility list; Flash video fallback prevention policy setting; Flash video fallback prevention error *.swf
Control compression of server-rendered video	Use video codec for compression; Use hardware encoding for video codec
Control the delivery of HTML5 multimedia web content to users	HTML5 video redirection

Prioritize Multi-Stream network traffic

For this task	Use this policy setting
Specify ports for ICA® traffic across multiple connections and establish network priorities	Multi-Port policy
Enable support for multi-stream connections among servers and user devices	Multi-Stream (computer and user settings)

Print

For this task	Use this policy setting
Control creation of client printers on the user device	Auto-create client printers and Client printer redirection
Control the location where printer properties are stored	Printer properties retention
Control whether the client or the server processes the print requests	Direct connections to print servers
Control whether users can access printers connected to their user devices	Client printer redirection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For this task	Use this policy setting
Control installation of native Windows drivers when automatically creating client and network printers	Automatic installation of in-box printer drivers
Control when to use the Universal Printer Driver	Universal print driver usage
Choose a printer based on a roaming user session information	Default printer
Load balance and set failover threshold for Universal Print Servers	Universal Print Servers for load balancing; Universal Print Servers out-of-service threshold

> **Note:**
>
> Policies can't be used to enable a screen saver in a desktop or application session. For users who require screen savers, the screen saver can be implemented on the user device.

ICA® policy settings

September 13, 2025

> **Note:**
>
> This page provides you descriptions and supported configuration values for ICA policy settings. For more information on working with policies, see Work with policies section.

Adaptive transport

This setting allows or prevents data transport over EDT as primary and over TCP as fallback.

By default, adaptive transport is enabled (**Preferred**), and EDT is used when possible, with fallback to TCP. You can change its setting as needed:

- **Preferred**. Adaptive transport over EDT is used when possible, with fallback to TCP.
- **Diagnostic mode**. EDT is forced on and fallback to TCP is disabled. We recommend this setting only for troubleshooting.
- **Off**. TCP is forced on, and EDT is disabled.

For more information, see Adaptive transport.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Drag and drop setting

This setting allows or prevents the dragging of files between the client and virtual applications or desktops. By default, the drag and drop policy is disabled. You can enable this policy if needed.

Application launch wait timeout

This setting specifies the wait timeout value in milliseconds for a session to wait for the first application to start. If the start of the application exceeds this time period, the session ends.

You can choose the default time (10,000 milliseconds) or specify a number in milliseconds.

Client clipboard redirection

This setting allows or prevents the clipboard on the user device being mapped to the clipboard on the server.

By default, clipboard redirection is allowed.

To prevent copy-and-paste data transfer between a session and the local clipboard, select **Prohibit**. Users can still copy and paste data between applications running in sessions.

After allowing this setting, configure the maximum allowed bandwidth the clipboard can consume in a client connection. Use the **Clipboard redirection bandwidth limit** or the **Clipboard redirection bandwidth limit percent** settings.

Client clipboard write allowed formats

When the **Restrict client clipboard write** setting is **Enabled**, host clipboard data cannot be shared with the client endpoint. You can use this setting to allow specific data formats to be shared with the client endpoint clipboard. To use this setting, enable it and add the specific formats to be allowed.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

The following custom formats are predefined in XenApp and XenDesktop and Citrix Virtual Apps and Desktops™:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML format is disabled by default. To enable this feature:

- Verify that **Client clipboard redirection** is set to **Allowed**.
- Verify that **Restrict client clipboard write** is set to **Enabled**.
- Add an entry for **CF_HTML** (and any other formats that you want supported) in **Client clipboard write allowed formats**.

You can add more custom formats. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if the **Client clipboard redirection** policy is set to **Prohibited** or the **Restrict client clipboard write** policy is set to **Disabled**.

> **Note:**
>
> Enabling HTML format clipboard copy support (CF_HTML) copies any scripts from the source of the copied content to the destination. Check that you trust the source before proceeding to copy. If you do copy content containing scripts, they are live only if you save the destination file as an HTML file and run it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limit clipboard client to session transfer size

This setting specifies the maximum size of clipboard data that a user can transfer from a client endpoint to a virtual session during a single copy-and-paste operation.

To limit clipboard transfer size, enable the **Limit clipboard client to session transfer size** setting. Then, in the **Size Limit** field, enter a value in kilobytes to define the size of data transfer between the local clipboard and a session.

By default, this setting is disabled and there's no limit on client to session transfers.

HDX™ Direct

HDX Direct allows the client to automatically establish a direct connection with the session host when direct communication is available. Connections are established securely using network-level encryption.

HDX Direct mode

HDX Direct can be used to establish direct connections with session hosts for internal and external clients. This setting determines if HDX Direct is available for internal clients only or for both internal and external clients.

When set to **Internal** only, HDX Direct attempts to establish direct connections for clients in the internal network only.

When set to **Internal** and **external**, HDX Direct attempts to establish direct connections for internal and external clients.

By default, HDX Direct is set for internal clients only.

HDX Direct port range

The range of ports that are used by HDX Direct for connections from external users.
By default, HDX Direct uses the port range: 55000–55250.

Limit clipboard session to client transfer size

This setting specifies the maximum size of clipboard data that a user can transfer from a virtual session to a client endpoint during a single copy-and-paste operation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To limit clipboard transfer size, enable the **Limit clipboard session to client transfer size** setting. Then, in the **Size Limit** field, enter a value in kilobytes to define the size of data transfer between a session and the local clipboard.

By default, this setting is disabled and there's no limit on session to client transfers.

Restrict client clipboard write

If this setting is **Enabled**, host clipboard data cannot be shared with the client endpoint. You can allow specific formats by enabling the **Client clipboard write allowed formats** setting.

By default, this setting is **Disabled**.

Restrict session clipboard write

When this setting is **Enabled**, client clipboard data cannot be shared with session applications. You can allow specific formats by enabling the **Session clipboard write allowed formats** setting.

By default, this setting is **Disabled**.

Session clipboard write allowed formats

When the **Restrict session clipboard write** setting is **Enabled**, client clipboard data cannot be shared with session applications. You can use this setting to allow specific data formats to be shared with the session clipboard.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

The following custom formats are predefined in XenApp and XenDesktop and Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML format is disabled by default. To enable this feature:

- Verify that **Client clipboard redirection** is set to **Allowed**.
- Verify that **Restrict session clipboard write** is set to **Enabled**.
- Add an entry for **CF_HTML** (and any other formats that you want supported) in **Session clipboard write allowed formats**.

You can add more custom formats. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if the **Client clipboard redirection** policy is set to **Prohibited** or the **Restrict session clipboard write** policy is set to **Disabled**.

> **Note:**
>
> Enabling HTML format clipboard copy support (CF_HTML) copies any scripts from the source of the copied content to the destination. Check that you trust the source before proceeding to copy. If you do copy content containing scripts, they are live only if you save the destination file as an HTML file and run it.

Desktop starts

This setting allows or prevents connections to a session on that VDA using an ICA connection by non-administrative users in a VDA Direct Access Users group.

By default, non-administrative users can't connect to these sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This setting doesn't affect non-administrative users in a VDA Direct Access Users group who are using an RDP connection. These users can connect to the VDA when this setting is enabled or disabled. This setting doesn't affect non-administrative users who aren't in a VDA Direct Access Users group. These users can't connect to the VDA when this setting is enabled or disabled.

ICA listener connection timeout

This setting specifies the maximum wait time for a connection using the ICA protocol to be completed.

By default, the maximum wait time is 120,000 milliseconds, or two minutes.

ICA listener port number

This setting specifies the TCP/IP port number used by the ICA protocol on the server.

By default, the port number is set to 1494.

Valid port numbers must be in the range of 0-65535 and must not conflict with other well-known port numbers. If you change the port number, restart the server for the new value to take effect. If you change the port number on the server, you must also change it on every Citrix Workspace™ app or plug-in that connects to the server.

Keyboard and Input Method Editor (IME)

This setting enables or disables the following:

- Dynamic keyboard layout synchronization
- Input Method Editor (IME)
- Unicode keyboard layout mapping
- Hides or shows the keyboard layout switch notification dialog message
- Automatic touch keyboard display for touch device end users

1. In Web Studio, select **Keyboard and IME**.
2. Select **Client keyboard layout synchronization and IME improvement** to control the dynamic keyboard layout synchronization and generic client Input Method Editor (IME) features in the VDA. You can configure:

   Disabled - dynamic keyboard layout synchronization and generic client Input Method Editor (IME).

   Support dynamic client keyboard layout synchronization - enables dynamic keyboard layout synchronization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support dynamic client keyboard layout synchronization and IME improvement - enables both dynamic keyboard layout synchronization and generic client Input Method Editor (IME).

3. Select **Enable Unicode keyboard layout mapping** to enable or disable Unicode keyboard mapping.
4. Select **Hide keyboard layout switch pop-up message box** to control whether or not a message appears, indicating that the keyboard layout is synchronizing when the user changes the client keyboard layout. If you prevent the message from appearing, the users must wait for a few moments before typing to avoid incorrect character input.
5. Select **Automatic keyboard display** to allow or prohibit whether the client side soft/touch keyboard shows or hides automatically when you enter or leave an input field.

Default settings:

- **Client keyboard layout synchronization and IME improvement**
  - Disabled in Windows Server 2019/2022/2025, and multi-session Win 10/11
  - Enabled in single-session Win 10/11
- **Unicode keyboard layout mapping**
  - Prohibited (indicates Unicode keyboard layout mapping is disabled by default, need to configure and allow it if end users are using Unicode input mode on the CWAs)
- **Hide keyboard layout switch pop-up message box**
  - Prohibited (indicates it will show the pop-up message box)
- **Automatic keyboard display**
  - Prohibited (indicated the client side soft/touch keyboard will not show or hide automatically when you enter or leave an input field)

This policy replaces the registry settings that are listed in the **Description** section of the policy settings.

Logoff checker startup delay

This setting specifies the duration to delay the logoff checker startup. Use this policy to set the time (in seconds) that a client session waits before disconnecting the session.

This setting also increases the time that it takes for a user to log off from the server.

Loss tolerant mode

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> - The feature requires a minimum of Citrix Workspace app 2002 for Windows. This version of the VDA supports it when it becomes available.
> - Loss tolerant mode for graphics is supported on Citrix Gateway and Citrix Gateway Service. This mode is available only with direct connections.

This setting enables or disables loss tolerant mode for graphics.

By default, loss tolerant mode for graphics is **Allowed**.

When allowed, the mode is entered when the packet loss and latency are above a threshold. You can set the thresholds using the loss tolerant thresholds policy.

Loss tolerant thresholds

When the Loss tolerant mode is available, this setting specifies the network metrics thresholds at which the session switches to loss tolerant mode for graphics.

The default thresholds are:

- Packet loss: 5%
- Latency: 300 ms (RTT)

For more information, see loss tolerant mode.

Loss tolerant mode for audio

This setting enables or disables the loss tolerant mode for audio.

When enabled, audio is sent over the loss tolerant mode.

By default, loss tolerant mode for audio is **Prohibited**.

To enable the policy, edit the registry of the loss tolerant mode for audio policy to **Allowed**.

EDT transport is required to enable loss tolerant mode for audio.

Rendezvous protocol

This setting changes how HDX sessions are proxied when using the Citrix Gateway Service. When enabled, HDX traffic no longer flows through the Citrix Cloud Connector. Instead, the VDA establishes an outbound connection directly to the Citrix Gateway Service (enhancing Cloud Connector scalability).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> A feature toggle in Citrix Cloud™ and an HDX policy setting controls this feature. The Citrix Cloud feature toggle is enabled by default while the HDX setting is disabled by default. The HDX setting affects only HDX sessions established through the Citrix Gateway Service. This setting does not affect sessions established directly between client and VDA or through an on-premises Citrix Gateway.

For information, see Rendezvous protocol.

Rendezvous proxy configuration

This setting allows you to configure an explicit proxy for use with the Rendezvous protocol. If using a transparent proxy, this setting does not need to be enabled.

By default, this setting is disabled.

When disabled, the VDA doesn't route outbound traffic through any non-transparent proxies when trying to establish a Rendezvous connection with the Gateway Service.

When enabled, the VDA attempts to establish a Rendezvous connection with the Gateway Service through the proxy defined in this setting.

The VDA supports using HTTP and SOCKS5 proxies for Rendezvous connections. To configure the VDA to use a proxy for the Rendezvous connection, you must enable this setting. Also, specify either the address of the proxy or the path to the PAC file. For example:

- Proxy address: `http://<URL or IP>:<port>` or `socks5://<URL or IP>:<port>`
- PAC file: `http://<URL or IP>/<path>/<filename>.pac`

  VDA version 2103 is the minimum supported version for proxy configuration with a PAC file. For more information on the PAC file schema for SOCKS5 proxies, see Proxy configuration.

> **Note:**
>
> Only SOCKS5 proxies support data transport through EDT. For an HTTP proxy, use TCP as the transport protocol for ICA.

For more information, see Rendezvous protocol.

Starting of non-published programs during client connection

This setting specifies whether to allow starting initial applications through RDP on the server.

By default, starting initial applications through RDP on the server isn't allowed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session metric collection

This setting allows Citrix to collect user and machine session metrics between the VDA and Workspace to improve the user experience.

Citrix collects data such as operating system, uptime, computer system information, video controller details, VDA version, deployment type, and domain joined status are collected. Additionally, you can gather some session configurations, along with performance and reliability data, to aid product improvement efforts. For more information on our Customer Experience Improvement Program, see:

- https://more.citrix.com/XD-CEIP
- https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program
- https://docs.citrix.com/en-us/mac-vda/configure/session/supportability-service

By default, this setting is enabled.

Tablet mode toggle policy settings

Tablet mode toggle optimizes the look and behavior of Store apps, Win32 apps, and the Windows shell on the VDA. It does so by automatically toggling the virtual desktop to Tablet mode when connecting from small form factor devices like phones and tablets, or any touch-enabled device.

If this policy is disabled, the VDA is in the mode the user sets it to and maintains the same mode throughout, regardless of the type of client.

Auto client reconnect policy settings

September 6, 2025

The **Auto Client Reconnect** section contains policy settings for controlling the automatic reconnection of sessions.

Auto client reconnect

This setting allows or prevents automatic reconnection by the same client after a connection has been interrupted.

For Citrix Receiver for Windows 4.7 and later and Citrix Workspace app 1808 and later, auto client reconnect uses only the policy settings from Citrix Studio. Updates to these policies in Studio synchronize auto client reconnect from server to client. With older versions of Citrix Receiver for Windows, to configure auto client reconnect, use a Studio policy and change the registry or the default.ica file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allowing automatic client reconnect allows users to resume working where they were interrupted when a connection was broken. Automatic reconnection detects broken connections and then reconnects the users to their sessions.

If the Citrix Workspace™ app cookie containing the key to the session ID and credentials isn't used, automatic reconnection might result in a new session being started. That is, instead of reconnecting to an existing session. The cookie is not used if it has expired. For example, the cookie might expire because of a delay in reconnection, or if credentials must be reentered. If users intentionally disconnect, auto client reconnect is not triggered.

A session window is grayed out when a reconnection is in progress. A countdown timer displays the time remaining before the session is reconnected. When a session times out, it is disconnected.

For application sessions, when automatic reconnect is allowed, a countdown timer appears in the notification area. This timer specifies the time remaining before the session is reconnected. Citrix Workspace app tries to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For user sessions, when automatic reconnect is allowed, Citrix Workspace app tries to reconnect to the session for a specified period, unless there's a successful reconnection or the user cancels the reconnection attempts. By default, this period is two minutes. To change this period, edit the policy.

By default, automatic client reconnect is allowed. You can disable it by setting the policy to **Prohibited**.

Auto client reconnect authentication

This setting specifies whether authentication is required for automatic client reconnections.

When a user initially logs on, the credentials are encrypted, stored in memory, and a cookie is created containing the encryption key. The cookie is sent to Citrix Workspace app. When this setting is configured, cookies are not used. Instead, a dialog box is displayed to users requesting credentials when Citrix Workspace app attempts to reconnect automatically.

By default, authentication is not required.

Auto client reconnect logging

This setting enables or disables recording of auto client reconnections in the event log.

When logging is enabled, the server System Log captures information about successful and failed automatic reconnection events. A site does not provide a combined log of reconnection events for all servers.

By default, logging is disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auto client reconnect timeout

By default, auto-client reconnect timeout is set to 120 seconds, the maximum configurable value for an auto-client reconnect timeout is 300 seconds. Use this policy to set the timeout value.

Reconnect UI transparency level

This setting lets you specify the opacity level applied to the XenApp or XenDesktop® session window during session reliability reconnection time.

By default, Reconnect UI transparency is set to 80%.

Audio policy settings

September 6, 2025

The **Audio** section includes policy settings that allow user devices to send and receive audio in sessions without reducing performance.

Adaptive Audio

This setting enables or disables adaptive audio. When you enable this policy, the audio quality settings are adjusted dynamically to provide the best user experience. This setting applies to both single-session OS and multi-session OS sessions of VDAs using Citrix Virtual Apps and Desktops™ 2109 or later.

When this setting is prohibited, the audio quality policy is applied. For more information see, Audio quality.

By default, the adaptive audio policy is enabled.

Audio over UDP real-time transport

This setting allows or prevents the transmission and receipt of audio between the VDA and user device over RTP using the User Datagram Protocol (UDP). When this setting is disabled, audio is sent and received over TCP.

By default, audio over UDP is allowed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Audio Plug N Play

This setting allows or prevents the use of multiple audio devices to record and play sound.

By default, the use of multiple audio devices is allowed.

This setting applies only to Windows Multi-session OS machines.

Audio quality

This setting specifies the quality level of sound received in user sessions.

By default, sound quality is set to High - high definition audio.

To control sound quality, choose one of the following options:

- Select Low - for low speed connections for low-bandwidth connections. Sounds sent to the user device are compressed up to 16 Kbps. This compression results in a significant reduction in the quality of the sound. But also allows reasonable performance for a low-bandwidth connection.
- Select Medium - optimized for speech to deliver Voice over Internet Protocol applications. This setting delivers media applications in challenging network connections with lines less than 512 Kbps, or significant congestion and packet loss. This codec offers fast encode time, making it ideal for use with softphones and Unified Communications applications when you require server-side media processing.

  Audio sent to the user device is compressed up to 64 Kbps. This compression results in a moderate reduction in the quality of the audio played on the user device while providing low latency and consuming low bandwidth. If Voice over Internet Protocol quality is unsatisfactory, ensure that the Audio over UDP Real-time Transport policy setting is set to Allowed.

  Now, Real-time Transport (RTP) over UDP is only supported when this audio quality is selected. Use this audio quality even for delivering media applications for challenging network connections like low (fewer than 512 Kbps) lines. Also, when there is congestion and packet loss in the network.
- Select High - high definition audio for connections where bandwidth is plentiful and sound quality is important. Clients can play sound at its native rate. Sounds are compressed at a high quality level maintaining up to CD quality, and using up to 112 Kbps of bandwidth. Transmitting this amount of data can result in increased CPU usage and network congestion.

Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption doubles.

To specify the maximum amount of bandwidth, configure the **Audio redirection bandwidth limit** or the **Audio redirection bandwidth limit percent** settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client audio redirection

This setting specifies whether applications hosted on the server can play sounds through a sound device installed on the user device. This setting also specifies whether users can record audio input.

By default, audio redirection is allowed.

After allowing this setting, you can limit the bandwidth consumed by playing or recording audio. Limiting the amount of bandwidth consumed by audio can improve application performance but might also degrade audio quality. Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption doubles. To specify the maximum amount of bandwidth, configure the **Audio redirection bandwidth limit** or the **Audio redirection bandwidth limit percent** settings.

On Windows Multi-session OS machines, ensure that the **Audio Plug N Play** setting is enabled to support multiple audio devices.

Important: Prohibiting Client audio redirection disables all HDX™ audio functionality.

Client microphone redirection

This setting enables or disables client microphone redirection. When enabled, users can use microphones to record audio input in a session.

By default, microphone redirection is allowed.

For security, users are alerted when untrusted servers by their devices try to access microphones. Users can choose to accept or not accept access. Users can disable the alert on Citrix Workspace™ app.

On Windows Multi-session OS machines, ensure that the Audio Plug N Play setting is Enabled to support multiple audio devices.

If the **Client audio redirection** setting is disabled on the user device, this rule has no effect.

Bandwidth policy settings

September 6, 2025

The **Bandwidth** section includes policy settings to avoid performance problems related to client session bandwidth use.

Important: Using these policy settings with the **Multi-Stream policy** settings might produce unexpected results. If you use Multi-Stream settings in a policy, ensure that these bandwidth limit policy settings aren't included.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Audio redirection bandwidth limit

This setting specifies the maximum allowed bandwidth for playing or recording audio in a user session. The maximum allowed bandwidth is specified in kilobits per second.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **Audio redirection bandwidth limit percent** setting, the most restrictive setting (lower value) is applied.

Audio redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth limit for playing or recording audio as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **Audio redirection bandwidth limit** setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions.

Client USB device redirection bandwidth limit

This setting specifies the maximum allowed bandwidth for the redirection of USB devices to and from the client. The maximum allowed bandwidth is specified in kilobits per second.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **Client USB device redirection bandwidth limit percent** setting, the most restrictive setting (the lower value) is applied.

Client USB device redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for the redirection of USB devices to and from the client as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **Client USB device redirection bandwidth limit** setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Clipboard redirection bandwidth limit

This setting specifies the maximum allowed bandwidth for data transfer between a session and the local clipboard. The maximum allowed bandwidth is specified in kilobits per second.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **Clipboard redirection bandwidth limit percent** setting, the most restrictive setting (the lower value) is applied.

Clipboard redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for data transfer between a session and the local clipboard as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **Clipboard redirection bandwidth limit** setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions.

COM port redirection bandwidth limit

> **Note:**
>
> For the Virtual Delivery Agent 7.0 through 7.8, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

This setting specifies the maximum allowed bandwidth in kilobits per second for accessing a COM port in a client connection. If you enter a value for this setting and a value for the **COM port redirection bandwidth limit percent** setting, the most restrictive setting (the lower value) is applied.

COM port redirection bandwidth limit percent

Note: For the Virtual Delivery Agent 7.0 through 7.8, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

This setting specifies the maximum allowed bandwidth for accessing COM ports in a client connection as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you enter a value for this setting and a value for the **COM port redirection bandwidth limit** setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions

File redirection bandwidth limit

This setting specifies the maximum allowed bandwidth for accessing a client drive in a user session. The maximum allowed bandwidth is specified in kilobits per second.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **File redirection bandwidth limit percent** setting, the most restrictive setting (the lower value) takes effect.

File redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth limit for accessing client drives as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **File redirection bandwidth limit** setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions.

HDX™ MediaStream Multimedia Acceleration bandwidth limit

This setting specifies the maximum allowed bandwidth limit for delivering streaming audio and video using HDX MediaStream Multimedia Acceleration. The maximum allowed bandwidth is specified in kilobits per second.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **HDX MediaStream Multimedia Acceleration bandwidth limit percent** setting, the most restrictive setting (the lower value) takes effect.

HDX MediaStream Multimedia Acceleration bandwidth limit percent

This setting specifies the maximum allowed bandwidth for delivering streaming audio and video using HDX MediaStream Multimedia Acceleration as a percentage of the total session bandwidth.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **HDX MediaStream Multimedia Acceleration bandwidth limit** setting, the most restrictive setting (the lower value) takes effect.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions.

LPT port redirection bandwidth limit

Note: For the Virtual Delivery Agent 7.0 through 7.8, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

This setting specifies the maximum allowed bandwidth for print jobs using an LPT port in a single user session. The maximum allowed bandwidth is specified in kilobits per second.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **LPT port redirection bandwidth limit percent** setting, the most restrictive setting (the lower value) is applied.

LPT port redirection bandwidth limit percent

Note: For the Virtual Delivery Agent 7.0 through 7.8, configure this setting using the registry; see Configure COM Port and LPT Port Redirection settings using the registry.

This setting specifies the bandwidth limit for print jobs using an LPT port in a single client session as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **LPT port redirection bandwidth limit** setting, the most restrictive setting (the lower value) is applied.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions.

Overall session bandwidth limit

This setting specifies the total amount of bandwidth available, in kilobits per second, for user sessions.

The maximum enforceable bandwidth cap is 20 Mbps (20,000 Kbps). By default, no maximum (zero) is specified.

Limiting the amount of bandwidth consumed by a client connection can improve performance when other applications outside the client connection are competing for limited bandwidth.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Printer redirection bandwidth limit

This setting specifies the maximum allowed bandwidth for accessing client printers in a user session. The maximum allowed bandwidth is specified in kilobits per second.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **Printer redirection bandwidth limit percent** setting, the most restrictive setting (the lower value) is applied.

Printer redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for accessing client printers as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **Printer redirection bandwidth limit** setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions.

TWAIN device redirection bandwidth limit

This setting specifies the maximum allowed bandwidth for controlling TWAIN imaging devices from published applications. The maximum allowed bandwidth is specified in kilobits per second.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **TWAIN device redirection bandwidth limit percent** setting, the most restrictive setting (the lower value) is applied.

TWAIN device redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for controlling TWAIN imaging devices from published applications as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the **TWAIN device redirection bandwidth limit** setting, the most restrictive setting (having the lower value) is applied.

If you configure this setting, you must also configure the **Overall session bandwidth limit** setting, which specifies the total amount of bandwidth available for client sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bidirectional content redirection policy settings

September 6, 2025

The **Bidirectional Content Redirection** section has policy settings to enable or disable the client-to-VDA and VDA-to-client URL redirection.

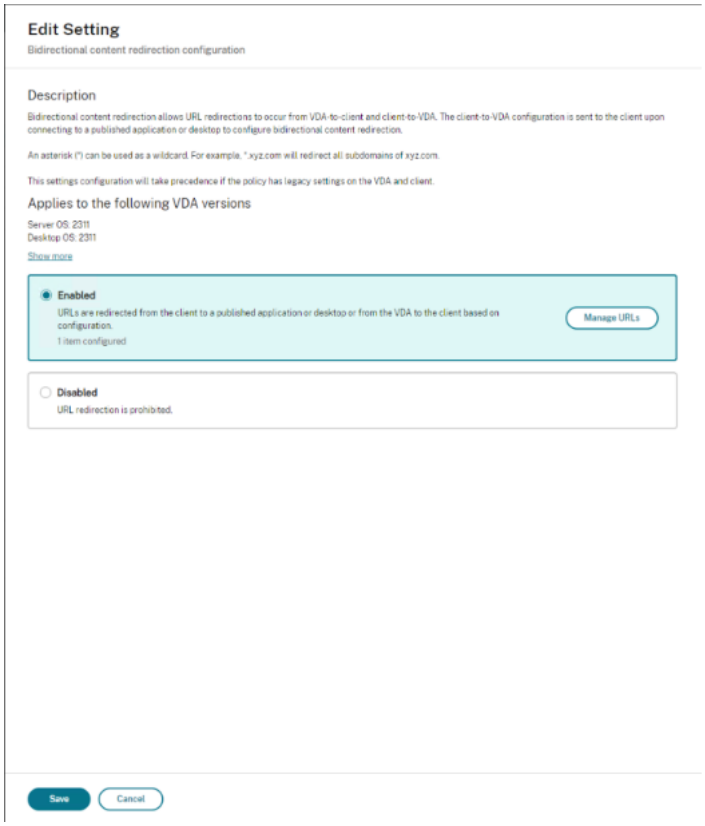
Server policies are set in Web Studio. Starting with the Citrix Workspace™ app version 2311, this setting replaces the following three legacy settings in Web Studio which are deprecated:

- 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 Group Policy Object (GPO) settings on Windows clients:

- Bidirectional content redirection
- Bidirectional content redirection overrides
- OAuth redirection

If this setting is enabled, the client-to-VDA settings are sent to the client upon connecting to a published app or desktop to configure bidirectional content redirection.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

If this setting is configured, it takes precedence over the legacy settings in Web Studio and on the client. Citrix® recommends using only the new policy settings and deleting any legacy settings to avoid unexpected behavior.

Client policies must not be set if the VDA and DDC are running version 2311 or later. Otherwise, client policies are set from the Citrix Workspace app Group Policy Object administration template.

Citrix offers host-to-client redirection and Local App Access for client-to-URL redirection. However, Citrix recommends that you use bidirectional content redirection for domain-joined Windows clients.

Citrix recommends using the new UI in Web Studio to configure the feature instead of the Desktop Studio.

Wildcard redirection

Bidirectional content redirection supports the use of wildcards when defining the URLs to be redirected. For more details and to configure bidirectional content redirection, see the Configuration instructions.
In Web Studio, set the wildcard URL by editing the JSON string as a value in the `url` key in the `hostToClientUrls` array or the `clientToHostUrls` array.

> **Note:**
>
> - Don't set the same URL in `hostToClientUrls` and `clientToHostUrls` to avoid infinite loops.
> - Top-level domains are not supported. For example, https://www.citrix.* or http://www.citrix.co* is not redirected.

Bidirectional content redirection configuration

Set this policy to `Enabled` to start configuring the feature and click **Manage URLs**. Set the following configurations:

- **VDA-to-client redirection**
- **Client-to-VDA redirection**

VDA-to-client redirection

To redirect URLs from VDA to the client, enter one URL per line. Wildcards are allowed.
OAuth redirection enables you to use the browser on the client endpoint to perform authentication and send the token back to the VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benefits:

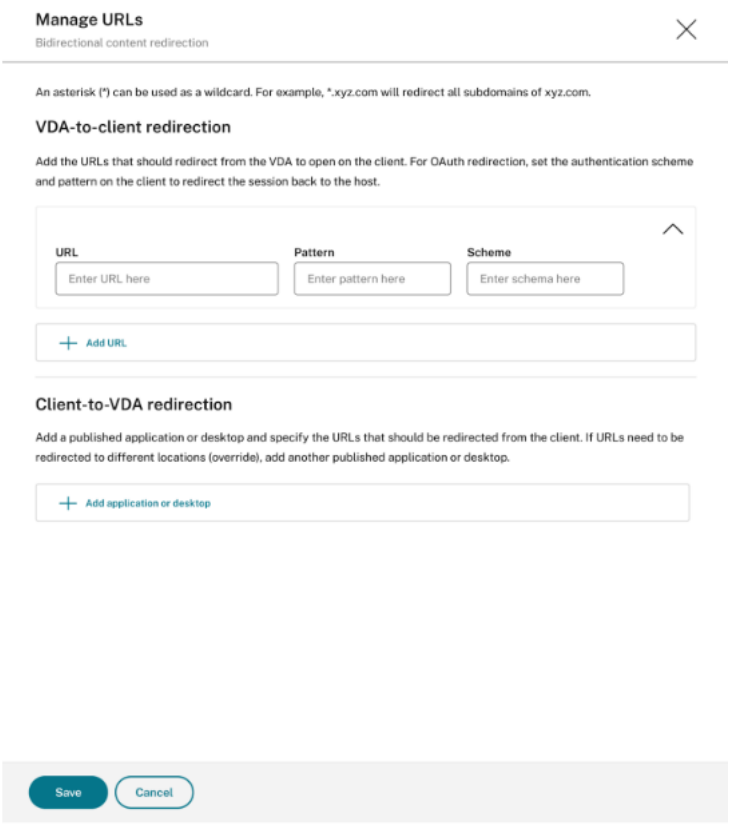
- You can avoid storing these credentials in the hosted environment.
- You can use biometric capabilities that are available on the endpoint and not on the VDA.

Configurations:

To configure VDA-to-client redirection for the URL, specify the following:

- **URL** (Required) Add the URL that must 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 **Scheme** is specified, the terminating URL is expected to be of the form: `<scheme>://<something>`. Consider Scheme is not specified (empty). In that case, the original resulting URL pattern is extracted from the Pattern through 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). In this case, any OAuth Authorization server must be configured to allow `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` redirect URLs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



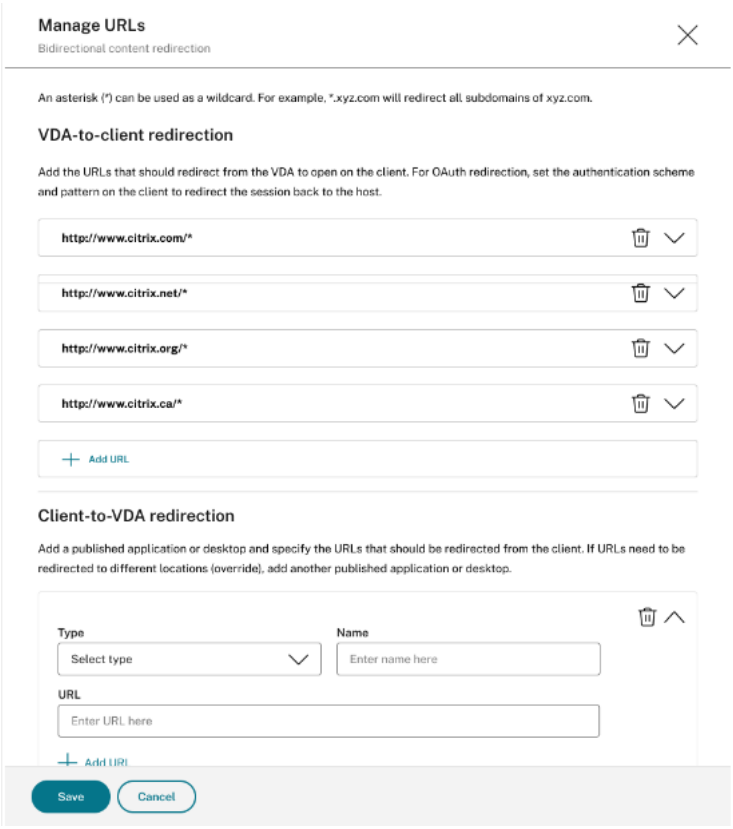
> **Note:**
>
> Though both **Pattern** and **Scheme** are optional, if **Pattern** is specified, you must also specify **Scheme**.

Client-to-VDA redirection

To redirect URLs from the client to VDA, complete the following steps:

1. Configure the destination for client URLs.
2. Select either Published Application or Published Desktop.
3. Specify the name of that resource.
4. Add all URLs that must be redirected to that resource.
   You can override this default resource by adding a new application or desktop and then specifying the URLs to redirect to that resource.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Desktop Studio

> **Note:**
>
> Citrix recommends using Web Studio to configure this feature from Citrix Virtual Apps and Desktops™ version 2402 onwards.

To configure bidirectional content redirection for 2311, create a JSON string with the following format:

```
{

  "version": 1,
  "hostToClientConfig": [
    {

      "hostToClientUrls": [
        {

          "url": "http://www.citrix.com/*"
        }
 ,
        {

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "url": "www.example.com"
          }
,
        {

          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/oauth2
             ?.*",
          "oAuthScheme": "idm.desktop-authentication"
         }

       ]
     }

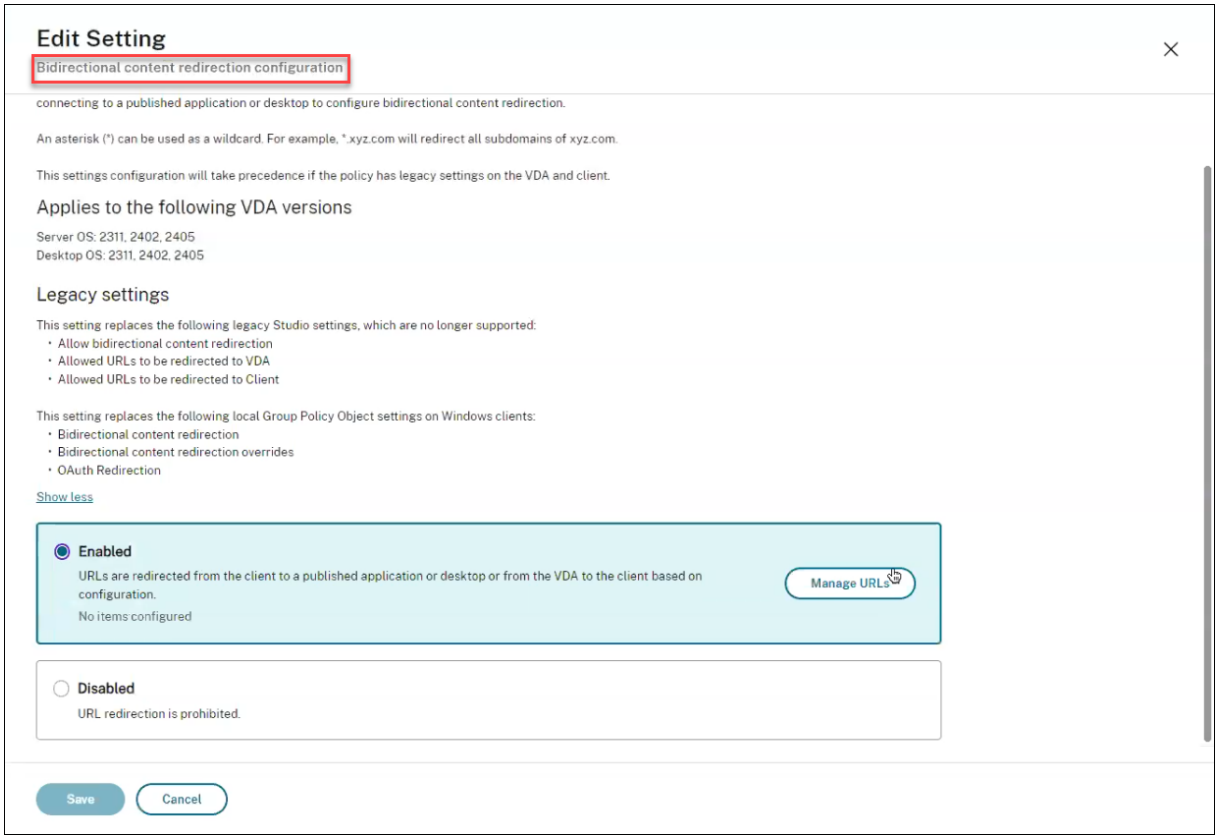
 ],
 "clientToHostConfig": [
   {

     "publishedAppOrDesktopNameType": "Desktop",
     "publishedAppOrDesktopName": "Win11Desktop",
     "clientToHostUrls": [
       "https://www.example.net",
       "https://*.citrix.example"
     ]
    }
,
   {

     "publishedAppOrDesktopNameType": "Application",
     "publishedAppOrDesktopName": "Chrome",
     "clientToHostUrls": [
       "https://tibco.example"
     ]
    }

 ]
}
```

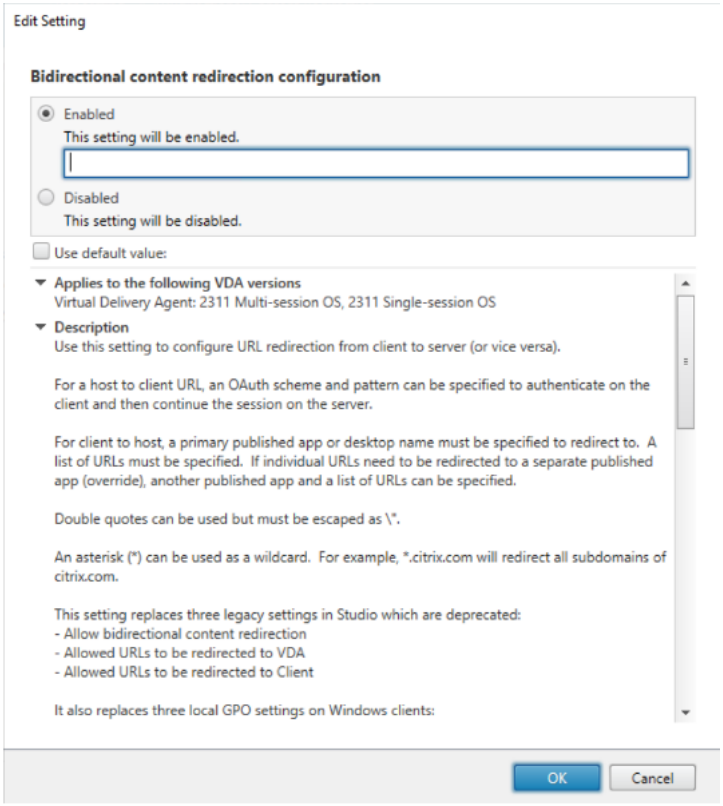
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following parameters must be set:

- **version**: (Required) Set to 1.
- For VDA-to-client URL redirection, create a single `hostToClientConfig`.
- **hostToClientUrls**: (Required) List of URLs to be redirected from host (VDA) to client. Wildcards are allowed. If '*'is specified, then `clientToHostConfig` must be specified with `publishedAppOrDesktopNameType`, an empty `publishedAppOrDesktopName`, and an empty `clientToHostUrls`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



OAuth redirection

OAuth redirection enables you to use the client endpoint browser to authenticate and send the token back to the VDA.

Benefits:

- You can avoid storing these credentials in the hosted environment.
- You can use biometric capabilities that are available on the endpoint and not on the VDA.

To configure OAuth redirection for the URL, specify the following parameters:

- **oAuthRedirectionPattern**: (Optional) URL regular expression that, when redirected to the client via 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.
- **oAuthScheme**: (Optional) If a Scheme is specified, the terminating URL is expected to be in the form: `<scheme>://<something>`. Consider Scheme is not specified (empty). In that case, the original resulting URL pattern is extracted from the Pattern through 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

redirected back into the Host (VDA). In this case, any OAuth Authorization server must be configured to allow `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` redirect URLs.

For a client-to-VDA redirection, create **clientToHostConfig** for each resource to redirect.
For each resource, include the following parameters:

- **publishedAppOrDesktopNameType**: (Required) Either a published desktop ("Desktop") or a published application ("Application") configured in Web Studio. If the resource is not valid, redirection does not function correctly.
- **publishedAppOrDesktopName**: (Required) Resource name as configured in Web Studio.
- **clientToHostUrls**: (Required) List of URLs to be redirected from client to host (VDA). Wildcards are allowed.

Known limitation

When you launch a browser using PowerShell with a custom URL scheme (not HTTP or HTTPS), the custom URLs are not redirected to the client.

Browser content redirection policy settings

September 6, 2025

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.
This documentation details each of the policy setting option available for Browser Content Redirection

Browser content redirection

This setting acts as the main on/off switch for Browser Content Redirection.

- **What it does:** Determines whether web pages are rendered on the server or your local device. When enabled, Citrix Workspace™ app tries to fetch and display web content on your device for a smoother experience. If that fails, it falls back to rendering on the server.
- **Options:**
  - **Allowed:** (Default) Enables Browser Content Redirection.
  - **Prohibited:** Disables Browser Content Redirection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Things to note:** If allowed, Citrix Workspace app attempts client fetch and client render. If client fetch and client render fails, Browser content redirection will fall back to server side rendering. To enable server fetch and client render, enable the "Browser Content Redirection Proxy Configuration"setting.

Browser content redirection ACL configuration

This setting lets you create a list of websites (URLs) that are allowed or not allowed from using Browser Content Redirection.

- **What it does:** Gives you fine-grained control over which websites are optimized with Browser Content Redirection. You can specify entire websites or specific pages.
- **How it works:**
  - **Allowed URLs:** Websites on this list will have their content displayed on your device. You can use wildcards (*) to include multiple pages or subdomains (e.g., *https://www.example.com/* or http://*.example.com/). Wild cards are not permitted within the protocol of the URL.
- **Default:** https://www.youtube.com/*
- **Example:**
  - **Allowed Patterns:** http://www.xyz.com/index.html, <https://www.xyz.com/* , http://www.xyz.com/*vi* , http://*.xyz.com/%3C>
  - **Not Allowed:** http://*.*.com/
  - You can achieve better granularity by specifying paths in the URL. For example, if you specify https://www.xyz.com/sports/index.html , only the index.html page is redirected

Browser content redirection block list configuration

This setting works in conjunction with the "Browser Content Redirection ACL Configuration"setting.

- **What it does:** Provides an extra layer of control by letting you block specific websites or pages, even if they are allowed in the ACL configuration. The block list takes priority.
- **How it works:** You specify websites or pages that you don't want to be redirected to your device, even if they are generally allowed by the ACL configuration.
- **Default:** No URL is configured
- **Wildcards:** Similar to the ACL configuration, you can use wildcards (*) to block multiple pages or subdomains.
- **Example:** To block only the index.html page on a website, you would enter: https://www.example.com/sports/index.html

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Browser content redirection authentication sites

This setting lets you manage how Browser Content Redirection works with websites that use external identity providers (IdPs) for logins.

- **What it does:** Ensures that Browser Content Redirection stays active even when you're redirected to a different website for authentication (like when a website uses Okta or another service for login).
- **How it works:** You add the URLs of the authentication websites to this list so that the redirection process isn't interrupted during login.
- **Default:** No URL is configured
- **Example:** If www.example.com uses www.example.okta.com for authentication, you would add www.example.com/ to the Browser content redirection ACL configuration and the authentication websites www.example.okta.com to the Browser content redirection authentication sites
- **More info:** See Citrix Knowledge Center article CTX238236 and Multimedia section in Browser Content Redirection for detailed information.

Browser content redirection proxy configuration

This setting gives you more control over how Browser Content Redirection uses your network's proxy server as well as facilitate server fetch client render in case your environment doesn't allow for client fetch client render.

- **What it does:** Forces Citrix Workspace app to use a server fetch method for fetching web content. When enabled, it always tries to fetch content from the server and display it on your device.
- **Options:**
    - Explicit Proxy: Use a specific proxy server. You'll need to provide the proxy server's address and port number (e.g., http://proxy.example.com:80)
        - Allowed patterns:

http://<hostname/ip address>:	Example: http://proxy.example.citrix.com:80 http://10.10.10.10:8080

        -
    - PAC/WPAD: Use a PAC file or WPAD to automatically determine proxy settings. You'll need to provide the URL of the PAC file (e.g., http://wpad.myproxy.com:30/configuration/pac/Proxy.pac).
        - Allowed patterns for PAC/WPAD files:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

http://<hostname/ip address>://.pac	Example: http://wpad.myproxy.com:30/configuration/pac/Proxy.pac

•

https://<hostname/ip address>://	Example: http://10.10.10.10/configuration/pac/wpad.dat

•

- Direct/Transparent: Do not use a proxy server, or use a transparent proxy.
  - Configure the key word "DIRECT"
  - The keyword is case sensitive

- **Default:** Prohibited (disabled)

Browser content redirection Integrated Windows authentication support

This setting simplifies logins to websites that use Integrated Windows Authentication (IWA).

- **What it does:** Allows Browser Content Redirection to use your existing Windows credentials to log in to websites automatically. This means you won't have to enter your username and password repeatedly.
- **Options:**
  - **Allowed:** Enables single sign-on (SSO) for websites using IWA.
  - **Prohibited:** (Default) Disables SSO, requiring you to enter your credentials each time.

Browser content redirection server fetch proxy auth

This setting controls how Browser Content Redirection interacts with your web proxy when fetching content from the server.

- **What it does:** Allows Browser Content Redirection to use your Windows credentials to authenticate with the proxy server, ensuring secure access to web content.
- **How it works:** When enabled, Browser Content Redirection will automatically obtain and use a Kerberos service ticket to authenticate with the proxy.
- **Requirements:** You need to configure your PAC file to route traffic through a downstream web proxy and set up the proxy to use Kerberos authentication.
- **Options:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Allowed:** Enables Kerberos authentication with the proxy server.
- **Prohibited:** (Default) Browser Content Redirection will use basic authentication or other available credentials to authenticate with the proxy.

Client sensors policy settings

September 6, 2025

The **Client Sensors** section includes policy settings for controlling how mobile device sensor information is handled in a user session.

Allow applications to use the physical location of the client device

This setting determines whether applications running in a session on a mobile device are allowed to use the physical location of the user device.

By default, the use of location information is prohibited

When this setting is prohibited, attempts by an application to retrieve location information return a ‘‘permission denied’’value.

When this setting is allowed, a user can prohibit use of location information by denying a Citrix Workspace™ app request to access the location. Android and iOS devices prompt at the first request for location information in each session.

When developing hosted applications that use the Allow applications to use the physical location of the client device setting, consider the following:

- Ensure that a location-enabled application doesn’t rely on location information being available because:
  - A user might not allow access to location information.
  - The location might not be available or might change while the application is running.
  - A user might connect to the application session from a different device that does not support location information.
- A location-enabled application must:
  - Have the location feature off by default.
  - Provide the user an option to allow or disallow the feature while the application is running.
  - Provide the user an option to clear location data that the application caches. (Citrix Workspace app does not cache location data.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A location-enabled application must manage the granularity of the location information. This management ensures that the data acquired is appropriate to the purpose of the application. Also, conforms to regulations in all relevant jurisdictions.
- Enforce a secure connection (for example, using TLS or a VPN) when using location services. Connect Citrix Workspace app to trusted servers.
- Consider obtaining legal advice regarding the use of location services.

Desktop UI policy settings

September 6, 2025

The **Desktop UI** section includes policy settings that control visual effects such as desktop wallpaper, menu animations, and drag images. These policy settings help to manage the bandwidth used in client connections. You can improve application performance on a WAN by limiting bandwidth usage.

> **Important:**
>
> We do not support legacy graphics mode and Desktop Composition Redirection (DCR) in this release. This policy is included only for backward compatibility when using:
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Previous VDA releases with Windows 7 and Windows 2008 R2.

Desktop Composition Redirection

This setting specifies whether to use the processing capabilities of the following for local DirectX graphics rendering to provide users with a more fluid Windows desktop experience:

- Graphics processing unit (GPU) on the user device
- Or,
- Integrated graphics processor (IGP) on the user device

When enabled, **Desktop Composition Redirection** delivers a highly responsive Windows experience while maintaining high scalability on the server.

By default, **Desktop Composition Redirection** is disabled.

To deselect **Desktop Composition Redirection** and reduce the bandwidth required in user sessions, select **Disabled** when you add this setting to a policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Desktop Composition Redirection graphics quality

This setting specifies the quality of graphics used for Desktop Composition Redirection.

The default is High.

Choose from High, Medium, Low, or Lossless quality.

Desktop wallpaper

This setting allows or prevents wallpaper showing in user sessions.

By default, user sessions can show wallpaper.

To deselect desktop wallpaper and reduce the bandwidth required in user sessions, select **Prohibited** when adding this setting to a policy.

Menu animation

This setting allows or prevents menu animation in user sessions.

By default, menu animation is allowed.

Menu animation is a Microsoft personal preference setting for ease of access. When enabled, it causes a menu to appear after a short delay, either by scrolling or fading in. An arrow icon appears at the bottom of the menu. The menu appears when you point to that arrow.

Menu animation is enabled on a desktop if this policy setting is set to **Allowed** and the menu animation Microsoft personal preference setting is enabled.

> **Note:**
>
> Changes to the menu animation Microsoft personal preference setting affect the desktop. Consider that you set the desktop to discard changes when the session ends. In this case, a user, who has enabled menu animations, might not have menu animation in subsequent sessions. For users who require menu animation, enable the Microsoft setting in the main image for the desktop or ensure that the desktop retains user changes.

View window contents while dragging

This setting allows or prevents the display of window contents when dragging a window across the screen.

By default, viewing window contents is allowed.

When set to **Allowed**, the entire window appears to move when you drag it. When set to **Prohibited**, only the window outline appears to move until you drop it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

End user monitoring policy settings

September 6, 2025

The **End User Monitoring** section includes policy settings for measuring session traffic.

Endpoint location data collection

By default, this policy is disabled.
When enabled, endpoint location data is collected, including the public IP address, country, city, and Internet Service Provider (ISP) of the endpoint device.
Data collected is shown in Citrix Director or Monitor under the **Session Performance** tab for a selected user session.

Endpoint network latency measurement interval

By default, this policy is disabled.
This setting specifies the frequency, in seconds, at which the endpoint measures the network latency.
When enabled, data collected is shown in Citrix Director or Monitor under the **Session Performance** tab for a selected user session.

Endpoint statistics interval

Endpoint statistics like Network interface type, Signal strength, Link speed, Throughput outgoing, Throughput incoming etc. are available as endpoint telemetry in the session topology on the Director or Monitor UI. This telemetry helps with triaging end-user session issues.
Endpoint statistics interval indicates the frequency, in seconds, at which endpoint telemetry is refreshed in the Session topology within Director or Monitor UI. By default, endpoint telemetry is enabled and refreshed every 60 seconds.
Data collected is shown in Citrix Director or Monitor under the **Session Performance** tab for a selected user session.

ICA® round trip calculation

This setting determines whether ICA round trip calculations are done for active connections.

By default, calculations for active connections are enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, each ICA round trip measurement initiation is delayed. This delay is until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

ICA round trip calculation interval

This setting specifies the frequency, in seconds, at which ICA round trip calculations are performed.

By default, the ICA round trip is calculated every 15 seconds.

ICA round trip calculations for idle connections

This setting determines whether ICA round trip calculations are done for idle connections.

By default, calculations are not performed for idle connections.

By default, each ICA round trip measurement initiation is delayed. This delay is until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

Enhanced desktop experience policy setting

September 6, 2025

The Enhanced desktop experience policy setting runs sessions on server-operating systems that look like local Windows 7 desktops.

By default, this setting is allowed.

If a user profile with the Windows Classic theme exists on the virtual desktop, this policy does not provide an enhanced desktop experience for that user. Consider a user with a Windows 7 theme user profile logs on to a virtual desktop running Windows Server 2012. Also, this policy is either not configured or disabled. In this case, that user sees an error message indicating failure to apply the theme.

In both cases, resetting the user profile resolves the issue.

If you disable the policy on a virtual desktop with active user sessions, the interface of those sessions becomes inconsistent on Windows 7 and Windows Classic desktops. To avoid this inconsistency, ensure you restart the virtual desktop after changing this policy setting. Then delete any roaming profiles on the virtual desktop. Citrix® also recommends deleting any other user profiles on the virtual desktop to avoid inconsistencies between profiles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consider that you are using roaming user profiles in your environment. In this case, ensure that the Enhanced Desktop Experience feature is enabled or disabled for all virtual desktops that share a profile.

Citrix does not recommend sharing roaming profiles between virtual desktops running server operating systems and client operating systems. Profiles for client and server operating systems differ. Sharing roaming profiles across both types can lead to inconsistencies in profile properties when a user moves between the two.

File Redirection policy settings

September 6, 2025

The **File Redirection** section includes policy settings relating to client drive mapping and client drive optimization.

Auto connect client drives

This setting allows or prevents automatic connection of client drives when users log on.

By default, automatic connection is allowed.

When adding this setting to a policy, ensure to enable the settings for the drive types you want automatically connected. For example, to allow automatic connection of users' CD-ROM drives, configure this setting and the **Client optical drives** setting.

The following policy settings are related:

- **Client drive redirection**
- **Client floppy drives**
- **Client optical drives**
- **Client fixed drives**
- **Client network drives**
- **Client removable drives**

Client drive redirection

This setting enables or disables file redirection to and from drives on the user device.

By default, file redirection is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Client drive redirection policy settings do not apply to drives mapped to sessions using generic USB redirection.

When enabled, users can save files to all their client drives. When disabled, all file redirection is prevented. This configuration is applicable regardless of the state of the individual file redirection settings. The individual file redirection settings include Client floppy drives and Client network drives.

The following policy settings are related:

- **Client floppy drives**
- **Client optical drives**
- **Client fixed drives**
- **Client network drives**
- **Client removable drives**

Client fixed drives

This setting allows or prevents users from accessing or saving files to fixed drives on the user device.

By default, accessing client-fixed drives is allowed.

When adding this setting to a policy, ensure that the **Client drive redirection** setting is present and set to Allowed. If these settings are disabled, client-fixed drives are not mapped and users cannot access these drives manually, regardless of the state of the **Client fixed drives** setting.

Configure the **Auto connect client drives** setting to ensure that fixed drives are automatically connected when users log on.

Client floppy drives

This setting allows or prevents users from accessing or saving files to floppy drives on the user device.

By default, accessing client-floppy drives is allowed.

When adding this setting to a policy, ensure that the **Client drive redirection** setting is present and set to Allowed. If these settings are disabled, client-floppy drives are not mapped and users cannot access these drives manually, regardless of the state of the **Client floppy drives** setting.

To ensure that floppy drives are automatically connected when users log on, configure the **Auto connect client drives** setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client network drives

This setting allows or prevents users from accessing and saving files to network (remote) drives through the user device.

By default, accessing client network drives is allowed.

When adding this setting to a policy, ensure that the **Client drive redirection** setting is present and set to Allowed. If these settings are disabled, client network drives are not mapped and users cannot access these drives manually. This configuration is applicable regardless of the state of the **Client network drives** setting.

To ensure that network drives are automatically connected when users log on, configure the **Auto connect client drives** setting.

Client optical drives

This setting allows or prevents users from accessing or saving files to the following:

- CD-ROM on the user device
- DVD-ROM on the user device
- BD-ROM drives on the user device.

By default, accessing client-optical drives is allowed.

When adding this setting to a policy, ensure that the **Client drive redirection** setting is present and set to **Allowed**. If these settings are disabled, client-optical drives aren't mapped and users can't access these drives manually. This configuration is applicable regardless of the state of the **Client optical drives** setting.

To ensure that optical drives are automatically connected when users log on, configure the **Auto connect client drives** setting.

Client removable drives

This setting allows or prevents users from accessing or saving files to USB drives on the user device.

By default, accessing client-removable drives is allowed.

When adding this setting to a policy, verify that the **Client drive redirection** setting is present and set to Allowed. If these settings are disabled, client-removable drives are not mapped and users cannot access these drives manually. This configuration is applicable regardless of the state of the **Client removable drives** setting.

Configure the **Auto connect client drives** setting to ensure that removable drives are automatically connected when users log on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Host to client redirection

This setting enables or disables file type associations for URLs and some media content to be opened on the user device. When disabled, content opens on the server.

By default, file type association is disabled.

These URL types are opened locally when you enable this setting:

- HTTP
- HTTPS
- Real Player and QuickTime (RTSP)
- Real Player and QuickTime (RTSPU)
- Legacy Real Player (PNM)
- Microsoft Media Server (MMS)

Preserve client drive letters

This setting enables or disables mapping of client drives to the same drive letter in the session.

By default, client drive letters are not preserved.

When adding this setting to a policy, ensure that the **Client drive redirection** setting is present and set to Allowed.

Read-only client drive access

This setting allows or prevents users and applications from the following:

- Creating files on mapped client drives
- Changing files on mapped client drives
- Changing folders on mapped client drives

By default, files and folders on mapped client drives can be changed.

If set to Enabled, files and folders are accessible with read-only permissions.

When adding this setting to a policy, ensure the **Client drive redirection** setting is present and set to Allowed.

Special folder redirection

This setting allows or prevents Citrix Workspace™ app and Web Interface users to see their local Documents and Desktop special folders from a session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, special folder redirection is allowed.

This setting prevents any objects filtered through a policy from having special folder redirection, regardless of settings that exist elsewhere. When this setting is prohibited, any related settings specified for StoreFront™, Web Interface, or Citrix Workspace app are ignored.

To define which users can have special folder redirection, select **Allowed** and include this setting in a policy filtered on the users you want to have this feature. This setting overrides all other special folder redirection settings.

Policy settings that prevent users from accessing or saving files to their local hard drives also prevent special folder redirection from working. This situation occurs because special folder redirection must interact with the user device.

When adding this setting to a policy, ensure that the **Client fixed drives** setting is present and set to Allowed.

File transfer policies

By default, file transfer is enabled. Use Web Studio to change these policies, located under **User setting - ICA\File Redirection**. Consider the following when using file transfer policies:

- **File transfer for Citrix Workspace app for Chrome OS/HTML5** - Allows or prevents users from transferring files between a Citrix Virtual Apps and Desktops session and their devices.
- **Upload file for Citrix Workspace app for Chrome OS/HTML5** - Allows or prevents users from uploading files from their device to a Citrix Virtual Apps and Desktops session.
- **Download file for Citrix Workspace app for Chrome OS/HTML5** - Allows or prevents users from downloading files from a Citrix Virtual Apps and Desktops session to their device.

> **Note:**
>
> The file transfer policies are applicable only for Citrix Workspace app for HTML5 and for Citrix Workspace app for Chrome OS.

Use asynchronous writes

This setting enables or disables asynchronous disk writes.

By default, asynchronous writes are disabled.

Asynchronous disk writes can improve the speed of file transfers and writing to client disks over WANs, which relatively high bandwidth and high latency typically characterize. However, if there is a connection or disk fault, the client file or files being written might end in an undefined state. If this undefined

© 1997–2026 Citrix Systems, Inc. All rights reserved.

state occurs, a pop-up window informs the user of the files affected. The user can then take remedial action such as restarting an interrupted file transfer on reconnection or when the disk fault is corrected.

Citrix® recommends enabling asynchronous disk writes only for users requiring remote connectivity having good file access speed. And who can easily recover files or data lost if there is a connection or disk failure.

When adding this setting to a policy, verify that the **Client drive redirection** setting is present and set to Allowed. If this setting is disabled, asynchronous writes don't occur.

Overview

September 13, 2025

Clipboard redirection is a fundamental feature in Citrix Virtual Apps and Desktops™, enabling seamless copy and paste of data between the user's local endpoint and their virtual Citrix sessions.

Clipboard redirection allows users to copy and paste data, such as text, images, and files, between applications running on their local device and those within their Citrix session. This is achieved by mapping the clipboard on the user device to the clipboard on the VDA. By default, clipboard redirection is allowed.

Clipboard redirection works over a separate virtual channel within the HDX™ protocol. An additional virtual channel is used for file transfer and Drag and Drop. When a user copies data on their local device, the Citrix Workspace™ app intercepts the data and makes it available for pasting into applications running in the session. Actual data will be transferred if and when the data is pasted to an application on the VDA. The process works in reverse when copying from the Citrix session to the client.

This combination of client to session and session to client clipboard redirection is also known as bidirectional clipboard redirection.

> **Note:**
>
> More information see, Citrix Virtual Channels

Key concepts

Client to session, also referred to as Endpoint to Session or client to VDA. Data copied (placed on the clipboard) on the user's local device is made available to be pasted inside the virtual session.

Session to Client, also referred to as Session to Endpoint or VDA to client). Data copied from an application within the virtual session is made available to be pasted on the user's local device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cross session (session to session or VDA to VDA). A new clipboard transfer method where data copied from one Citris session can be pasted into another Citrix session without ever being stored on the local endpoint's clipboard. This functionality is available on Citrix Virtual Apps and Desktops version 2507 as a Preview feature and is referred to as the Cross-session clipboard exchange feature. See 'Cross session clipboard'for more information.

Configuration

September 6, 2025

Clipboard redirection is controlled through Citrix® policies. These policies offer a range of settings to fine-tune the clipboard redirection behavior.

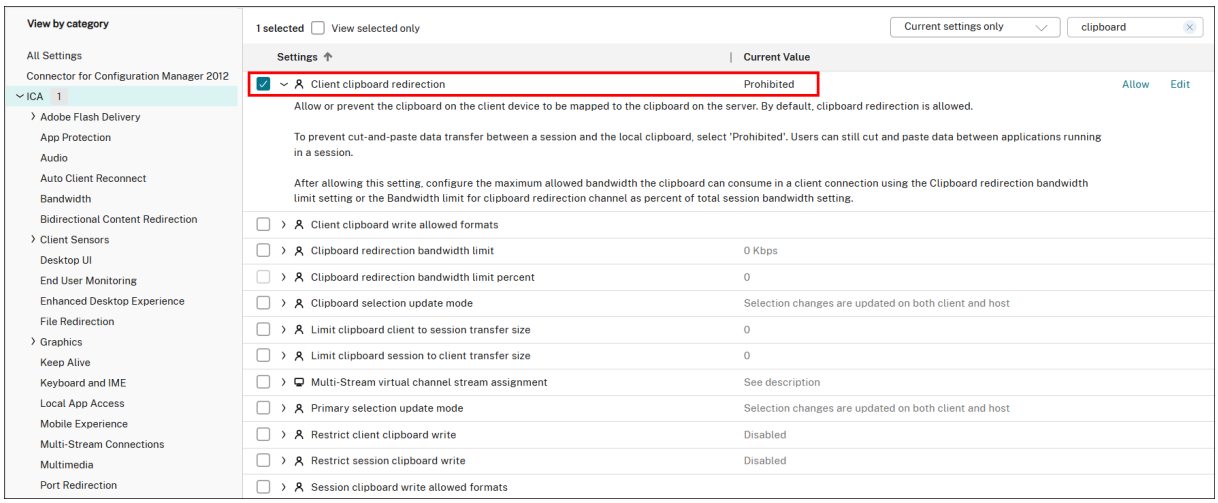
By default, bidirectional clipboard redirection is enabled: users can copy and paste data from their Citrix session to their local endpoint and vice versa.

Core Setting

The core clipboard redirection configuration is the 'Client clipboard redirection policy'. This policy controls whether clipboard redirection is allowed. By default, clipboard redirection is allowed.

Disabling clipboard redirection can improve security by preventing accidental or malicious transfer of sensitive data outside the Citrix virtual environment. It also helps in preventing the introduction of potentially harmful data into the Citrix environment via the clipboard. However, this may negatively affect the end-user experience.

To prohibit clipboard redirection, set the 'Client clipboard redirection policy'to 'prohibited':



© 1997–2026 Citrix Systems, Inc. All rights reserved.

If set to Prohibited, clipboard redirection is disabled entirely and all other clipboard-related policies are ignored.

Users can still copy and paste data between applications running inside their Citrix sessions and on their local endpoint device; however, copying and pasting from and to their Citrix session is not available.

Directional clipboard control

With directional clipboard control, admins have granular control over the direction of clipboard data flow. This is also known as unidirectional clipboard control.

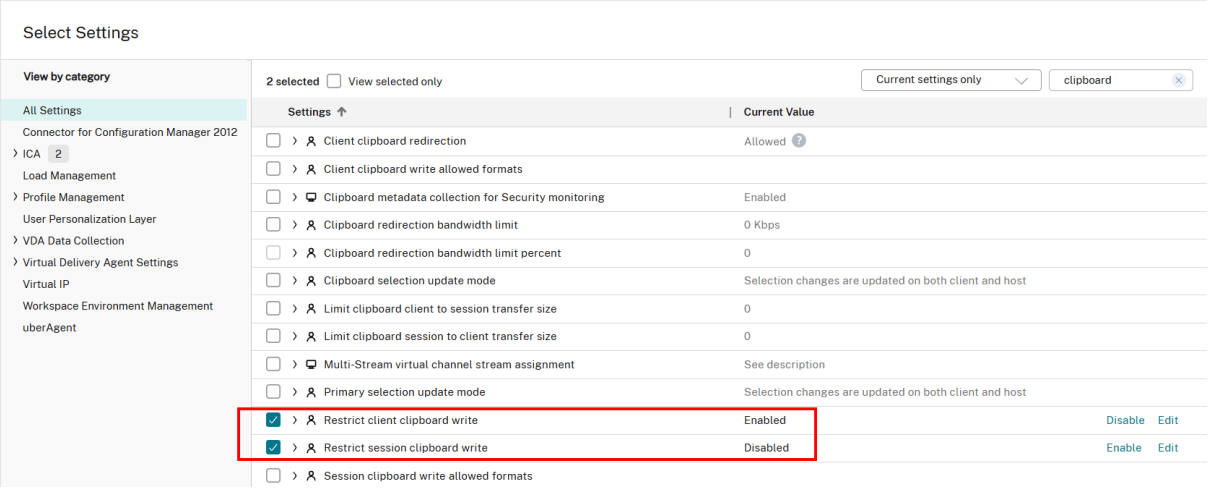
There are two primary modes of unidirectional control available:

- **Client-to-session:** In this configuration, the 'Restrict client clipboard write' policy is used, and clipboard data is permitted to flow exclusively from the user's endpoint device (client) to the remote Citrix session. This means that users can copy information from their local machine and paste it into applications running within the Citrix session, but they cannot copy data from the Citrix session and paste it back to their local machine. This mode is beneficial for scenarios where data leakage from the secure session to the less-controlled endpoint is a significant concern.
- **Session-to-client:** In this configuration, the 'Restrict session clipboard write policy' allows clipboard data to flow exclusively from the Citrix session to the client device. Users can copy information from applications within the remote session and paste it onto their local machine, but they are prevented from copying data from their local machine and pasting it into the Citrix session. This setting is often used when the primary goal is to prevent the introduction of potentially malicious or unauthorized data from the endpoint into the secure Citrix environment.

The following table describes the Citrix clipboard policies for unidirectional clipboard control:

Clipboard Directionality	Clipboard Policies
Bidirectional - Session to Client and Client to Session	Client clipboard redirection: Enabled (Default)
Unidirectional - Client to Session only	Client clipboard redirection: Enabled (Default) Restrict client clipboard write: Enabled
Unidirectional - Session to Client only	Client clipboard redirection: Enabled (Default) Restrict session clipboard write: Enabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In the example above, both directional clipboard policies are highlighted, and in this configuration, only client-to-session clipboard redirection is permitted because the 'Restrict client clipboard write' setting is set to 'Enabled'.

Clipboard Format control

August 19, 2025

Citrix Clipboard format control policies enhance clipboard security by limiting data transfer to specific clipboard formats, thereby controlling the types of data that can be copied and pasted between session and client and vice versa. It can be used to selectively allow or deny certain clipboard data formats.

Clipboard exchange formats are used to enable seamless transfer of information between diverse applications, ranging from multimedia programs to complex spreadsheets and word processors. These formats define the structure and encoding of data that can be copied, cut, and pasted, allowing applications to understand and process the content exchanged.

For instance, when copying text from a web browser and pasting it into a word document, the clipboard employs a text-based format. However, if the copied content includes images, tables, or rich text formatting, the clipboard will utilize more sophisticated formats like RTF (Rich Text Format) or HTML (HyperText Markup Language) to preserve the original appearance and structure. Similarly, when exchanging data between specialized applications, such as a CAD program and a presentation tool, the clipboard might use application-specific formats or common metafile formats to ensure accurate representation of the graphical or complex data.

The clipboard format control policies are designed to work in conjunction with the directional clipboard control policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With Clipboard Format control, admins can which formats are allowed for example:

- Allow plain text only in both directions
- Allow session to client clipboard transfer only for plain text and images

Or a combination where you can limit the formats that can be pasted from the client to the session, but allow all formats to be pasted from the session back to the client.

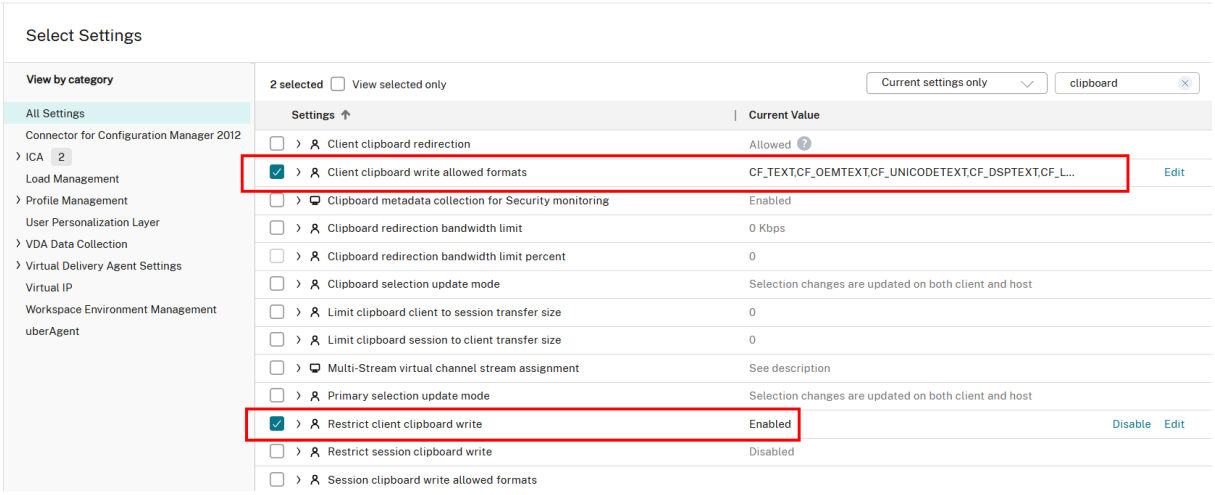
Two primary policies control the behavior of clipboard formats:

Client Clipboard Write Allowed Formats: This policy dictates explicitly which clipboard data formats are permitted to be written from the remote session to the client clipboard. For example, an administrator might configure this policy to allow only plain text to be copied to the client, preventing the transfer of potentially malicious rich text, images, or files.

Session Clipboard Write Allowed Formats: Secondly, this policy specifies which clipboard data formats are allowed to be copied from the client to the remote session. This policy is vital for controlling what kind of information can be transferred into the remote environment. An organization might restrict this to only allow plain text, preventing users from inadvertently or intentionally pasting sensitive files or images from their local machine into a less secure or unauthorized remote application.

> **Note:**
>
> The Clipboard allowed formats are only evaluated if the corresponding unidirectional clipboard policy is also set.

To restrict the client clipboard write formats to accept only text-based data formats, both the 'Restrict client clipboard write' policy AND 'Client Clipboard Write Allowed Formats' need to be configured. In this example, 'Restrict client clipboard write' needs to be set to **Enabled**, and the 'Client Clipboard Write Allowed Formats' needs to contain all clipboard text formats:



To configure the write format restriction, please edit the corresponding policy and ensure each entry is placed on a separate line.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

As an example:

CF_TEXT
CF_BITMAP

Is correct, however the following is incorrect:

CF_TEXT,CF_BITMAP

Standard clipboard data formats

September 6, 2025

The table below describes the standard clipboard formats.

Clipboard Format	Type	Description
CF_TEXT	Text format	Text in the standard ANSI character set. Each line ends with a carriage return/linefeed (CR-LF) combination.
CF_OEMTEXT	Text format	Text using the Original Equipment Manufacturer (OEM) character set. Similar to CF_TEXT.
CF_UNICODETEXT	Text format	Text in Unicode format. It does not require a null terminator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Clipboard Format	Type	Description
CF_LOCALE	Text format	A handle to the locale identifier associated with clipboard text. This helps in correctly interpreting the text's language and regional settings.
CF_HTML*	Text format	Represents HTML-formatted text, allowing for rich text, links, and images to be copied and pasted between applications that support it.
CF_BITMAP	Image Format	A device-dependent bitmap. The image data is specific to a particular output device.
CF_DIB	Image Format	A Device-Independent Bitmap. This format contains color information and dimensions, allowing it to be displayed correctly on any device.
CF_DIBV5	Image Format	An extension of CF_DIB (Device-Independent Bitmap, Version 5) that includes more advanced features like color profiles and alpha channels for transparency.
CF_PALETTE	Image Format	A handle to a color palette. It's used by applications to control the colors of other clipboard data, typically a bitmap.
CF_TIFF	Image Format	Tagged Image File Format. A common, high-quality image format used in publishing and photography.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Clipboard Format	Type	Description
CF_METAFILEPIC	Metafile format	A handle to a metafile picture structure. This is an older format for storing a collection of GDI (Graphics Device Interface) functions to recreate an image
CF_ENHMETAFILE**		A handle to an enhanced metafile. This is a more modern and robust version of CF_METAFILEPICT, offering better image quality and device independence.

Note:

- HTML format is disabled by default. Enabling HTML format clipboard support can introduce a security risk. When content is copied from a web page, any embedded scripts are also copied. If this content is then pasted into an application that renders HTML, the scripts could be executed. Use caution when enabling this format.
- Enhanced metafile clipboard transfer is not available on Citrix Virtual Apps and Desktops™ version prior to 2511.
  Besides these standard formats, Citrix® also supports the following specific clipboard data formats like Data Exchange Formats and specialized formats.

Data Exchange formats

September 6, 2025

Clipboard data exchange formats facilitate the transfer of data between various applications, such as multimedia programs or spreadsheets.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Clipboard Format	Description
CF_SYLK	Symbolic Link format. An older format created by Microsoft for exchanging data between spreadsheet applications like Microsoft Excel.
CF_DIF	Data Interchange Format. A text-based format for exchanging data between spreadsheet programs.
CF_RIFF	Resource Interchange File Format. A container format for storing multimedia data, such as audio and video.
CF_WAVE	Waveform audio format. Represents audio data.

Special & System Formats

August 19, 2025

These formats serve specialized purposes, such as handling file drops, private data, or custom rendering.

Clipboard Format	Description
CF_HDROP	A handle to a list of dropped files. This is used for drag-and-drop operations from the file system (e.g., dropping files into an application window).
CF_PENDATA	Represents data from a pen or stylus, used in pen computing applications.
CF_OWNERDISPLAY	A format where the original window that placed data on the clipboard is responsible for drawing and updating the content in the clipboard viewer.

CF_DSPTEXT, CF_DSPBITMAP, CF_DSPMETAFILEPICT, CF_DISPENHMETAFILE are "display"formats that correspond to standard formats (TEXT, BITMAP, etc.) but are used for private data that can be rendered within the clipboard viewer application. They are intended for application-specific use.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Apps and Desktops™ clipboard formats

September 13, 2025

CFX clipboard formats are customized Citrix Virtual Apps and Desktops clipboard formats. These are highly optimized compared to the regular clipboard formats.

Clipboard Format	Description
CFX_RICHTEXT	Used to efficiently transfer formatted text—including different fonts, sizes, colors, and styles like bold or italic
CFX_OfficeDrawingShape	Handles Microsoft Office drawing objects. It allows users to copy and paste vector shapes, diagrams, and other graphics created within Office applications (like Word, Excel, or PowerPoint)
CFX_BIFF8	This corresponds to the BIFF8 (Binary Interchange File Format 8), which is the native file format for Microsoft Excel 97-2003. CFX_BIFF8 is the Citrix-optimized version for copying and pasting data and formulas between Excel spreadsheets.
CFX_FILE*	Used for file object transfers. When you copy a file on your local computer and paste it into a virtual desktop (or vice-versa), this format manages the data transfer. It's an optimized alternative to the standard CF_HDROP format

> **Note:**
>
> To allow file copy and paste and drag and drop, you must explicitly add CFX_FILE to the allowed formats.

Custom Clipboard Format

August 19, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Besides these clipboard formats, you can also configure additional custom clipboard formats. This is only applicable to those formats which are registered with the operating system on the VDA.

For more information, see custom registered clipboard formats.

Convertible clipboard formats

September 6, 2025

Microsoft Windows natively supports different clipboard formats. When copying and pasting clipboard content, Windows will automatically attempt to convert the clipboard data to other compatible clipboard formats, making it easier to paste the content into different applications.

When data formats are posted to the clipboard, Windows will automatically add additional formats that can be obtained by converting from any of the formats that were originally posted in order to increase the likelihood of successful pasting into other applications.

Windows will then automatically convert the clipboard data from one format to another if the target application requests a format that the source cannot directly provide.

For example, when copying formatted text from a Word processor, Windows will make other formats available to a requesting application, such as plain text as well as the originally posted formatted text.

As another example, if the clipboard data contains plain text data in the CF_TEXT clipboard format and the application that the data is pasted into requests Unicode text in the format of CF_UNICODETEXT, Windows will automatically convert the clipboard data during the pasting process.

> **Note:**
>
> With some conversion, information might be lost, for example with automatically converting rich text to plain text.

Clipboard Format	Description
CF_TEXT	CF_TEXT CF_OEMTEXT CF_UNICODETEXT CF_LOCALE
CF_BITMAP	CF_BITMAP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Clipboard Format	Description
	CF_DIB
	CF_DIBV5
CF_METAFILEPICT	CF_METAFILEPICT
	CF_ENHMETAFILE
CF_OEMTEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_DIB	CF_BITMAP
	CF_DIB
	CF_DIBV5
CF_UNICODETEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_ENHMETAFILE	CF_METAFILEPICT
	CF_ENHMETAFILE
CF_DIBV5	CF_BITMAP
	CF_DIB
	CF_DIBV5

> **Note:**
>
> The clipboard format conversion is Windows OS dependent and this table could change in future OS versions.

It's important to understand that the Windows clipboard system doesn't convert between all formats freely. Automatic conversions, are limited to a few core types, primarily between different text encodings and between bitmap variations.

For most other formats, compatibility is achieved when the source application places multiple formats onto the clipboard at once. For example, when you copy a chart from Excel, it might place the data as an Office Drawing Shape (CFX_OfficeDrawingShape), an Enhanced Metafile (CF_ENHMETAFILE), and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a simple Bitmap (CF_DIB). This isn't a conversion by the clipboard, but rather the source application providing multiple representations for different pasting scenarios.

Clipboard Format control & convertible formats

Convertible formats should be taken into consideration when designing the clipboard format control policies and the cross session clipboard configuration. For example, if you want to explicitly allow only text-based content to be copied from the client to the clipboard, you must add all text-based formats to the "Session Clipboard Write Allowed Formats"policy. In this example, you must add the following formats to the policy:

CF_TEXT

CF_UNICODETEXT

CF_DSPTEXT

CF_LOCALE

CF_OEMTEXT

Likewise, if you want to funnel all file formats through cross session when copying those types of data from one session to another, you will need to add all the file clipboard formats to the CrossSession-Formats configuration:

CFX_FILES

CFX_HFDROP

Clipboard transfer size limits

September 6, 2025

With Clipboard transfer size limits you can set limits on the size of data that can be transferred in a single copy-and-paste clipboard operation. By default, these settings are disabled and there's no limit on client to session and session to client clipboard transfers.

Transfer size limits can help in bandwidth management. Large clipboard transfers can consume significant network bandwidth, especially in environments with many concurrent users. By setting limits, administrators can ensure smoother performance for all users and prevent network congestion.

Unrestricted clipboard transfers can potentially pose a security risk. Malicious software or unauthorized users could potentially copy large amounts of sensitive data in or out of the session. Limiting transfer sizes acts as a preventative measure against such data breaches.

When configuring clipboard transfer size limits, administrators should consider:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

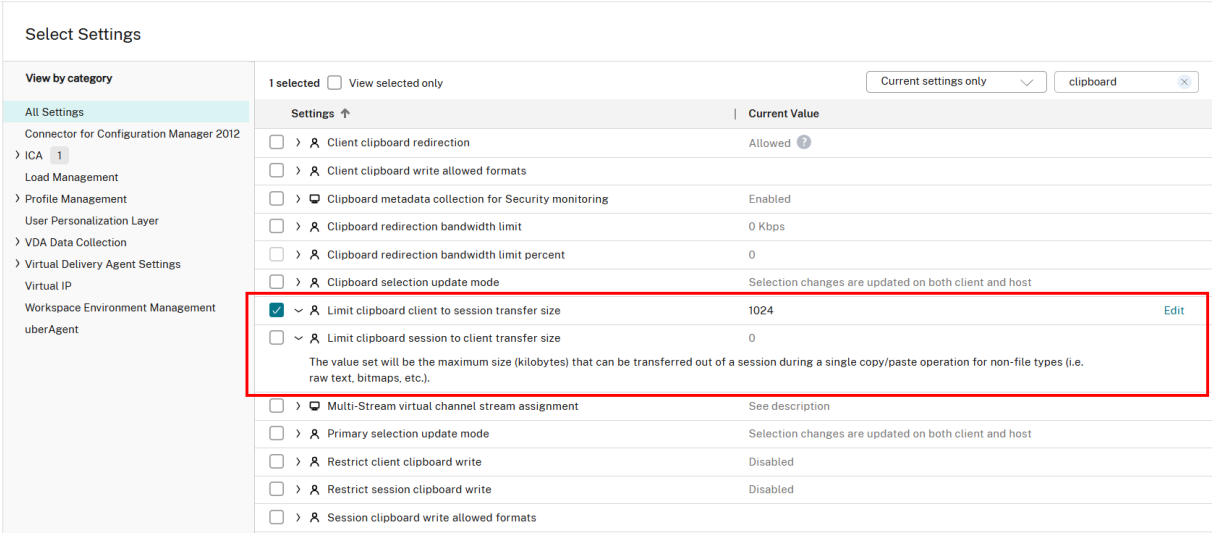
- User Needs: What are the typical copy-and-paste requirements of the users? Imposing overly restrictive limits can hinder productivity.
- Bandwidth usage: What is the available network bandwidth, and how many concurrent users are expected?
- Relevant Security policies: What are the organization's data security and compliance requirements?

Two primary settings provide granular control over clipboard data transfer:

Limit clipboard client to session transfer size: This setting configures the maximum size of data, in kilobytes, that can be copied from the user's local device (the client) and pasted into the remote session (e.g., a virtual desktop or seamless application).

Limit clipboard session to client transfer size: Secondly, this setting controls the maximum size of data, in kilobytes, that can be copied from within the remote session and pasted back to the user's local device. This is particularly relevant when users are working with sensitive data within the virtualized environment and need to prevent large data exfiltrations to the client.

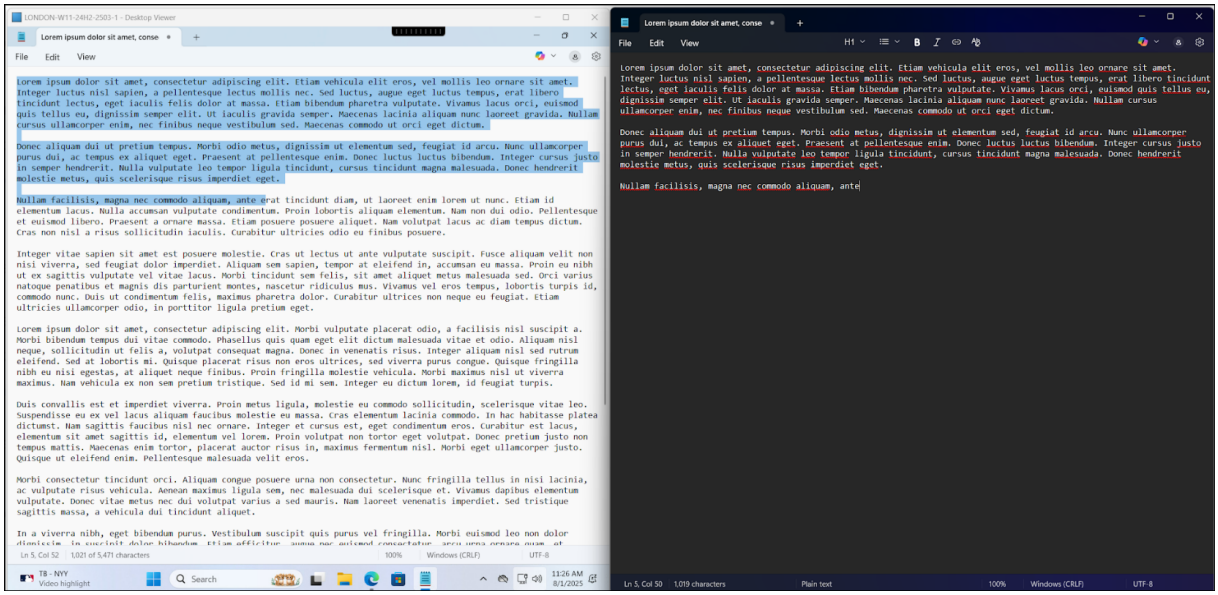
In this example, the client to session clipboard limit was restricted to 1024 kilobytes:



> **Note:**
>
> The size limit is based on data size (in kilobytes, KB), not a fixed character count. Due to variable character encodings (like for example, Unicode), the number of characters that can be copied will vary. For example, a 10 KB limit will hold fewer characters for Unicode text than for standard ANSI text.

In the following example, the 'Limit clipboard session to client transfer size'policy has been set to 1 KB.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



With this clipboard transfer size limit in place, the selected text is the maximum number of characters that can be transferred from the Citrix® session on the left to the local Notepad on the right. If a user were to attempt to copy more characters from this Citrix session to his client, the text would not be truncated, but instead the entire paste operation would fail. Attempting to copy other data types, such as images or files will also fail if the content is larger than the maximum configured transfer size.

When setting this policy, consider the type of text data your users handle. If they frequently work with multilingual content or rich text, you may need to set a higher kilobyte limit to accommodate the larger data size of Unicode text.

The clipboard transfer size limits will be applied to **all allowed clipboard formats**.

Clipboard size limits are universally enforced across all permitted clipboard formats. This means that the limit determines the maximum amount of data that can be transferred, regardless of data type (e.g., text, images, files).

Cross session Clipboard Exchange (Preview)

September 6, 2025

Cross session clipboard exchange is a new data loss prevention and mitigating control for clipboard. It enables clipboard data to be shared between Citrix® sessions without placing the data on the local endpoint's clipboard.

Cross session clipboard exchange works in conjunction with the current clipboard polices to provide a more secure method of sharing clipboard data between VDA and client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature is currently in Preview.

When users place data on the VDA's clipboard, the clipboard data is automatically shared with the endpoint when the 'Client clipboard redirection policy' clipboard policy is enabled. This enables users to copy and paste data from their remote session to their client.

Users may have access to multiple remote sessions and applications from multiple sources and can share data between these sessions via the clipboard. In this case, the clipboard data will also be available on the local endpoints' clipboard by default.

In environments that handle sensitive data, customers may choose to prohibit sharing of clipboard data from the remote session to the client clipboard; however, this will also limit the clipboard functionality between Citrix sessions.

Cross-session clipboard exchange will allow for the clipboard transfer between Citrix sessions (both seamless sessions as well as Desktop sessions) that could be published on different servers and/or sessions while preventing the clipboard data from flowing through the local endpoints clipboard and thereby preventing data exfiltration risks and accidental data loss while improving user experience.

Requirements

The prerequisites for the cross session clipboard exchange Preview are as follows:

- Windows endpoint running CWA for Windows 2507 LTSR later;
- Windows VDA running VDA 2507 LTSR or later.

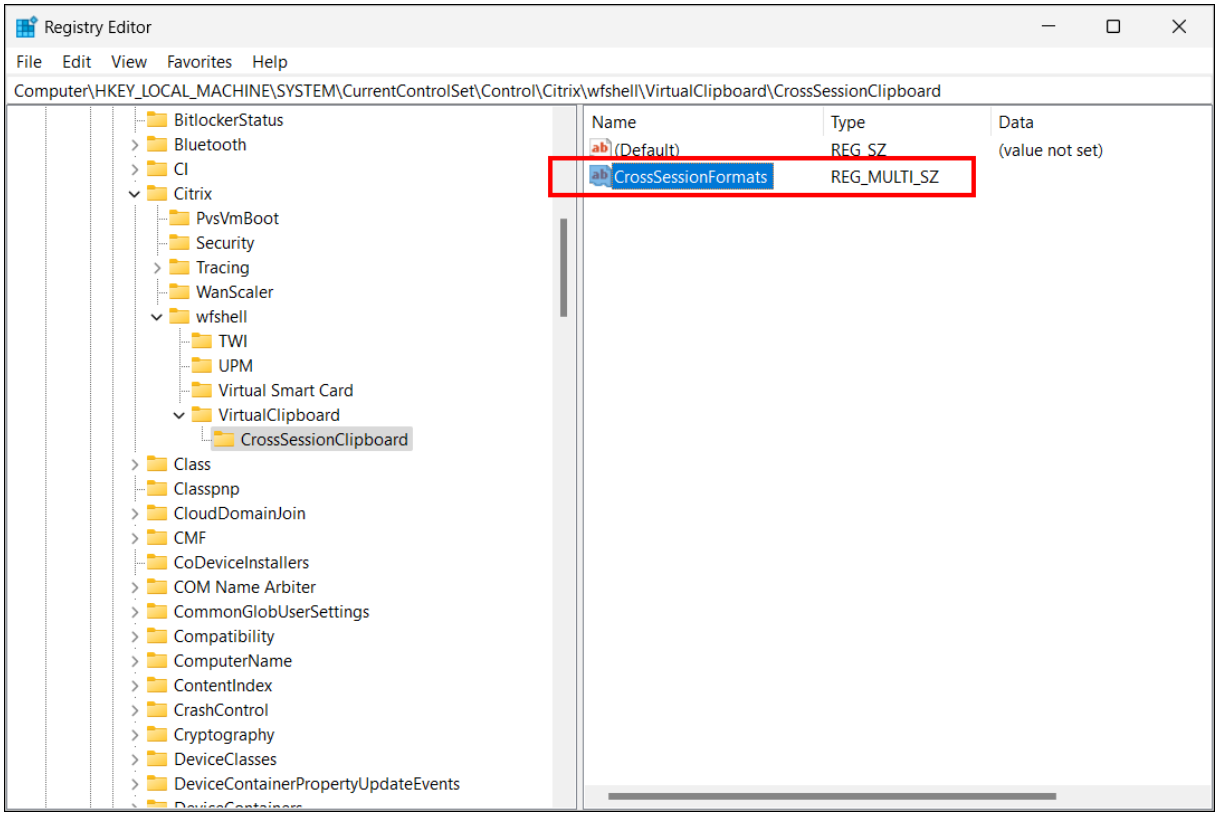
Configuration

September 6, 2025

The Cross session clipboard Preview can be enabled by creating the following registry entry on the VDA:

1. Open the Windows Registry Editor using regedit.exe.
2. Navigate to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\wfshell\Virtual Clipboard\CrossSessionClipboard\`
3. Create a REG_MULTI_SZ value named `CrossSessionFormats`

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The CrossSessionFormats can be configured with a list of clipboard formats that will be tunnelled through Cross session clipboard. Each entry must be entered on a separate line.

As an example:

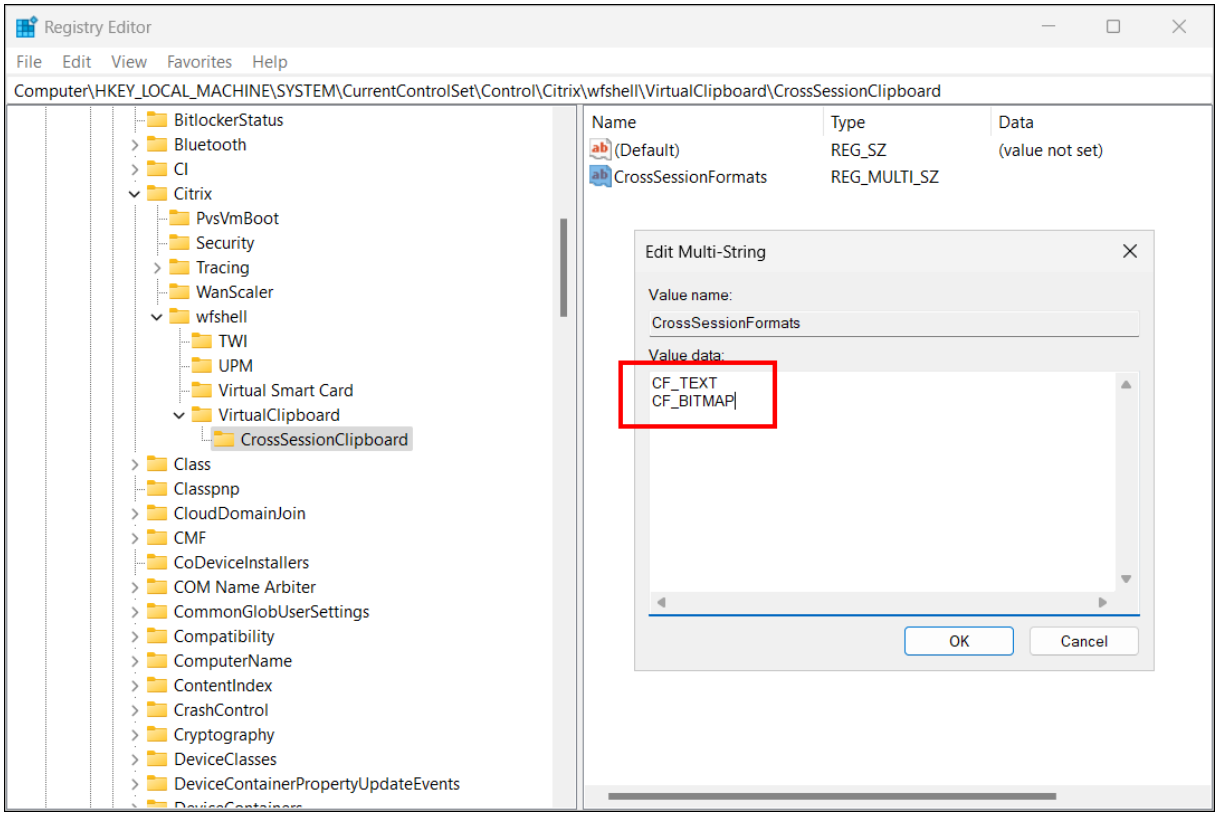
CF_TEXT

CF_BITMAP

Is correct, however the following is incorrect:
CF_TEXT,CF_BITMAP

In the following example the CF_TEXT and CF_BITMAP clipboard items will be sent tunneled through cross session when copying these data formats from one session to another:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Cross session will need to be configured with the desired clipboard data formats on all VDAs that the user will want to share clipboard data to and from in order for cross session clipboard to function.

Cross session clipboard formats that are configured will be blocked from clients that do not have cross session support (CWA client prior to CWA for Windows 2507).

Both the sending as well as the receiving Citrix® session will need to have matching clipboard data formats configured for Cross session.

Clipboard content to be copied between sessions is only allowed if the clipboard data that needs to be copied between sessions matches. If the clipboard format is not configured for cross session on the receiving VDA, the clipboard transfer will be denied and a user will not be able to paste the data in the receiving citrix session.

> **Note:**
>
> Both VDAs do not need to have all configured cross session clipboard formats to match, however only formats that appear in both CrossSessionFormats configurations will be shared between sessions.

For example i

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note:

- The Cross session configuration is for Session to session only. If configured it could change session to client behaviour based on the configuration set. Cross session clipboard will not change client to session clipboard. Client to session configuration is done solely through the client to session related clipboard policies.
- If a user is connecting to Citrix sessions that are configured for Cross session clipboard, but their client does not support cross session (e.g. using a Citrix Workspace App version prior to 2507, or connecting from an unsupported CWA like CWA Linux), clipboard transfer of those formats listed in the cross session configuration, from the Citrix session to the client will be denied.

Policy and registry priority

September 6, 2025

The cross session clipboard exchange registry configuration works in conjunction with the clipboard policies.

If clipboard redirection is explicitly prohibited through policy by setting the 'client clipboard redirection' policy to prohibit, the Cross session clipboard registry configuration will be ignored and clipboard transfer between Citrix® sessions will also be prohibited, no matter how the registry is configured.

If a clipboard data format is explicitly prohibited by the 'xxx' policy setting, but the clipboard data format is enabled for cross session, the clipboard format will be prohibited. The configuration in the cross session registry will be ignored.

Clipboard size limitations will also be enforced for clipboard data that is shared through cross session clipboard exchange between sessions.

Examples

Example 1

Everything default

Except:

- Cross session configured on both VDAs for CF_TEXT, CF_UNICODETEXT, CF_DSPTEXT, CF_OEMTEXT, CF_LOCALE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The data formats that are configured in the Cross session clipboard exchange registry configuration will be tunneled through cross session and will not be available on the client, in this case text formats will be allowed to be shared from the source VDA to the receiving VDA. All other formats allowed by policy will still be allowed onto the Client and onto the remote sessions. Only the Text-Formats will be prohibited on the client clipboard when copied from remote sessions.

Clipboard data transfer from client to session is not restricted.

Example 2

Everything default

Except:

- Restrict session clipboard write: Enabled configured on both VDAs
- Cross session configured on both VDAs for CF_TEXT

Clipboard data will not be shared between sessions because 'Restrict session clipboard write'is enabled on both VDAs. This setting takes precedence over the cross session configuration.

Clipboard data transfer from client to session will be also prohibited by that same policy.

Because CF_TEXT is configured for cross session, this also means that CF_TEXT will not be copyable from the VDA to the client as it is blocked due to the cross session configuration.

All other clipboard formats will be available from session to client.

Example 3

Everything default

Except:

- Session Clipboard Write Allowed Formats is limited to CF_TEXT on both VDAs
- Cross session is configured on both VDAs for all clipboard data formats

The Session clipboard Write Allowed Formats takes precedence over the cross session clipboard configuration and only CF_TEXT data is allowed to be copied to the receiving VDA through the clipboard

All clipboard formats listed in cross session will be prevented from being copied to the client clipboard.

Example 4

Everything default

Except:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Session Clipboard Write Allowed Formats is set to everything but CF_TEXT
- Cross session is configured on both VDAs for CF_TEXT

The Session clipboard Write Allowed Formats takes precedence over the cross session clipboard configuration and CF_TEXT data will not be allowed to be shared over the clipboard between VDAs

Scenarios and use case examples

September 6, 2025

Properly configuring clipboard redirection policies is key to balancing user productivity and corporate security. The optimal configuration depends on the specific use cases.

The following are some common use case examples:

Standard knowledge worker

For most users like knowledge workers and the typical office users, the goal is seamless copy-paste of text and simple images between local and remote applications. In this scenario, the default policy configuration is often sufficient.

Configuration:

- Client clipboard redirection: **Allowed** (Default)

Sensitive data use cases

Consider a healthcare or financial institution where users need to paste information into a secure session (e.g., patient data into an EHR) but must be prevented from copying sensitive data out to their local device. This can help prevent accidental data exfiltration via the clipboard:

Configuration:

- Client clipboard redirection: **Allowed**
- Restrict client clipboard write: **Enabled** (Blocks copy from session to client)
- For added security, enable Restrict session clipboard write and use Session clipboard write allowed formats to only permit plain text (CF_TEXT).

Alternatively, customers can use the new Cross session clipboard functionality (PREVIEW) to allow clipboard session-to-session while preventing session-to-client redirection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Developers and IT Administrators

These users often require the ability to copy files, such as scripts, log files, or installers, between their local machine and the VDA. This requires a more permissive configuration.

Configuration:

- Client clipboard redirection: **Allowed**
- To enable file copy from session to client, ensure Restrict client clipboard write is **Disabled**, or if enabled, add the CFX_FILE format to the Client clipboard write allowed formats list.
- To enable file copy from client to session, ensure Restrict session clipboard write is **Disabled**, or if enabled, add CFX_FILE to the Session clipboard write allowed formats list.

Configure these policies to target the relevant groups containing the developer or IT Admins instead of individually adding users to the policy.

Graphics policy settings

September 13, 2025

The **Graphics** section includes policy settings for controlling how images are handled in user sessions.

Allow visually lossless compression

This setting allows visually lossless compression to be used instead of true lossless compression for graphics. Visually lossless improves performance over true lossless, but has minor loss that is unnoticeable by sight. This setting changes the way the values of the Visual quality setting are used.

By default this setting is disabled.

Graphics status indicator

This setting configures the graphics status indicator to run in the user session. This tool lets the user see information about the active graphics mode. The information includes details about video codec, hardware encoding, image quality, and monitors in use for the session. With the graphics status indicator, the user can also enable or disable pixel-perfect mode.

Releases of Citrix Virtual Apps and Desktops™ 2103 and later include an image quality slider to help the user find the right balance between image quality and interactivity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Releases of Citrix Virtual Apps and Desktops 2109 and later include functionality to configure a virtual display layout through a user interface launched using the graphics status indicator.

The graphics status indicator replaces the lossless indicator tool from previous versions. This policy enables the lossless indicator for Citrix Virtual Apps and Desktops versions 7.16 through 1809.

Screen sharing

This setting enables users to share their sessions, including screen contents, keyboards, and mice, with other users.

By default, the setting is disabled.

The VDA attempts to use ports from the TCP port range to exchange data, starting with the lowest port and incrementing on each subsequent connection. The port handles both inbound and outbound traffic.

By default, the TCP port range is set to 52525-52625.

The port used for screen sharing must be added to the firewall exception list. This option is shown as a check box when installing the VDA. By default, this option is not checked.

Display memory limit

This setting specifies the maximum video buffer size in kilobytes for the session.

For VDA versions 2308 and prior, specify an amount in kilobytes from 128 to 4,194,303. When not specified, the setting defaults to 65,536 kilobytes.

For VDA versions 2311 and later, specify any amount in kilobytes. When not specified, or when specified as 0, the setting defaults to no maximum.

> **Note:**
>
> For VDA version 2311 and later, Citrix® recommends leaving this setting at default.

Using higher resolution and multiple monitors for connections requires more memory. Always calculate the amount of video memory needed based on the upper echelon of configurations in your environment as HDX™ allocates only the amount of display memory needed for each session. So, if only some users require more than the default, there is no negative impact on scalability by increasing the display memory limit.

The required amount of video memory needed be calculated using the following formula:

Total Video Memory = ((32 / 8) x Σ [(vertical-resolution-in-pixels) x (horizontal-resolution-in-pixels)])

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example 1

In the following example we'll use a session with two monitors, one with a resolution of 1920x1080 and the other with a resolution of 1280x720.

1. Calculate the sum of the products of resolutions:
    - (1080 x 1920) + (720 x 1280)
    - = 2073600 + 921600
    - = 2995200
2. Calculate total video memory:
    - ((32 / 8) x 2995200)
    - = (4 x 2995200)
    - = 11,980,800 bytes or 11,700 Kilobytes

In this example, 11,700 kilobytes of video memory would be needed to support a session with these two monitor configurations.

Example 2

When using 4 x 4K monitors, using the formula specified above, these sessions would need a minimum of 129,600 kilobytes of video memory.

For both examples, when using VDA versions 2311 or later, Citrix recommends leaving the display memory limit at the default.

Display mode degrade preference

> **Note:**
>
> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

When the session display memory limit is reached, this setting specifies whether color depth or resolution degrades first.

By default, color depth is degraded first.

When the session memory limit is reached, you can reduce the quality of displayed images. You can reduce this quality by choosing whether color depth or resolution is degraded first. When color depth is degraded first, displayed images use fewer colors. When resolution is degraded first, displayed images use fewer pixels per inch.

To notify users when either color depth or resolution is degraded, configure the Notify user when display mode is degraded setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dynamic windows preview

This setting enables or disables the display of seamless windows in:

- Flip-
- Flip 3D
- Taskbar preview
- Windows peek

Windows Aero preview option	Description
Taskbar Preview	When the user hovers over a window's taskbar icon, an image of that window appears above the taskbar.
Windows Peek	When the user hovers over a taskbar preview image, a full-sized image of the window appears on the screen.
Flip	When the user presses ALT+TAB, small preview icons are shown for each open window.
Flip 3D	When the user presses the TAB+Windows logo key, large images of the open windows cascade across the screen.

By default, this setting is enabled.

Image caching

> **Note:**
>
> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting enables or disables the caching and retrieving of sections of images in sessions. Caching images in sections and retrieving these sections when needed makes the following:

- Scrolling smoother on the user device
- Reduces the amount of data transmitted over the network on the user device
- Reduces the processing required on the user device

By default, the image caching setting is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The image caching setting controls how images are cached and retrieved. The setting does not control whether images are cached. Images are cached if the Legacy graphics mode setting is enabled.

Legacy graphics mode - not supported. For backward compatibility only

> **Important:**
>
> We do not support legacy graphics mode and Desktop Composition Redirection (DCR) in this release. This policy is included only for backward compatibility when using XenApp 7.15 LTSR, XenDesktop 7.15 LTSR, and previous VDA releases with Windows 7 and Windows 2008 R2.

This setting disables the rich graphics experience. Use this setting to revert to the legacy graphics experience, reducing bandwidth consumption over a WAN or mobile connection. Bandwidth reductions introduced in XenApp and XenDesktop 7.13 make this mode obsolete.

By default, this setting is disabled and users are provided with the rich graphics experience.

Legacy graphics mode is supported on the following:

- Windows 7
- Windows Server 2008 R2 VDAs.

Legacy graphics mode is not supported on the following:

- Windows 8.x and 10
- Windows Server 2012, 2012 R2, and 2016.

See CTX202687 for more on optimizing graphics modes and policies in XenApp and XenDesktop 7.6 FP3 or higher.

Maximum allowed color depth

> **Note:**
>
> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting specifies the maximum color depth allowed for a session.

By default, the maximum allowed color depth is 32 bits per pixel.

This setting applies only to Thinwire drivers and connections. It does not apply to VDAs that have a non-ThinWire driver as the primary display driver. These VDAs are VDAs that use a Windows Display

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Driver Model (WDDM) driver as the primary display driver. For Single-session OS VDAs using a WDDM driver as the primary display driver, such as Windows 8, this setting has no effect. For Windows Multi-session OS VDAs using a WDDM driver, such as Windows Server 2019, this setting might prevent users from connecting to the VDA.

Setting a high color depth requires more memory. To degrade color depth when the memory limit is reached, configure the **Display mode degrade preference** setting. When color depth is degraded, displayed images use fewer colors.

Notify user when display mode is degraded

> **Note:**
>
> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting displays a brief explanation to the user when the color depth or resolution is degraded.

By default, notifying users is disabled.

Optimize for 3D graphics workload

This setting configures the appropriate default settings that best suit graphically intense workloads. Enable this setting for users whose workload focuses on graphically intense applications. Apply this policy only in cases where a GPU is available to the session. Any other settings that explicitly override the default settings set by this policy take precedence.

By default, optimize for the 3D graphics workload is disabled.

Queuing and tossing

> **Note:**
>
> For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting discards queued images that another image replaces.

By default, queuing and tossing is enabled.

This setting improves response when graphics are sent to the user device. Configuring this setting can cause animations to become choppy because of dropped frames.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use video codec for compression

Allows use of a video codec to compress graphics when video decoding is available on the endpoint. When **For the entire screen** is chosen the video codec is applied as the default codec for all. When **For actively changing regions** is selected the video codec is used for areas where there is constant change on the screen, other data uses still image compression and bitmap caching. When video decoding is not available on the endpoint, or when you specify **Do not use video codec**, a combination of still image compression and bitmap caching is used. When **Use when preferred** is selected, the system chooses, based on various factors. The results might vary between versions as the selection method is enhanced.

Select **Use when preferred** to allow the system to make its best effort to choose appropriate settings for the current scenario.

Select **For the entire screen** to optimize for improved user experience and bandwidth, especially in cases with heavy use of server-rendered video and 3D graphics.

Select **For actively changing regions** to optimize for improved video performance, especially in low bandwidth, while maintaining scalability for static and slowly changing content. This setting is supported in multi-monitor deployments.

Select **Do not use video codec** to optimize for server CPU load and for cases that do not have numerous server-rendered videos or other graphically intense applications.

The default is **Use when preferred**.

Use hardware encoding for video

This setting allows the use of graphics hardware, if available, to compress screen elements with the video codec. If such hardware is not available, the VDA falls back to CPU-based encoding using the software video codec.

The default option for this policy setting is **Enabled**.

Multiple monitors are supported.

Any Citrix Workspace™ app that supports video decoding can be used with hardware encoding.

NVIDIA

For NVIDIA GRID GPUs, hardware encoding is supported with VDAs for Multi-session OS and Single-session OS.

NVIDIA GPUs must support NVENC hardware encoding. See NVIDIA video codec SDK for a list of supported GPUs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NVIDIA GRID requires driver version 3.1 or higher. NVIDIA Quadro requires driver version 362.56 or higher. Citrix recommends drivers from the NVIDIA Release R361 branch.

Lossless text is not compatible with NVENC hardware encoding. If you enabled lossless text, lossless text takes priority over NVENC hardware encoding.

Selective use of the H.264 hardware codec for actively changing regions is supported.

Visually lossless (YUV 4:4:4) compression is supported. Visually lossless (graphics policy setting, Allow visually lossless compression) requires Citrix Workspace app 1808 or higher or Citrix Receiver for Windows 4.5 or higher.

Intel

For Intel Iris Pro graphics processors, hardware encoding is supported with VDAs for Single-session OS and Multi-session OS.

Intel Iris Pro graphics processors in the Intel Broadwell processor family and later are supported. Intel Remote Displays SDK version 1.0 is required and can be downloaded from the Intel website: Remote Displays SDK.

Lossless text is supported only when the Video codec policy is set for the entire screen and the **Optimize for 3D graphics workload** policy is disabled.

Visually lossless (YUV 4:4:4) is not supported.

The Intel encoder provides a good user experience for up to eight encoding sessions (for example one user using eight monitors or eight users using a monitor each). If more than eight encoding sessions are required, check how many monitors the virtual machine connects with. The administrator decides to configure this policy setting on a per user or per machine basis to maintain a good user experience.

AMD

For AMD, hardware encoding is supported with VDAs for a Single-session OS.

AMD GPUs must support the RapidFire SDK. For example, the AMD Radeon Pro or FirePro GPUs.

For encoding to work, install the latest AMD drivers. You can download those drivers from https://www.amd.com/en/support.

Lossless text isn't compatible with AMD hardware encoding. If you enabled lossless text, lossless text takes priority over AMD hardware encoding.

Selective use of the H.264 hardware codec for actively changing regions is supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Caching policy settings

September 6, 2025

This section includes policy settings that enable caching image data on user devices when client connections are limited in bandwidth.

Persistent cache threshold

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the **Legacy graphics mode** policy setting is enabled.

This setting caches bitmaps on the hard drive of the user device and thus enables reuse of large, frequently used images from previous sessions.

By default, the threshold is 3000000 bits per second.

The threshold value represents the point below which the Persistent Cache feature takes effect. For example, using the default value, bitmaps are cached on the hard drive of the user device when bandwidth falls below 3000000 bps.

Keep alive policy settings

September 6, 2025

The **Keep Alive** section contains policy settings for managing ICA® keep-alive messages.

ICA keep-alive timeout

This setting specifies the number of seconds between successive ICA keep-alive messages.

By default, the interval between keep-alive messages is 60 seconds.

Specify an interval between 1-3600 seconds in which to send ICA keep-alive messages. Do not configure this setting if your network monitoring software is responsible for closing inactive connections.

ICA keep-alive messages

This setting enables or disables sending ICA keep-alive messages periodically.

By default, keep-alive messages are not sent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enabling this setting prevents broken connections from being disconnected. If the server detects no activity, this setting prevents Remote Desktop Services (RDS) from disconnecting the session. The server sends keep-alive messages every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

ICA keep-alive does not work if you are using session reliability. Configure ICA keep-alive only for connections that are not using Session Reliability.

Related policy settings: Session reliability connections.

Local App Access policy settings

September 6, 2025

The **Local App Access** section includes policy settings that manage the users' locally installed applications with hosted applications. These policy settings manage integration in a hosted desktop environment.

Allow Local App Access

This setting allows or prevents the integration of users' locally installed applications with hosted applications. These policy settings manage integration in a hosted desktop environment.

When a user starts a locally installed application, that application appears to run within their virtual desktop, even though it's actually running locally.

If you set the **Allow local app access** policy setting to **Enabled**, browser content redirection isn't supported and the client-side notification area battery status does not appear in desktop sessions.

By default, **Allow Local App Access** is prohibited.

URL redirection block list

This setting specifies websites that are redirected to and started in the local Web browser. These websites might include the following:

- Websites requiring locale information, such as msn.com or newsgoogle.com
- Websites containing rich media content that are better rendered on the user device.

By default, no sites are specified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

URL redirection allow list

This setting specifies websites that are rendered in the environment in which they're started.

By default, no sites are specified.

Mobile experience policy settings

September 6, 2025

The **Mobile Experience** section includes policy settings for handling the Citrix Mobility Pack.

Automatic keyboard display

This setting enables or disables the automatic display of the keyboard on mobile device screens.

By default, the automatic display of the keyboard is disabled.

Launch touch-optimized desktop

This setting is disabled and not available for Windows 10 or Windows Server 2016 machines.

This setting determines the overall Citrix Workspace™ app interface behavior. This setting allows or prohibits a touch-friendly interface that is optimized for tablet devices.

By default, a touch-friendly interface is used.

To use only the Windows interface, set this policy setting to Prohibited.

Remote the combo box

This setting determines the types of combo boxes that you can display in sessions on mobile devices. Set this policy setting to Allowed to display the device-native combo box control. When this setting is allowed, a user can change a Citrix Workspace app for iOS session setting to use the Windows combo box.

By default, the **Remote the combo box** feature is prohibited.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multimedia policy settings

September 13, 2025

The **Multimedia** section includes policy settings for managing streaming HTML5 and Windows audio and video in user sessions.

> **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 the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Multimedia policies

By default, all multimedia policies set on the Delivery Controller™ are stored in these registries:

Machine policies:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

User policies:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

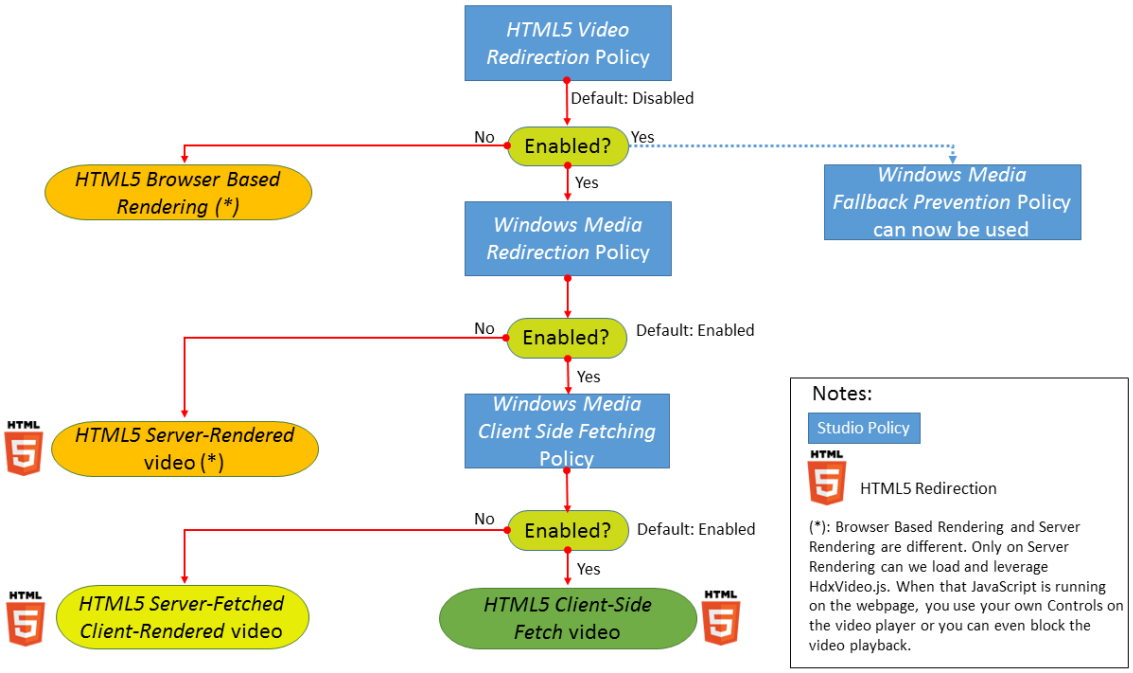
To locate the current user session ID, issue the **qwinsta** command on the Windows command line.

HTML5 video redirection

Controls and optimizes the way Citrix Virtual Apps and Desktops™ servers deliver HTML5 multimedia web content to users.

By default, this setting is disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this release, this feature is available for controlled webpages only. It requires the addition of JavaScript to the webpages where the HTML5 multimedia content is available, for example, videos on an internal training site.

To configure HTML5 video redirection:

1. Copy the file, **HdxVideo.js**, from %Program Files%/Citrix/ICA Service/HTML5 Video Redirection on the VDA install to the location of your internal webpage.
2. Insert this line into your webpage (if your webpage has other scripts, include **HdxVideo.js** before those scripts):
   ```
   <script src="HdxVideo.js"type="text/javascript"\></script>
   ```

Note: If HdxVideo.js isn't in the same location as your webpage, use the **src** attribute to specify the full path to it.

Consider that the JavaScript isn't added to your controlled webpages and the user plays an HTML5 video. In this case, Citrix Virtual Apps and Desktops default to the server-side rendering.

For redirection of HTML5 videos to work, allow ***Windows Media Redirection***. This policy is mandatory for Server Fetch Client Render, and necessary for Client Side Fetching. Client Side Fetching in turn also requires *Windows Media client-side content fetching* to be Allowed.

Microsoft Edge doesn't support this feature.

HdxVideo.js replaces the browser HTML5 Player controls with its own. To check that the HTML5 video redirection policy is in effect on a certain website, compare the player controls to a scenario where the **HTML5 video redirection** policy is Prohibited:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(Citrix custom controls when the policy is Allowed)

(Native webpage controls when the policy is Prohibited or not configured)

The following video controls are supported:

- play
- pause
- seek
- repeat
- audio
- full screen

You can view an HTML5 video redirection test page.

TLS, HTML5 video redirection, and browser content redirection

You can use HTML5 video redirection to:

- Redirect videos from HTTPS websites
- Or
- Browser content redirection to redirect the entire website

The JavaScript injected into those websites must establish a TLS connection to the Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) running on the VDA. Citrix HDX HTML5 Video Redirection Service in the certificate store on the VDA generates two custom certificates to:

- Achieve video redirection
- Maintain the TLS integrity of the webpage

HdxVideo.js uses Secure WebSockets to communicate with WebSocketService.exe running on the VDA. This process runs as a Local System account, and does SSL termination and user session mapping.

WebSocketService.exe is listening on 127.0.0.1 port 9001.

Limit video quality

This setting applies only to Windows Media and not to HTML5. It requires you enable **Optimization for Windows Media multimedia redirection over WAN**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This setting specifies the maximum video quality level allowed for an HDX™ connection. When configured, maximum video quality is limited to the specified value, ensuring that multimedia Quality of Service (QoS) is maintained within an environment.

By default, this setting isn't configured.

To limit the maximum video quality level allowed, choose one of the following options:

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

Playing multiple videos simultaneously on the same server consumes large amounts of resources and can impact server scalability.

Microsoft Teams redirection

This setting enables optimization of Microsoft Teams, based on the HDX technology.

If this policy is enabled, and you're using a supported version of Citrix Workspace™ app, this registry key is set to **1** on the VDA. The Microsoft Teams application reads the key to load in VDI mode.
Note it is not required to set the registry key manually.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Name: MSTeamsRedirSupport

Value: DWORD (1 - on, 0 - off)

> **Note:**
>
> Consider that you're using version 1906.2 VDAs or later with older versions of the Controller, which do not have the policy available in Web Studio. An example for an older version of the controller is version 7.15. In this case, HDX optimization is enabled by default on the VDA. If the Workspace app version is 1907 or later, Microsoft Teams launches in optimized mode. For information about caveats in mixing 7.15 LTSR Controllers and CR VDAs, see Knowledge Center article CTX205549.
>
> In this case, to disable the feature for specific users, you can override the registry setting. Override the registry settings by using a group policy to apply a logon script to the user's organizational unit.

By default, Microsoft Teams redirection is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multimedia conferencing

This setting allows or prevents the use of optimized webcam redirection technology by video conferencing applications.

By default, video conferencing support is allowed.

When adding this setting to a policy, verify that the **Windows Media redirection** setting is present and set to **Allowed** (the default).

When using **Multimedia conferencing**, verify that the following conditions are met:

- Manufacturer-supplied drivers for the webcam used for multimedia conferencing are installed on the client.
- Connect the webcam to the user device before starting a video conferencing session. The server uses only one installed webcam at any given time. If multiple webcams are installed on the user device, the server attempts to use each webcam in succession. This attempt continues until a video conferencing session is created successfully.

This policy isn't needed when redirecting the web cam using Generic USB redirection. In that case, install the webcam drivers on the VDA.

Optimization for Windows Media multimedia redirection over WAN

This setting applies only to Windows Media and not to HTML5. The setting enables the following:

- Real-time multimedia transcoding
- Allows audio and video media streaming to mobile devices over degraded networks
- Enhances the user experience by improving how Windows Media content is delivered over a WAN.

By default, the delivery of Windows Media content over the WAN is optimized.

When adding this setting to a policy, make sure the **Windows Media Redirection** setting is present and set to **Allowed**.

When this setting is enabled, real-time multimedia transcoding is deployed automatically as needed to enable media streaming. Also, provide a seamless user experience even in extreme network conditions.

Use GPU for optimizing Windows Media multimedia redirection over WAN

This setting applies only to Windows Media and enables real-time multimedia transcoding to be done in the Graphics Processing Unit (GPU) on the Virtual Delivery Agent (VDA). It improves server scala-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

bility. GPU transcoding is available only if the VDA has a supported GPU for hardware acceleration. Otherwise, transcoding falls back to the CPU.

Note: GPU transcoding is supported only on NVIDIA GPUs.

By default, using the GPU on the VDA to optimize the delivery of Windows Media content over the WAN is prohibited.

When adding this setting to a policy, make sure that the following settings are present and set to Allowed:

- **Windows Media redirection**
- **Optimization for Windows Media multimedia redirection over WAN settings**

Windows Media fallback prevention

This setting applies to browser content redirection, HTML5, and Windows Media. For it to support HTML5, set the **HTML5 video redirection** policy to **Allowed**.

Administrators can use the **Windows Media fallback prevention** policy setting to specify the methods that is attempted to deliver streamed content to users.

By default, this setting isn't configured. When the setting is set to Not Configured, the behavior is the same as **Play all content**.

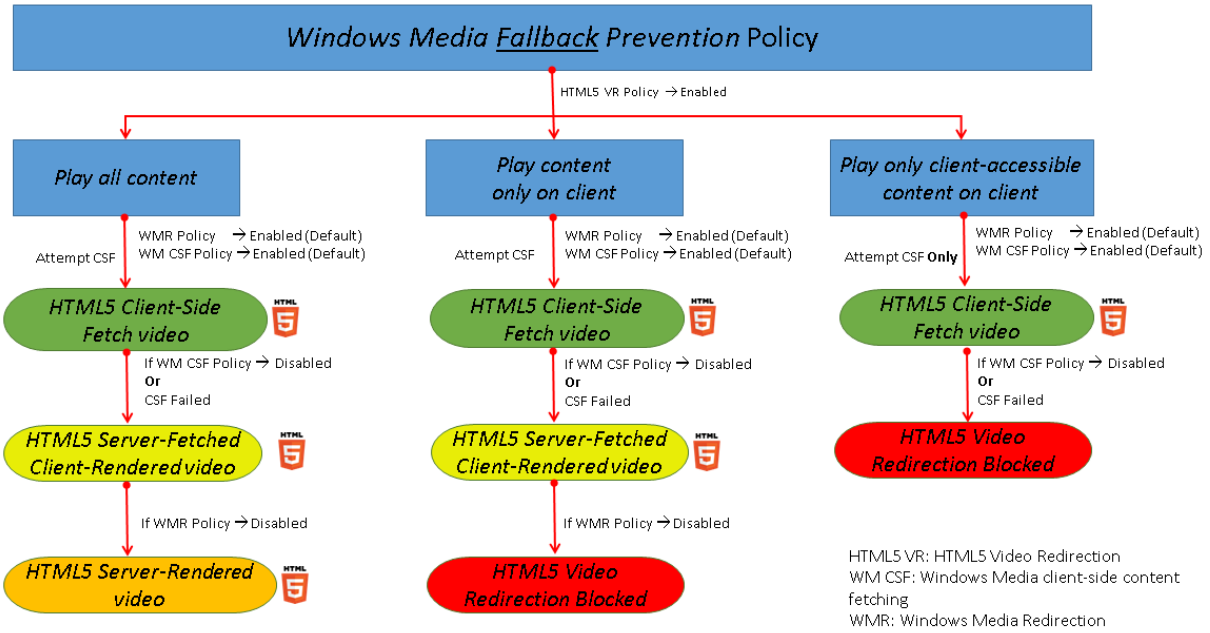
To configure this setting, choose one of the following options:

- **Play all content**. Attempt client-side content fetching, then Windows Media Redirection. If unsuccessful, play content on the server.
- **Play all content only on client**. Attempt client-side fetching, then Windows Media Redirection. If unsuccessful, the content does not play.
- **Play only client-accessible content on client**. Attempt only client-side fetching. If unsuccessful, the content does not play.

When the content does not play, the following error message displays in the player window (for a default duration of 5 seconds):

"Company has blocked video because of lack of resources"

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The duration of this error message can be customized with the following registry key on the VDA. If the registry entry does not exist, the duration defaults to 5 seconds.

The registry path varies depending on the architecture of the VDA:

`\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream`

Or

\HKLM\SOFTWARE\Citrix\HdxMediastream

Registry key:

Name: VideoLoadManagementErrDuration

Type: DWORD

Range: 1 - up to DWORD limit (default = 5)

Unit: seconds

Windows Media client-side content fetching

This setting applies to both HTML5 and Windows Media. The setting enables a user device to stream multimedia files directly from the source provider on the internet or intranet, rather than through the XenApp or XenDesktop® host server.

By default, this setting is **Allowed**. Allowing this setting improves network usage and server scalability. This improvement is achieved by moving any processing on the media from the host server to the user device. It also removes the requirement that an advanced multimedia framework such as Microsoft

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DirectShow or Media Foundation be installed on the user device. The user device requires only the ability to play a file from a URL

When adding this setting to a policy, make sure the **Windows Media Redirection** setting is present and set to **Allowed**. If **Windows Media Redirection** is disabled, the streaming of multimedia files to the user device direct from the source provider is also disabled.

Windows Media redirection

This setting applies to both HTML5 and Windows Media and controls and optimizes the way servers deliver streaming audio and video to users.

By default, this setting is **Allowed**. For HTML5, this setting doesn't take effect if the policy **HTML5 video redirection** is **Prohibited**.

When this setting is enabled the quality of audio and video rendered from the server increases to a level that compares with audio and video that played locally on a user device. The server streams multimedia to the client in the original, compressed form and allows the user device to decompress and render the media.

Windows Media redirection optimizes multimedia files that are encoded with codecs that adhere to Microsoft DirectShow, DirectX Media Objects (DMO), and Media Foundation standards. To play back a given multimedia file, a codec compatible with the encoding format of the multimedia file must be present on the user device.

By default, audio is disabled on Citrix Workspace app. To allow users to run multimedia applications in ICA® sessions, turn on audio or give users permission to turn on audio in their Citrix Workspace app interface.

Select **Prohibited** only if playing media using Windows Media redirection appears worse than when rendered using basic ICA compression and regular audio. This situation is rare but can happen under low bandwidth conditions, for example, with media with a low frequency of key frames.

Windows Media Redirection buffer size

This setting is a legacy and does not apply to HTML5.

This setting specifies a buffer size from 1 to 10 seconds for multimedia acceleration.

By default, the buffer size is 5 seconds.

Windows Media Redirection buffer size use

This setting is a legacy and does not apply to HTML5.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This setting enables or disables using the buffer size specified in the **Windows Media Redirection buffer size** setting.

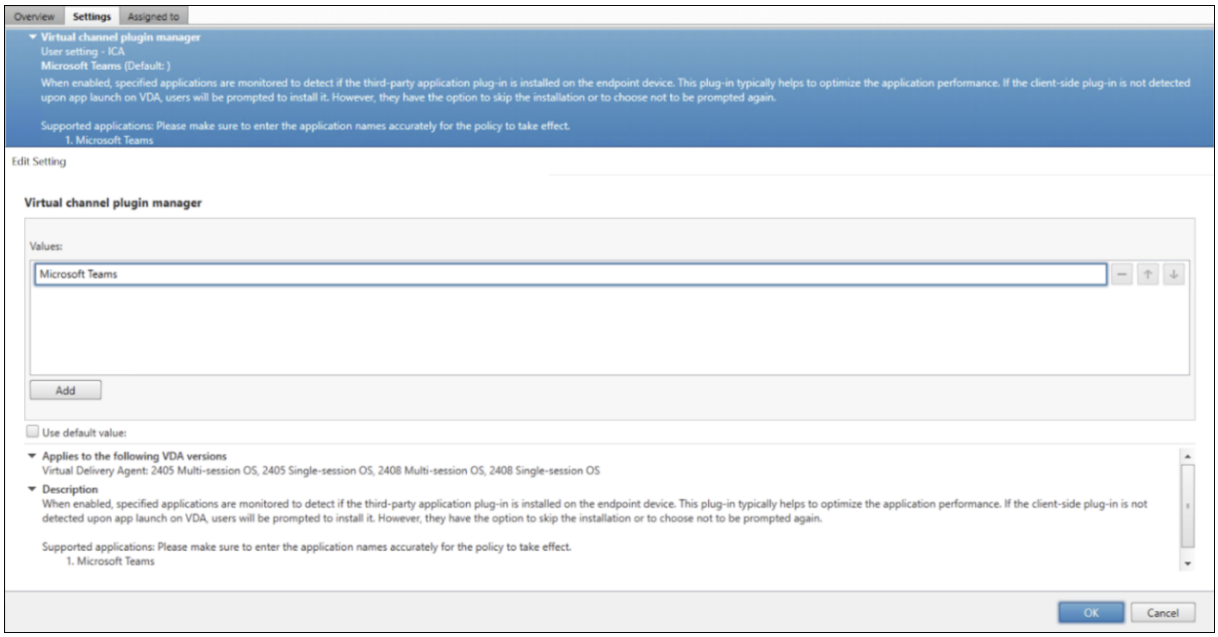
By default, the buffer size specified isn't used.

If this setting is disabled or if the **Windows Media Redirection buffer size** setting is not configured, the server uses the default buffer size value (five seconds).

Virtual channel plugin manager policy

The Virtual channel plugin manager section includes policy settings to configure this feature.

Virtual channel plugin manager is designed to deploy plugins across client endpoints for certain specified applications. The plugin manager detects specific applications running on the VDA and prompts the user to install the plugin on the endpoint for attaining best experience when running the application.



- Administrators can use the policy and specify the application for which they need the plugin to be installed across their endpoints.
- Application name should be the same as the name mentioned in the Supported applications in the policy description.
- By default, the policy is disabled.
- Currently supported applications
  - "Microsoft Teams"
- In the future, more applications are planned to be supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multi-stream connections policy settings

September 6, 2025

The **Multi-Stream connections** section includes policy settings for managing Quality of Service prioritization for multiple ICA® connections in a session.

> **Note:**
>
> MTU Discovery is not supported if the Multi-Stream connections policy is enabled.

Audio over UDP

This setting allows or prevents audio over UDP on the server.

By default, audio over UDP is allowed on the server.

When enabled, this setting opens a UDP port on the server to support all connections configured to use Audio over UDP Real-time Transport.

Audio UDP port range

This setting specifies the range of port numbers (lowest port number, highest port number) used by the Virtual Delivery Agent (VDA). This specification helps to exchange audio packet data with the user device. The VDA attempts to use each UDP port pair to exchange data with the user device, starting with the lowest and incrementing by two for each subsequent attempt. Each port handles both inbound and outbound traffic.

By default, this range is set to 16500,16509.

Multi-Port policy

This setting specifies the TCP ports to be used for ICA traffic and establishes the network priority for each port.

By default, the primary port (2598) has a High priority.

When you configure ports, you can assign the following priorities:

- **Very High:** for real-time activities, such as webcam conferences
- **High:** for interactive elements, such as screen, keyboard, and mouse
- **Medium:** for bulk processes, such as client drive mapping
- **Low:** for background activities, such as printing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each port must have a unique priority. For example, you cannot assign a Very High priority to both CGP port 1 and CGP port 3.

To remove a port from prioritization, set the port number to 0. You cannot remove the primary port and you cannot change its priority level.

When configuring this setting, restart the server. This setting takes effect only when the **Multi-Stream computer** setting policy setting is enabled.

Multi-Stream computer setting

This setting enables or disables Multi-Stream on the server.

By default, Multi-Stream is disabled. Configure the Multi-Stream computer policy setting if you use Citrix SD-WAN™ or third-party routers to achieve the desired Quality of Service.

If Multi-Stream is enabled, MTU Discovery, a feature of Adaptive Transport, is not supported.

When configuring this setting, reboot the server to ensure that changes take effect.

> **Important:**
>
> Using this policy setting with bandwidth limit policy settings such as Overall session bandwidth limit might produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

Multi-Stream user setting

This setting enables or disables Multi-Stream on the user device.

By default, Multi-Stream is disabled for all users. Configure the Multi-Stream user setting if you use Citrix SD-WAN or third-party routers to achieve the desired Quality of Service.

This setting takes effect only on hosts where the **Multi-Stream computer** setting policy setting is enabled.

> **Important:**
>
> Using this policy setting with bandwidth limit policy settings such as Overall session bandwidth limit might produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

Multi-Stream virtual channel assignment settings

This setting specifies the ICA stream the virtual channels are assigned to when multi-stream is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you do not configure these settings, virtual channels are kept in their default stream. To assign a virtual channel to an ICA stream, select the desired stream number (0, 1, 2, 3) from the **Stream Number** list next to the virtual channel name.

If there is a custom virtual channel in use in the environment, click **Add**, specify the virtual channel name in the text box under **Virtual Channels**, and select the desired stream number from the **Stream Number** list next to it. The name you specify must be the actual virtual channel name and not a friendly name. For example, CTXSBR instead of Citrix Browser Acceleration.

These settings take effect only when you've enabled the multi-stream computer setting.

By default, the virtual channels and their stream assignments are:

- AppFlow®: 2
- Audio: 0
- Browser Content Redirection: 2
- Client COM Port Mapping: 3
- Client Drive Mapping: 2
- Client Printer Mapping: 3
- Clipboard: 2
- CTXDND: 1 (**Note:** This supports the dragging and dropping files between a Citrix session and a local endpoint.)
- DVC Plug-in (Static VC name auto-generated from DVC Plug-in Friendly Name, or admin-assigned): 2
- End User Experience Monitoring: 1
- File Transfer (HTML5 Receiver): 2
- Generic Data Transfer: 2
- ICA Control: 1
- Input Method Editor: 1
- Legacy Client Printer Mapping (COM1): 1, 3
- Legacy Client Printer Mapping (COM2): 2, 3
- Legacy Client Printer Mapping (LPT1): 1, 3
- Legacy Client Printer Mapping (LPT2): 2, 3
- License Management: 1
- Microsoft Teams/WebRTC Redirection: 1
- Mobile Receiver: 1
- MultiTouch: 1
- Port Forwarding: 2
- Remote Audio and Video Extensions (RAVE): 2
- Seamless (Transparent Window Integration): 1
- Sensor and Location: 1
- Smart Card: 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Thinwire Graphics: 1
- Transparent UI Integration/Logon Status: 2
- TWAIN Redirection: 2
- USB: 2
- Zero Latency Font and Keyboard: 2
- Zero Latency Data Channel: 2

For more information on virtual channel assignments and priorities, see the Knowledge Center article CTX131001.

Port redirection policy settings

September 6, 2025

The **Port Redirection** section contains policy settings for client LPT and COM port mapping.

For Virtual Delivery Agent versions **earlier than 7.0**, use the following policy settings to configure port redirection. For the VDA versions **7.0 through 7.8**, configure these settings using the registry; see Configure COM Port and LPT Port Redirection settings using the registry. For the VDA version **7.9**, use the following policy settings.

Auto connect client COM ports

This setting enables or disables automatic connection of COM ports on user devices when users log on to a site.

By default, client COM ports are not automatically connected.

Auto connect client LPT ports

This setting enables or disables automatic connection of LPT ports on user devices when users log on to a site.

By default, client LPT ports are not connected automatically.

Client COM port redirection

This setting allows or prevents access to COM ports on the user device.

By default, COM port redirection is prohibited.

The following policy settings are related:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- COM port redirection bandwidth limit
- COM port redirection bandwidth limit percent

Client LPT port redirection

This setting allows or prevents access to LPT ports on the user device.

By default, LPT port redirection is prohibited.

LPT ports are used only by legacy applications that send print jobs to the LPT ports. These ports are not used by legacy applications that send print jobs to the print objects on the user device. Most applications today can send print jobs to printer objects. This policy setting is necessary only for servers that host legacy applications that print to LPT ports.

Note, although Client COM port redirection is bi-directional, LPT port redirection is output only and limited to \\client\LPT1 and \\client\LPT2 within an ICA session.

The following policy settings are related:

- LPT port redirection bandwidth limit
- LPT port redirection bandwidth limit percent

FIDO2 redirection

September 6, 2025

This setting enables or disables FIDO2 redirection. FIDO2 redirection lets users take advantage of the local endpoint FIDO2 components in a virtual machine. Users can authenticate virtual session through FIDO2 security keys or integrated biometrics on devices that have TPM 2.0 and Windows Hello.

When this setting is **Allowed**, users can do FIDO2 authentication by using the local endpoint capabilities. By default, this setting is **Allowed**.

Printing policy settings

September 6, 2025

The Printing section contains policy settings for managing client printing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client printer redirection

This setting controls whether client printers are mapped to a server when a user logs on to a session.

By default, client printer mapping is allowed. If this setting is disabled, the PDF printer for the session is not auto-created.

Related policy settings: auto-create client printers

Default printer

This setting specifies how the default printer on the user device is established in a session.

By default, the user's current printer is used as the default printer for the session.

To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do not adjust the user's default printer. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session is the first printer auto-created in the session, which is either:

- The first printer added locally to the Windows server in **Control Panel > Devices** and **Printers**.
- The first auto-created printer, if there are no printers added locally to the server.

You can use this option to present users with the nearest printer through profile settings (known as proximity printing).

Printer assignments

This setting provides an alternative to the Default printer and Session printers settings. Use the individual Default printer and Session printers settings to configure behaviors for a site, large group, or organizational unit. Use the **Printer assignments** setting to assign a large group of printers to multiple users.

This setting specifies how the default printer on the listed user devices is established in a session.

By default, the user's current printer is used as the default printer for the session.

It also specifies the network printers to be auto-created in a session for each user device. By default, no printers are specified.

- When setting the default printer value:

  To use the current default printer for the user device, select Do not adjust.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do no adjust. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session is the first printer auto-created in the session, which is either:

- The first printer added locally to the Windows server in **Control Panel > Devices** and Printers.
- The first auto-created printer, if there are no printers added locally to the server.

- When setting **session printers value: to add printers**, type the UNC path of the printer you want to auto-create. Alternatively, click **Browser** to search the entire network for a printer. You can also browse for printers by entering the printer server's FQDN or NetBIOS name. For more information, see Session printers. After adding the printer, you can apply customized settings for the current session at every logon.

Printer auto-creation event log preference

This setting specifies the events that are logged during the printer auto-creation process. You can choose to log no errors or warnings, only errors, or errors and warnings.

By default, errors and warnings are logged.

An example of a warning is an event in which a printer's native driver cannot be installed and the Universal print driver is installed instead. To use the Universal print driver in this scenario, configure the Universal print driver usage setting to Use universal printing only or Use universal printing only if the requested driver is unavailable.

Session printers

This setting specifies the network printers to be auto-created in a session. Inside the ICA/HDX session, the Citrix Print Manager service (CpSvc.exe) creates a network printer connection during the session logon for each network printer specified in the **Session Printer** policy setting. It deletes the printers during the session logoff. By default, no printers are specified.

In the **Session Printer** policy setting, the network printers can reside on a Windows Print Server or a Citrix Universal™ Print Server.

- **Windows Print Server:** Shares one or more network printers. It also has the native printer drivers required to use the network printers.
- **Universal Print Server:** A Windows Print Server where the Citrix Universal Print Server software has been installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When using a Windows Print Server, the Citrix Print Manager service creates the network printer connections using native printer drivers. The Citrix Virtual Apps™ server must have the native printer drivers installed on it.

When using a Citrix Universal Print Server, the Citrix Print Manager service creates the network printer connections using either native printer drivers, Citrix Universal Printer Driver, or Citrix Universal XPS Printer Driver. The driver that you use is controlled by the Universal Print Driver usage policy setting.

All Windows printer drivers currently fall within either the v3 or v4 driver version. For more information, see Support for the Microsoft V3 and V4 Printer Driver Architectures.

To add session printers and verify if they appear in the sessions, complete the following procedure:

1. Sign in to Web Studio, select **Policies** in the left pane, and then click the **Policies** tab.
2. Select the **Session printers** policy and click **Edit**.
3. On the **Edit Setting** page, clear the **Use default value** checkbox, and then click **Add** to add a printer by following these steps:

   a) Enter the UNC path of the printer in the format of `\\<FQDN of the printer server>\<printer name>`. Alternatively, click **Browse** to search the entire network for a printer. You can also browse for printers by entering the printer server's FQDN or NetBIOS name.

   > **Note:**
   >
   > To ensure you can search for a specific printer using **Browse**, when configuring the printer, make sure that the **List in the directory** option is selected under **Printer Settings > Printer Properties > Sharing**.

   b) By default, your user name and password are used to browse printer servers. If different domain credentials are required, select **Use different domain credentials to browse**, enter the necessary user name and password, and then click **Browse**.

   c) Click **Done**.

4. After the policy has been set, the published application might not display session printers. This issue might occur because the printer driver is missing from the Citrix Virtual Apps server or the policy has been created but not enabled.

   > **Note:**
   >
   > If a session printer needs a native printer driver and the native printer driver is not installed on the VDA, then the session printer might not be created in the session.

5. Start the published desktop and manually add the session printer in **Devices and Printers > Control Panel**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. If this fails, investigate the communication between the Citrix Virtual Apps server and the print server. Consider running a test with RDP.

Wait for printers to be created

Use the policy on the Delivery Controller to enable the feature on Citrix Virtual Desktops.

Wait for printers to be created (Server Desktop):

This setting allows a delay in connecting to a session so that client-redirected printers can be auto-created.

By default, a connection delay does not occur.

Wait for printers to be created (Citrix Virtual Apps):

Running the following PowerShell cmdlet allows a delay in connecting to virtual apps running on multi-session hosts so that client-redirected printers can be auto-created before the application is opened.

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation
$true
```

By default, a connection delay does not occur.

Client printers policy settings

September 6, 2025

The **Client Printers** section includes policy settings for client printers, including settings to auto-create client printers, retain printer properties, and connect to print servers.

Auto-create client printers

This setting specifies the client printers that are auto-created. This setting overrides default client printer auto-creation settings.

By default, all client printers are auto-created.

This setting takes effect only if the **Client printer redirection** setting is present and set to **Allowed**.

When adding this setting to a policy, select an option:

- **Auto-create all client printers** automatically creates all printers on a user device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Auto-create the client's default printer only** automatically creates only the printer selected as the default printer on the user device.
- **Auto-create local (non-network) client printers only** automatically creates only printers directly connected to the user device through an LPT, COM, USB, TCP/IP, or other local port.
- **Do not auto-create client printers** turns off autocreation for all client printers when users log on. Choosing this option causes the Remote Desktop Services (RDS) settings for autocreating client printers to override this setting in lower priority policies.

Auto-create generic universal printer

This setting enables or disables auto-creation of the generic Citrix Universal™ Printer object for sessions. These sessions include only the sessions where a user device compatible with Universal Printing is in use.

By default, the generic Universal Printer object isn't auto-created.

The following policy settings are related:

- Universal print driver usage
- Universal driver preference

Auto-create PDF universal printer

This setting enables or disables auto-creation of the Citrix PDF printer for sessions using:

- Citrix Workspace app for Windows (starting from VDA 7.19)
- Citrix Workspace™ app for Linux
- Citrix Workspace app for MacOS
- Citrix Workspace app for HTML5
- Citrix Workspace app for Chrome

By default, the Citrix PDF printer is not auto-created.

Client printer names

This setting selects the naming convention for auto-created client printers.

By default, standard printer names are used.

Select **Standard printer names** to use printer names such as "HPLaserJet 4 from client name in session 3."

Select **Legacy printer names** to use old-style client printer names and to preserve backward compatibility with legacy printers names as present in the XenDesktop versions of the product. You can use

© 1997–2026 Citrix Systems, Inc. All rights reserved.

this option with the current, Citrix Virtual Apps and Desktops versions of the product. An example of a legacy printer name is "Client/clientname#/HPLaserJet 4."This option is less secure.

When you use Citrix PDF printer in a session launched from Citrix Workspace app for HTML5, set the **Client printer names** setting as default or select **Standard printer names**. If you select **Legacy printer names**, Citrix Workspace app for HTML5 doesn't support the Citrix PDF Printer option.

Direct connections to print servers

This setting enables or disables direct connections from the virtual desktop or server-hosting applications to a print server for client printers. Here, the client printers are hosted on an accessible network share.

By default, direct connections are enabled.

Enable direct connections if the network print server is not across a WAN from the virtual desktop or server-hosting applications. Direct communication results in faster printing if the network print server and the virtual desktop or server-hosting applications are on the same LAN.

Disable direct connections if the network is across a WAN or has substantial latency or limited bandwidth. Print jobs are routed through the user device where they're redirected to the network print server. Data sent to the user device is compressed, so less bandwidth is consumed as the data travels across the WAN.

If two network printers have the same name, the printer on the same network as the user device is used.

Printer driver mapping and compatibility

This setting specifies the driver substitution rules for auto-created client printers.

This setting is configured to exclude Microsoft OneNote and XPS Document Writer from the auto-created client printers list.

When you define driver substitution rules, you can allow or prevent printers to be created with the specified driver. Also, you can allow created printers to use only universal print drivers. Driver substitution overrides or maps the printer driver names the user device provides, substituting an equivalent driver on the server. These rules give server applications access to client printers that have the same drivers as the server, but different driver names.

You can do the following:

- Add a driver mapping
- Edit an existing mapping
- Override custom settings for a mapping

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Remove a mapping
- Change the order of driver entries in the list

When adding a mapping, enter the client printer driver name and then select the server driver you want to replace.

Printer properties retention

This setting specifies whether to store printer properties and where to store them.

By default, the system determines if printer properties are stored on the user device, if available, or in the user profile.

When adding this setting to a policy, select an option:

- Saved on the client device only is for user devices that have a mandatory or roaming profile that is not saved.
- Retained in user profile only is for user devices constrained by bandwidth (this option reduces network traffic) and logon speed or for users with legacy plug-ins. This option stores printer properties in the user profile on the server and prevents any properties exchange with the user device. This option is applicable only if a Remote Desktop Services (RDS) roaming profile is used.
- Held in profile only if not saved on the client allows the system to determine where printer properties are stored. Printer properties are stored either on the user device, if available, or in the user profile. Although this option is the most flexible, it can also slow logon time and use extra bandwidth for system-checking.
- Do not retain printer properties prevents storing printer properties.

Retained and restored client printers

This setting enables or disables the retention and re-creation of printers on the user device. By default, client printers are auto-retained and auto-restored.

Retained printers are user-created printers that are created again, or remembered, at the start of the next session. When Citrix Virtual Apps™ recreates a retained printer, it considers all policy settings except the **Auto-create client printers** setting.

Restored printers are printers fully customized by an administrator, with a saved state that is permanently attached to a client port.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix PDF Universal Printer driver

The Citrix PDF Universal Printer driver enables users to print documents opened with hosted applications or applications that are running on virtual desktops delivered by Citrix Virtual Apps and Desktops. When a user selects the **Citrix PDF Printer** option, the driver converts the file to PDF and transfers the PDF to the local device. The PDF is then opened for viewing and printing from a locally attached printer. PDF is one of the formats supported with Citrix Universal Printing (in addition to EMF and XPS).
The PDF printer can be enabled, configured, and set as default using a Citrix Policy. The **Citrix PDF Printer** option is available to users of the Citrix Workspace app for Windows, Linux, MacOS, Chrome, and HTML5.

> **Note:**
>
> A PDF viewer is required for Windows endpoints. The client must have an application that has file type association registered on Windows to open PDF files.

Drivers policy settings

May 5, 2025

The **Drivers** section includes policy settings related to printer drivers.

Automatic installation of in-box printer drivers

> **Note**
>
> This policy does not support VDAs in this release.

This setting enables or disables the automatic installation of printer drivers from the following:

- Windows in-box driver set
- Driver packages staged on the host using `pnputil.exe /a`

By default, these drivers are installed as needed.

Universal driver preference

This setting specifies the order in which universal printer drivers are used, beginning with the first entry in the list.

By default, the preference order is:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- EMF
- XPS
- PCL5c
- PCL4
- PS

You can add, edit, or remove drivers, and change the order of drivers in the list.

Universal print driver usage

This setting specifies when to use universal printing.

By default, universal printing is used only if the requested driver is unavailable.

Universal printing employs generic printer drivers instead of standard model-specific drivers, potentially simplifying the burden of driver management on host computers. The availability of universal print drivers depends on the capabilities of the user device, host, and print server software. In certain configurations, universal printing might not be available.

When adding this setting to a policy, select an option from the following table:

Option	Description
Use only printer model specific drivers	Specifies that the client printer uses only the standard model-specific drivers that are auto-created during sign in. If the requested driver is unavailable, the client printer cannot be auto-created.
Use universal printing only	Specifies that no standard model-specific drivers are used. Only universal print drivers are used to create printers.
Use universal printing only if requested driver is unavailable	Uses standard model-specific drivers for printer creation if they are available. If the driver is not available on the server, the client printer is created automatically with the appropriate universal driver.
Use printer model specific drivers only if universal printing is unavailable	Uses the universal print driver if it is available. If the driver is not available on the server, the client printer is created automatically with the appropriate model-specific printer driver.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Universal Print Server policy settings

September 6, 2025

The **Universal Print Server** section includes policy settings for handling the Universal Print Server.

SSL cipher suite

This setting specifies the set of SSL/TLS cipher suites that are used in the Universal Print Client for encrypted print data stream (CGP) connections.

To control the cipher suite package used by the Universal Print Client for encrypted print web service (HTTPS/SOAP) connections, see [SCHANNEL].

Default value: ALL

This setting has the following values: ALL, COM or GOV.

The cipher suites corresponding to each value are the following:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL compliance mode

This setting specifies the level of compliance with NIST Special Publication 800-52 that is used by the Universal Print Client for encrypted print data stream (CGP) connections.

Default value: None.

This setting has the following values:

None.

The encrypted print data stream (CGP) connections use the default compliance mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SP800-52.

The encrypted print data stream (CGP) connections use the NIST Special Publication 800-52 compliance mode.

SSL enabled

This setting specifies whether SSL/TLS is used by the Universal Print Client for the following:

- Print data stream (CGP) connections
- Web service (HTTP/SOAP) connections

When you set **Universal Print Server enable** to **Enabled with fallback to Windows' native remote printing**, fallback connections are made by the Microsoft Windows Network Print Provider. This setting does not affect these fallback connections.

Default value: Disabled

This setting has the following values:

Enabled.

The Universal Print Client uses SSL/TLS to connect to the Universal Print Server.

Disabled.

The Universal Print Client uses SSL/TLS to connect to the Universal Print Server.

SSL FIPS mode

This setting specifies whether the SSL/TLS cryptographic module used by the Universal Print Client for print data stream (CGP) connections run in FIPS mode.

Default value: Disabled

This setting has the following values:

Enabled.

FIPS mode is on.

Disabled.

FIPS mode is off.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL protocol version

This setting specifies the SSL/TLS protocol version used by the Universal Print Client.

Default value: ALL

This setting has the following values:

ALL.

Use TLS versions 1.0, 1.1 or 1.2.

TLSv1.

Use TLS version 1.0.

TLSv1.1.

Use TLS version 1.1.

TLSv1.2.

Use TLS version 1.2.

SSL Universal Print Server encrypted print data stream (CGP) port

This setting specifies the TCP port number of the Universal Print Server encrypted print data stream (CGP) port. This port receives data for print jobs.

Default value: 443

SSL Universal Print Server encrypted web service (HTTPS/SOAP) port

This setting specifies the TCP port number of the Universal Print Server encrypted web service (HTTP-S/SOAP) port. This port receives data for print commands.

Default value: 8443

Universal Print Server enable

This policy enables or disables the use of the Citrix Universal Print Server (UPS). Apply this policy setting to Organizational Units (OUs) that includes the virtual desktop or server-hosting applications.This policy settings include fallback options to allow connections to print servers using the native Windows remote printing service in the event that the Citrix UPS component is not installed or unavailable on the requested print server. Changes to this policy is applicable only after the VDA is restarted.

By default, the Universal Print Server is disabled.

When adding this setting to a policy, select one of the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Enabled with fallback to Windows native remote printing**: The Universal Print Server services the Network printer connections, if possible. If the Universal Print Server is not available, the Windows Print Provider is used. The Windows Print Provider continues to handle all printers previously created with the Windows Print Provider.
- **Enabled with no fallback to Windows native remote printing**: The Universal Print Server services the Network printer connections exclusively. If the Universal Print Server is unavailable, the network printer connection fails. This setting effectively disables network printing through the Windows Print Provider. Printers previously created with the Windows Print Provider are not created while a policy containing this setting is active.
- **Disabled**: The Universal Print Server feature is disabled. No attempt is made to connect with the Universal Print Server when connecting to a network printer with a UNC name. Connections to remote printers continue to use the Windows native remote printing facility.

Universal Print Server print data stream (CGP) port

This setting specifies the TCP port number used by the Universal Print Server print data stream Common Gateway Protocol (CGP) listener. Apply this policy setting only to OUs containing the print server.

By default, the port number is set to 7229.

Valid port numbers must be in the range of 1-65535.

Universal Print Server print stream input bandwidth limit (Kbps)

This setting specifies the upper boundary (in kilobits per second) for the transfer rate of print data. The transfer rate is calculated for the print data that is delivered from each print job to the Universal Print Server using CGP. Apply this policy setting to OUs containing the virtual desktop or server-hosting applications.

By default, the value is 0, which specifies no upper boundary.

Universal Print Server web service (HTTP/SOAP) port

This setting specifies the TCP port number used by the Universal Print Server's web service (HTTP/-SOAP) listener. The Universal Print Server is an optional component that enables the use of Citrix universal print drivers for network printing scenarios.

When the Universal Print Server is used, printing commands are sent from Citrix Virtual Apps and Desktops hosts to the Universal Print Server via SOAP over HTTP. This setting modifies the default TCP port on which the Universal Print Server listens for incoming HTTP/SOAP requests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You must configure both host and print server HTTP port identically. If you do not configure the ports identically, the host software doesn't connect to the Universal Print Server. This setting changes the VDA on Citrix Virtual Apps and Desktops. In addition, you must change the default port on the Universal Print Server.

By default, the port number is set to 8080.

Valid port numbers must be in the range of 0-65535.

Universal Print Servers for load balancing

This setting lists the Universal Print Servers to be used to load balance printer connections established at session launch, after evaluating other Citrix® printing policy settings. To optimize printer creation time, Citrix recommends that all print servers have the same set of shared printers. There is no upper limit to the number of print servers which can be added for load balancing.

This setting also implements print server failover detection and printer connections recovery. The print servers are checked periodically for availability. If a server failure is detected, that server is removed from the load balancing scheme. Also, the printer connections on that server are redistributed among other available print servers. When the failed print server recovers, it is returned to the load balancing scheme.

Click **Validate Servers** to check that each server is a print server, that the server list doesn't include duplicate server names, and that all servers have an identical set of shared printers installed. This operation might take some time.

Universal Print Servers out-of-service threshold

This setting specifies how long the load balancer must wait for an unavailable print server to recover before it determines that the server is permanently offline and redistributes its load to other available print servers.

By default, the threshold value is set to 180 (seconds).

Universal Print Server web service (HTTP/SOAP) connect timeout

This setting specifies the number of seconds that the Universal Print Client must wait until a Universal Print Server web service connect() operation times out. This setting has the following values. All these values are numeric and the units (of time) are seconds.

- The minimum value is 0.
- The maximum value is 60.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The default value is 10.

When the timeout is between 1 and 60 (inclusive), the Universal Print Client waits for the specified time for the operation to complete. The operation is a connect TCP socket operation. Sockets are a facility of the Windows operating system that allows interprocess communication over TCP/IP networks.

When the timeout is 0, the Universal Print Client uses the default timeout defined by the operating system. This configuration was the available configuration present in the previous versions of the Universal Print Client before this change.

The Universal Print Client is the component of the Virtual Delivery Agent (VDA) that communicates with the Universal Print Server.

> **Note:**
>
> This policy setting is applicable in the VDA version 7.35 and later.

Universal Print Server web service (HTTP/SOAP) receive timeout

This setting specifies the number of seconds that the Universal Print Client must wait until a Universal Print Server web service recv() operation times out. This setting has the following values and all these values are numeric and the units (of time) are seconds.

- The minimum value is 0.
- The maximum value is 60.
- The default value is 10.

When the timeout is between 1 and 60 (inclusive), the Universal Print Client waits for the specified time for the operation to complete. The operation is a receive TCP socket operation. Sockets are a facility of the Windows operating system that allows interprocess communication over TCP/IP networks.

When the timeout is 0, the Universal Print Client uses the default timeout defined by the operating system. This configuration was the available configuration present in the previous versions of the Universal Print Client before this change.

Universal Print Client is the component of the Virtual Delivery Agent (VDA) that communicates with the Universal Print Server.

> **Note:**
>
> This policy setting is applicable in the VDA version 7.35 and later.

Universal Print Server web service (HTTP/SOAP) send timeout

This setting specifies the number of seconds that the Universal Print Client must wait until a Universal Print Server web service send() operation times out. This setting has the following values. All these

© 1997–2026 Citrix Systems, Inc. All rights reserved.

values are numeric and the units (of time) are seconds.

- The minimum value is 0.
- The maximum value is 60.
- The default value is 10.

When the timeout is between 1 and 60 (inclusive), the Universal Print Client waits for the specified time for the operation to complete. The operation is a send TCP socket operation. Sockets are a facility of the Windows operating system that allows interprocess communication over TCP/IP networks.

When the timeout is 0, the Universal Print Client uses the default timeout defined by the operating system. This configuration was the available configuration present in the previous versions of the Universal Print Client before this change.

Universal Print Client is the component of the VDA that communicates with the Universal Print Server.

> **Note:**
>
> This policy setting is applicable in the VDA version 7.35 and later.

Universal printing policy settings

September 6, 2025

The **Universal Printing** section includes policy settings for managing universal printing.

Universal printing EMF processing mode

This setting controls the method of processing the EMF spool file on the Windows user device.

By default, EMF records are spooled directly to the printer.

When adding this setting to a policy, select an option:

- Reprocess EMFs for printer forces the EMF spool file to be reprocessed and sent through the GDI subsystem on the user device. You can use this setting for drivers that require EMF reprocessing but that might not be selected automatically in a session.
- Spool directly to printer, when used with the Citrix Universal™ print driver, ensures the EMF records are spooled and delivered to the user device for processing. Typically, these EMF spool files are injected directly to the client's spool queue. For printers and drivers that are compatible with the EMF format, this is the fastest printing method.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Universal printing image compression limit

This setting specifies the following:

- Maximum quality available for images printed with the Citrix Universal print driver
- Minimum compression level available for images printed with the Citrix Universal print driver

By default, the image compression limit is set to Best quality (lossless compression).

If No Compression is selected, compression is disabled for EMF printing only.

When adding this setting to a policy, select an option:

- No compression
- Best quality (lossless compression)
- High quality
- Standard quality
- Reduced quality (maximum compression)

When adding this setting to a policy that includes the **Universal printing optimization defaults** setting, be aware of the following:

- Consider the compression level in the **Universal printing image compression limit** setting is lower than the level defined in the **Universal printing optimization defaults** setting. In this case, the images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

Universal printing optimization defaults

This setting specifies the default values for printing optimization when the universal print driver is created for a session.

- Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
- Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.
- Image and Font Caching settings specify whether to cache images and fonts that appear multiple times in the print stream or not. This setting ensures that each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached. These settings apply only if the user device supports this behavior.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Allow non-administrators to modify these settings specifies whether users can change the default print optimization settings within a session or not. By default, users aren't allowed to change the default print optimization settings.

Note: All of these options are supported for EMF printing. For XPS printing, only the Desired image quality option is supported.

When adding this setting to a policy that includes the **Universal printing image compression limit** setting, be aware of the following:

- Consider the compression level in the **Universal printing image compression limit** setting is lower than the level defined in the **Universal printing optimization defaults** setting. In this case, the images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

Universal printing preview preference

This setting specifies whether to use the print preview function for auto-created or generic universal printers.

By default, print preview isn't used for auto-created or generic universal printers.

When adding this setting to a policy, select an option:

- Do not use print preview for auto-created or generic universal printers
- Use print preview for auto-created printers only
- Use print preview for generic universal printers only
- Use print preview for both auto-created and generic universal printers

Universal printing print quality limit

This setting specifies the maximum dots per inch (dpi) available for generating printed output in a session.

By default, No Limit is enabled, meaning users can select the maximum print quality allowed by the printer to which they connect.

If this setting is configured, it limits the maximum print quality available to users in terms of output resolution. Both the print quality itself and the print quality capabilities of the printer to which the user connects are restricted to the configured setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, if configured to Medium Resolution (600 DPI), users can print the output with a maximum quality of 600 DPI only. Also, the **Print Quality** setting on the **Advanced** tab of the **Universal Printer** dialog box shows resolution settings only up to and including Medium Quality (600 DPI).

When adding this setting to a policy, select an option:

- Draft (150 DPI)
- Low Resolution (300 DPI)
- Medium Resolution (600 DPI)
- High Resolution (1200 DPI)
- No Limit

Security policy settings

May 5, 2025

The **Security** section includes the policy setting for configuring session encryption and encryption of logon data.

SecureICA minimum encryption level

This setting specifies the minimum level at which to encrypt session data sent between the server and a user device.

Important: For the Virtual Delivery Agent 7.x, this policy setting can be used only to enable the encryption of the logon data with RC5 128-bit encryption. Other settings are provided only for backwards compatibility with legacy versions of Citrix Virtual Apps and Desktops.

For the VDA 7.x, encryption of session data is set using the basic settings of the VDA's Delivery Group. If Enable Secure ICA is selected for the Delivery Group, session data is encrypted using RC5 (128 bit) encryption. If Enable Secure ICA is not selected for the Delivery Group, session data is encrypted with Basic encryption.

When adding this setting to a policy, select an option:

- Basic encrypts the client connection using a non-RC5 algorithm. It protects the data stream from being read directly, but it can be decrypted. By default, the server uses Basic encryption for client-server traffic.
- RC5 (128 bit) logon only encrypts the logon data using RC5 128-bit encryption and the client connection using Basic encryption.
- RC5 (40 bit) encrypts the client connection using RC5 40-bit encryption.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- RC5 (56 bit) encrypts the client connection using RC5 56-bit encryption.
- RC5 (128 bit) encrypts the client connection using RC5 128-bit encryption.

The settings you specify for client-server encryption can interact with any other encryption settings in your environment and your Windows operating system. Consider a higher priority encryption level is set on either a server or user device. In this case, the settings you specify for published resources can be overridden.

You can raise encryption levels to further secure communications and message integrity for certain users. If a policy requires a higher encryption level, Citrix Receivers using a lower encryption level are denied connection.

SecureICA does not perform authentication or check data integrity. To provide end-to-end encryption for your site, use SecureICA with TLS encryption.

SecureICA does not use FIPS-compliant algorithms. If this setting is an issue, configure the server and Citrix Receivers to avoid using SecureICA.

SecureICA uses the RC5 block cipher as described in RFC 2040 for confidentiality. The block size is 64 bits (a multiple of 32-bit word units). The key length is 128 bits. The number of rounds is 12.

Keys for the RC5 block cipher are negotiated when a session is created. Negotiation is performed using the Diffie-Hellman algorithm. This negotiation uses Diffie-Hellman public parameters. These parameters are stored in the Windows registry when the Virtual Delivery Agent is installed. Public parameters are not secret. The result of the Diffie-Hellman negotiation is a secret key, from which the session keys for the RC5 block cipher are derived. Separate session keys are used for user logon, and for data transfer. Also, separate session keys are used for traffic to and from the Virtual Delivery Agent. Therefore there are four session keys for each session. The secret keys and session keys are not stored. Initialization vectors for the RC5 block cipher are also derived from the secret key.

Server limits policy settings

September 6, 2025

The **Server Limits** section includes the policy setting for controlling idle connections.

Server idle timer interval

This setting determines how long an uninterrupted user session is maintained if there is no input from the user. The data is calculated in milliseconds.

By default, idle connections are not disconnected (server idle timer interval = 0). Citrix® recommends setting this value to a minimum of 60000 milliseconds (60 seconds).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To display the policy, select **Multiple Versions**, clear the Single-session OS versions, and then select **Server Limits**.

> **Note**
>
> When this policy setting is used, an "Idle timer expired"dialog box might appear to users when the session has been idle for the specified time. Citrix policy settings don't control this Microsoft dialog box message. For more information, see http://support.citrix.com/article/CTX118618.

Session limits policy settings

September 6, 2025

The **Session Limits** section includes policy settings that control how long sessions remain connected before they are forced to log off.

Disconnected session timer

This setting enables or disables a timer that specifies how long a disconnected, locked desktop remains locked before the session is logged off.

If this timer is enabled, the disconnected session is logged off when the timer expires.

By default, disconnected sessions aren't logged off.

Remote PC Access disconnected session timer

This setting enables or disables a timer that logs off a disconnected user session after the timer expires. If you enable this setting, use the **Disconnected session timer interval** setting to specify how many minutes a disconnected desktop remain locked before the user session is logged off.

By default, this setting is disabled.

Disconnected session timer interval

This setting specifies how many minutes a disconnected, locked desktop remain locked before the session is logged off.

By default, the time period is 1,440 minutes (24 hours).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disconnected session timer –Multi-session

This setting enables or disables a timer to determine how long a disconnected RDS session can persist before the session logs off. By default, this timer is disabled and disconnected sessions are not logged off.

Disconnected session timer interval –Multi-session

This setting determines how many minutes, a disconnected RDS session can persist before the session is logged off. By default, the time period is 1440 minutes (24 hours).

Session connection timer

This setting enables or disables a timer that specifies the maximum duration of an uninterrupted connection between a user device and a desktop. If this timer is enabled, the session is disconnected or logged off when the timer expires. The Microsoft **End session when time limits are reached** setting determines the next state for the session.

By default, this timer is disabled.

Session connection timer interval

This setting specifies the maximum number of minutes for an uninterrupted connection between a user device and a desktop.

By default, the maximum duration is 1,440 minutes (24 hours).

Session connection timer –Multi-session

This setting enables or disables a timer that specifies the maximum duration of an uninterrupted connection between a user device and a terminal server. By default, this timer is disabled.

Session connection timer interval –Multi-session

This setting specifies the maximum number of minutes for an uninterrupted connection between a user-device and an RDS session. By default, the maximum duration is 1440 minutes (24 hours).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session idle timer

When a user supplies no input, this setting is used to enable or disable:

- A timer that specifies how long an uninterrupted user device connection to a desktop is maintained.

When this timer expires, the session is placed in the disconnected state and the **Disconnected session timer** applies. If the **Disconnected session timer** is disabled, the session is not logged off.

By default, this timer is enabled.

Session idle timer interval

When there is no input from the user, this setting is used to specify:

- The number of minutes for which an uninterrupted user device connection to a desktop is maintained.

By default, idle connections are maintained for 1,440 minutes (24 hours).

Session idle timer –Multi-session

This setting enables or disables a timer to determine the maximum duration of an idle connection between a user device and a terminal server. By default, this timer is disabled.

Session idle timer interval–Multi-session

This setting specifies how many minutes an idle connection between a user device and an RDS session. By default, the maximum duration is 1440 minutes (24 hours).

> **Note:**
>
> Timer settings for multi-session machines configured using Citrix® policies are expected to override timer settings configured through Microsoft Group Policies. To avoid unexpected behavior, we recommend you configure timer settings using one of the two methods.

Session reliability policy settings

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **session reliability** section includes policy settings for managing session reliability connections.

Session reliability connections

This setting allows or prevents sessions to be kept open during a loss of network connectivity. Session reliability, along with auto client reconnection, allows users to reconnect automatically to their Citrix Workspace™ app sessions after recovering from network disruptions. By default, session reliability is Allowed.

The settings in Web Studio are enforced on the client for the following:

- Citrix Workspace app 1808 and later
- Citrix Receiver for Windows 4.7 and later.

Web Studio policy overrides Citrix Receiver™ Group Policy Object on the clients. Updates to these policies in Web Studio synchronize session reliability from server to client.

> **Note:**
>
> - Citrix Receiver for Windows 4.7 and later and Citrix Workspace apps for Windows - Set the policy in Web Studio.
> - Citrix Receivers for Windows earlier than 4.7 - Set policies in Web Studio. Also set the Citrix Receiver Group Policy Object template on the client for consistent behavior.

Session reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application that they're using until network connectivity resumes.

Use session reliability, to keep the session active on the server. To indicate that connectivity is lost, the user display becomes opaque. The user might see a frozen session during the interruption. User can resume interacting with the application when the network connection is restored. Session reliability reconnects users without reauthentication prompts.

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 time specified in the session reliability timeout setting. After that, the auto client reconnect settings take effect, trying to reconnect the user to the disconnected session.

By default, session reliability is Allowed.

> **Note:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> When Citrix ADC is in use, you must select **Enable session reliability** in the Citrix StoreFront > **Manage Citrix Gateways** / **Secure Ticket Authority** to proxy ICA connections.

Session reliability port number

This setting specifies the TCP port number for incoming session reliability connections.

By default, the port number is set to 2598.

Session reliability timeout

This setting specifies the length of time, in seconds. This time is the time that the session reliability proxy waits for a user to reconnect before allowing the session to be disconnected.

Although you can extend the amount of time a session is kept open, this feature is a convenience and doesn't prompt the user for reauthentication. The longer a session is open, the chances increase that a user might leave the device unattended and potentially accessible to unauthorized users.

By default, the timeout is set to 180 seconds, or three minutes.

Session watermark policy settings

September 6, 2025

The **session watermark** section includes policy settings to configure this feature.
Enabling this feature causes a significant rise in the network bandwidth and CPU usage by the VDA machine. We recommend that you configure the session watermark for selected VDA machines based on your available hardware resources.

> **Important**
>
> Enable session watermark for the other watermark policy settings to be effective. To achieve a better user experience, don't enable more than two watermark text items.

Enable session watermark

When you enable this setting, the session display has an opaque textual watermark displaying session-specific information. The other watermark settings depend on this one being enabled.

By default, the session watermark is disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Include client IP address

When you enable this setting, the session displays the current client IP address as a watermark.

By default, Include client IP address is disabled.

Include connection time

When you enable this setting, the session watermark displays a connect time. The format is yyyy/mm/dd hh:mm. The time displayed is based on the system clock and time zone.

By default, Include connection time is disabled.

Include logon user name

When you enable this setting, the session displays the current logon user name as a watermark. The display format is USERNAME@DOMAINNAME. We recommend that the user name is a maximum of 20 characters. When a user name is more than 20 characters, excessively small character fonts or truncation might occur and lessen the watermark effectiveness.

By default, Include logon user name is enabled.

Include VDA host name

When you enable this setting, the session displays the VDA host name of the current ICA® session as a watermark.

By default, Include VDA host name is enabled.

Include VDA IP address

When you enable this setting, the session displays the VDA IP address of the current ICA session as a watermark.

By default, the VDA IP address is disabled.

Session watermark style

This setting controls whether you display a single watermark text label or multiple labels. Choose **Multiple** or **Single** from the **Value** drop-down menu.

Multiple displays five watermark labels in the session. One in the center and four in the corners.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Single displays a single watermark label in the center of the session.

By default, the Session watermark style is Multiple.

Watermark custom text

This setting lets you apply custom text (for example, the corporate name) to display in the session watermark. When you configure a non-empty string, it displays the text in a new line appending other information enabled in the watermark. The watermark custom text is limited to 25 Unicode characters. If you configure a longer string, it is truncated to 25 characters.

There is no default text.

Starting with Citrix Virtual Apps and Desktops™ 7 2206, you can add more customization using custom tags in the text. As a result, the maximum number of characters in the custom text is increased to 1024.

The available tags for watermark settings are described in the following table:

Tag	Description	Example
`<font=value>`	Allows you to change the font of watermark text. The value is the name of a font available on the VDA.	`<font=Courier New>`
`<fontzoom=value>`	Allows you to set the percentage of the font zoom factor. The value is 200 for 200% zoom on watermark text.	`<fontzoom=200>`
`<position=value>`	Allows you to change the position of the watermark text. The values are `center`, `topleft`, `topright`, `bottomleft`, and `bottomright`. This tag is only applicable with single style.	`<position=topright>`
`<rotation=value>`	Allows you to rotate watermark text. The value is specified in degree and the range is from -360 and 360.	`<rotation=45>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tag	Description	Example
<style=value>	Allows you to change the display style. This tag overrides the Session watermark style policy.	<style=single>

The following watermark styles are available:

- Single style - A single watermark text label appears at the center of the session. You can use the position tag to change the location.
- xstyle or multiple - Five watermark labels appear in the session - one in the center and one in each corner.
- Tile - Multiple labels appear in the session. Watermark text is placed equally across the entire screen.

The available tags for changing watermark text are described in the following table:

Tag	Description
<clientip>	The IP address of the endpoint.
<date>	The date the session was established.
<domain>	The domain name of the logged-in user account.
<hostname>	The machine name of the VDA.
<newline>	Creates an extra line.
<serverip>	The IP address of the VDA.
<time>	The time the session was established.
<username>	The name of the user.

> **Note:**
>
> - The **Watermark custom text** policy takes effect only when the **Enable session watermark** policy is enabled. Its default value is *Disabled*.
> - If you use the tags for changing watermark text, all other session watermark policies, except **Enable session watermark**, are ignored. If you use the tags for watermark text settings, you can use all other watermark policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Watermark transparency

You can specify watermark opacity from 0 through 100. The larger the value specified, the more opaque the watermark.

By default, the value is 17.

Time zone control policy settings

April 1, 2026

The **Time Zone Control** section includes policy settings related to using local time in sessions.

Estimate local time for legacy clients

This setting enables or disables estimating the local time zone of user devices. These devices include the user devices that send inaccurate time zone information to the server.

By default, the server estimates the local time zone when necessary.

This setting is intended for use with legacy Citrix Receivers or ICA clients that do not send detailed time zone information to the server. Consider that this setting is used with Citrix Receivers that send detailed time zone information to the server. For example, supported versions of Citrix Receiver™ for Windows. In this case, this setting has no effect.

Restore desktop OS time zone on session disconnect or logoff

Consider that the user disconnects or logs off a session. In this case, this setting determines whether the time zone setting for a Single-session OS VDA is restored to the machine's original time zone. If you enable this setting, the VDA restores the machine's time zone to its original setting when the user disconnects or logs off. For this setting to take effect, set the **Use local time of client** to **Use client time zone**.

By default, this setting is enabled.

Use local time of client

This setting determines the time zone setting of the user session. The choices are the time zone of the user session (server time zone) or the time zone of the user device (client time zone).

By default, the time zone of the user session is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For this setting to take effect in **multi-session** session hosts, enable the **Allow time zone redirection** setting in the Group Policy Editor. The setting is in **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Device and Resource Redirection**.

> **IMPORTANT:**
>
> When using the single-session VDA version 2507 on machines running a server OS, you must add **Users** to the **Change the time zone** User Rights Assignment policy. This policy is located under **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**. This is not required when using version 2507 CU1 or later.
>
> When using the single-session VDA version 2507 CU1 and later, the **Citrix Portica Timezone Service (CtxPicaTzSvc)** is automatically added to the **Change the time zone** User Rights Assignment policy during the VDA installation. If you have any policies or processes in place that remove users or processes from these policies, make sure to modify them so that the Citrix services are not removed. Otherwise, time zone redirection will not work.

TWAIN devices policy settings

September 6, 2025

The **TWAIN devices** section includes policy settings related to the following:

- Mapping client TWAIN devices, such as digital cameras or scanners
- Optimizing image transfers from server to client

> **Note:**
>
> TWAIN 2.0 is supported with Citrix Receiver for Windows 4.5.

Client TWAIN device redirection

TWAIN devices communicate with server-hosted image processing applications by using the TWAIN protocol.

This setting allows or prevents users from accessing TWAIN devices on the user device. By default, TWAIN device redirection is allowed.

The following policy settings are related:

- TWAIN compression level
- TWAIN device redirection bandwidth limit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- TWAIN device redirection bandwidth limit percent

TWAIN compression level

This setting specifies the level of compression of image transfers from client to server. Use Low for best image quality, Medium for good image quality, or High for low image quality. By default, medium compression is applied.

USB devices policy settings

September 13, 2025

The **USB devices** section includes policy settings for managing file redirection for USB devices.

Client USB device optimization rules

Client USB device optimization rules can be applied to devices to disable optimization, or to change the optimization mode.

When a user plugs in a USB input device, the host checks if the **USB policy** settings allow the device. If the device is allowed, the host then checks the **Client USB device optimization rules** for the device. If no rule is specified, then the device is not optimized. Capture mode (04) is the recommended mode for signature devices. For other devices which have degraded performance over higher latency, administrators can enable Interactive mode (02). See descriptions of the available modes in the table in this article.

Good to know

- For the use of Wacom signature pads and tablets, we recommend that you disable the screen saver. Steps on how to disable the screen saver are at the end of this section.
- Support for the optimization of Wacom STU signature pads and tablets series of products has been preconfigured in the installation of Citrix Virtual Apps and Desktops™ policies.
- Signature devices work across Citrix Virtual Apps and Desktops and do not require a driver to be used as a signature device. Wacom has more software that can be installed to customize the device further. See http://www.wacom.com/.
- Drawing tablets. Certain drawing input devices might present as an HID device on PCI/ACPI buses and are not supported. Attach these devices on a USB host controller on the client to be redirected inside a Citrix Virtual Desktops session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy rules take the format of tag=value expressions separated by whitespace. The following tags are supported:

Tag Name	Description
Mode	The optimization mode is supported for input devices for class=**03**. Supported modes are: No optimization - value **01**. Interactive mode - value **02**. Recommended for devices such as pen tablets and 3D Pro mice. Capture mode - value **04**. Preferred for devices such as signature pads.
VID	Vendor ID from the device descriptor, as a four-digit hexadecimal number.
PID	Product ID from the device descriptor, as a four-digit hexadecimal number.
REV	Revision ID from the device descriptor, as a four-digit hexadecimal number.
Class	Class from either the device descriptor or an interface descriptor.
SubClass	Subclass from either the device descriptor or an interface descriptor.
Prot	Protocol from either the device descriptor or an interface descriptor.

Examples

Mode=00000004 VID=067B PID=1230 class=03 #Input device operating in capture mode

Mode=00000002 VID=067B PID=1230 class=03 #Input device operating in interactive mode (default)

Mode=00000001 VID=067B PID=1230 class=03 #Input device operating without any optimization

Mode=00000100 VID=067B PID=1230 # Device setup optimization disabled (default)

Mode=00000200 VID=067B PID=1230 # Device setup optimization enabled

Disabling the screen saver for Wacom signature pad devices

For the use of Wacom signature pads and tablets, Citrix® recommends that you disable the screen saver as follows:

1. Install the **Wacom-STU-Driver** after redirecting the device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Install **Wacom-STU-Display MSI** to gain access to the signature pad control panel.
3. Go to **Control Panel > Wacom STU Display > STU430** or **STU530**, and select the tab for your model.
4. Choose **Change**, then select **Yes** when the UAC security window pops up.
5. Select **Disable slideshow**, then **Apply**.

After the setting is set for one signature pad model, it is applied to all models.

Client USB device redirection

This setting allows or prevents redirection of USB devices to and from the user device.

By default, USB devices are not redirected.

Client USB device redirection rules

This setting specifies the redirection rules for USB devices.

By default, no rules are specified.

When a user plugs in a USB device, the host device checks it against each policy rule in turn until a match is found. The first match for any device is considered definitive. If the first match is an Allow rule, the device is remoted to the virtual desktop. If the first match is a Deny rule, the device is available only to the local desktop. If no match is found, default rules are used.

Policy rules take the format {Allow: | Deny:} followed by a set of tag= value expressions separated by whitespace. The following tags are supported:

Tag Name	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
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, remember:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Rules are case-insensitive.
- Rules can have an optional comment at the end, introduced by #.
- Blank and pure comment lines are ignored.
- Tags must use the matching operator = (for example, VID=067B_.
- Each rule must start on a new line or form part of a semicolon-separated list.
- See the USB class codes available from the USB Implementers Forum, Inc. website.

Examples of administrator-defined USB policy rules:

- Allow: VID=067B PID=0007 # Another Industries, Another Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- To create a rule that denies all USB devices, use "DENY:"without other tags.

Client USB plug and play device redirection

This setting allows or prevents plug-and-play devices such as cameras or point-of-sale (POS) devices to be used in a client session.

By default, plug-and-play device redirection is allowed. When set to Allowed, all plug-and-play devices for a specific user or group are redirected. When set to Prohibited, no devices are redirected.

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.

> **Note:**
>
> In Receiver for Windows 4.2, USB devices are also automatically redirected when operating in Desktop Appliance mode. Also, the connection bar is not present. In earlier versions of Citrix Receiver for Windows, USB devices are also auto-redirected when operate in the following:
>
> - Desktop appliance mode
> - Virtual machine (VM) hosted applications

It is not always best to redirect all USB devices. Users can explicitly redirect devices from the USB device list that is not automatically redirected. To prevent USB devices from being listed or redirected, use DeviceRules on either the client endpoint or the DDC policy. See Administration Guides for further details.

> **Caution:**
>
> Using the Registry Editor incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

User preferences settings for auto redirection of USB devices

Policy:

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**.

Citrix Receiver:

1. Go to **Citrix Receiver Preferences > Connections**.
2. Ensure that the following options are selected:
    - When a session starts, connect devices automatically
    - When a new device is connected while a session is running, connect the device automatically.
3. Click **OK**.

All the registry keys and the policy changes are applied to the Windows client device.

Plain USB printers redirection

The best solution for plain USB printers is to use the dedicated Universal Printer Driver and virtual channel to perform printing. By default, plain USB printers are not automatically redirected.

Plain printers are detected using heuristics. Also, it is expected that advanced printers with scanning functions for example, might need to be redirected using USB support to work completely.

Use this registry to configure whether plain printers are automatically redirected:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectPrinters

Type: DWORD

Data: 00000000

The default value is 0 (does not automatically redirect). Changing the value to any number greater than zero enables USB support to redirect plain USB printers.

You can also deploy Active Directory policies to this registry key and override the non-policy value if both are present:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectPrinters

Type: DWORD

Data: 00000000

Plain audio devices redirection

Like plain printers, the best user experience is achieved using the dedicated audio virtual channel of ICA® to send audio data from plain audio devices. However, you might need to redirect some specialty devices using USB support. Heuristics are used to determine which devices are plain audio devices.

Use this registry on client endpoint to configure whether plain audio devices are automatically redirected:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectAudio

Type: DWORD

Data: 00000000

The default is set to 0 (does not automatically redirect). Changing the value to non-zero, redirects plain USB audio devices with USB support.

You can use Active Directory policies to deploy this value to the registry key and override the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectAudio

Type: DWORD

Data: 00000000

Plain storage devices (mass storage device) redirection

For plain storage devices, you achieve the best user experience using the dedicated virtual channel, such as client drive mapping that also performs optimization. In addition to simple reading or writing files, to perform certain special tasks like burning a CD/DVD or accessing encrypted file systems devices, the device might still need to be redirected using generic USB support.

Heuristics are used to determine which devices are plain storage devices. Use this registry key to configure whether plain storage devices are automatically redirected:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectStorage

Type: DWORD

Data: 00000000

The default is set to 0 (does not automatically redirect). Changing the value to non-zero, redirects plain USB storage devices using generic USB support.

You can also use Active Directory policies to deploy this value to the following registry key and override the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectStorage

Type: DWORD

Data: 00000000

> **Note:**
>
> Read only access to the plain storage device is not configurable if you are using generic USB support, while it is configurable if using CDM.

USB flash drives with hardware encryption redirection

USB flash drives with hardware encryption typically consist of an encrypted storage partition and a second *utility* partition that contains a utility for unlocking the encrypted partition. For USB Flash Drive devices, achieve the best user experience using the dedicated client drive mapping/dynamic thumb drive mapping HDX virtual channel that also performs optimization.

Generic USB redirection is necessary for the following:

- Non-Windows clients (for example, Linux clients)
- Clients where the customer has restricted (locked down) user access to local functions on the client

Generic USB redirection can redirect any USB storage device without hardware encryption into both Single-session OS and Multi-session OS VDA sessions.

Before Citrix Virtual Apps and Desktops 7 1808, USB flash drives with hardware encryption could not be redirected in any useful way into Single-session OS or Multi-session OS VDA sessions. A new feature enhancement introduced in Citrix Virtual Apps and Desktops 7 1808 supports generic USB redirection of USB flash drives with hardware encryption into Single-session OS and Multi-session OS VDA sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After the device is redirected, none of its drives appear on the local client. So, if unlocking the drive is required, perform it in the session. This feature requires Windows update KB4074590.

Plain still image devices (scanners and digital cameras)

For plain still image devices, achieve the best user experience using the dedicated virtual channel (such as the TWAIN virtual channel) that also performs optimization. These devices must adhere to industry standards. Consider that a device is non-compliant or it is not used according to the original intentions. In this case, generic USB redirection might be the only way to use the device. Heuristics are used to determine which devices are plain still image devices.

Use this registry key to configure whether plain still image devices are automatically redirected:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectImage

Type: DWORD

Data: 00000000

The default is set to 0 (does not automatically redirect). Changing the value to non-zero, redirects plain USB still image devices with generic USB.

You can also use Active Directory policies to deploy this value to this registry key and override the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectImage

Type: DWORD

Data: 00000000

Device specific settings

The heuristics used to select Citrix optimizable devices do not always match what you want. The examples for Citrix optimizable devices are printers, audio, video, storage, and still image devices. You might want to control automatic redirection of devices that are not listed above. You can control automatic redirection on a device specific basis.

As an example, the DemoTech 2,000 bar code reader doesn't need to be redirected using USB support. It has a vendor identifier of 12AB and a product identifier of 5678. These hexadecimal numbers can be found in Device Manager.

To prevent this being automatically redirected, create this device specific registry key:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Name: AutoRedirect

Type: DWORD

Data: 00000000

A value of 0 prevents the device from being automatically redirected. A non-zero value indicates that the device must be considered for automatic redirection (subject to user preferences). There is a single space character between the vendor and product identifiers.

You can also deploy this value using Active Directory policies to this registry key. It overrides the non-policy value if both are present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Name: AutoRedirect

Type: DWORD

Data: 00000000

Device specific AutoRedirect settings take precedence over the more general AutoRedirectXXX values explained above. The default heuristics for Citrix optimized devices might misinterpret a device as generic. Therefore, set the device specific AutoRedirect value to 1 to redirect it automatically.

Allow existing USB devices to be automatically connected

This setting allows or prevents the automatic connection of the existing USB devices that are connected to the endpoint at the start of a session to the remote session.

When adding this setting to a policy, select one of the following options:

- Ask before redirecting available USB devices.
- Do not automatically redirect available USB devices.
- Automatically redirect available USB devices.

By default, the **Ask before redirecting available USB devices** option is selected. Based on the policy selected, the option selected at the client's **Preferences** > **Devices** section can be overridden.

> **Note:**
>
> Currently, the **Allow existing USB devices to be automatically connected** policy is applicable only for Citrix Workspace™ app for Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allow newly arrived USB devices to be automatically connected

This setting allows or prevents the automatic connection of the USB devices that are inserted at the endpoint during a session to the remote session.

When adding this setting to a policy, select one of the following options:

- Ask before redirecting available USB devices.
- Do not automatically redirect available USB devices.
- Automatically redirect available USB devices.

By default, the **Ask before redirecting available USB devices** option is selected. Based on the policy selected, the option selected at the client's **Preferences** > **Devices** section can be overridden.

> **Note:**
>
> Currently, the **Allow newly arrived USB devices to be automatically connected** policy is applicable only for Citrix Workspace app for Windows.

Client USB device redirection rules (Version 2)

This setting specifies rules for filtering, splitting, and auto-connecting USB devices to a remote session.

When this setting is selected, the host overrides the *Client USB device redirection rules* setting with the device rules configured in this setting.

For more information, see Configuring composite USB device redirection.

Virtual channel allow list policy settings

September 6, 2025

The **Virtual channel allow list** policy setting enables the use of an allow list that specifies which virtual channels are allowed to be opened in an ICA® session.

When disabled, all virtual channels are allowed.

When enabled, only Citrix® virtual channels are allowed.

To use custom or third-party virtual channels, add the virtual channels to the list. To add a virtual channel to the list:

1. Enter the virtual channel name followed by a comma.
2. Enter the path to the process that accesses the virtual channel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More executable paths can be listed, and the paths are separated by commas.

For example,

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Starting with Citrix Virtual Apps and Desktops 7 2109, virtual channel allow lists are enabled by default. For more information on adding virtual channels to the allow list, see Adding virtual channels to the allow list

If you're using the HDX RealTime Optimization Pack for Skype for Business, add the virtual channel to the allow list. For more information, see the HDX RealTime Optimization Pack documentation.

> **Important:**
>
> The VDA machines must be rebooted for the setting to take effect.

For more information about virtual channels, see ICA virtual channels.

Virtual channel allow list logging

You can use this policy setting to configure the level for Virtual Channel Allow List logging.

The following options are available:

Options	Description
Disabled	Disables all log events.
Log warnings only	Events are logged only for custom Virtual Channels that try to open and that are not part of the allow list.
Log all events	All events are logged

Virtual channel allow list log throttling

You can use this policy setting to configure the frequency for logging events for an active session.

All events for each virtual channel will be logged on their first occurrence. Repeated events will be suppressed for the duration of the throttling period while the session is active. If a session is disconnected, the throttling period is reset.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual channel allow list for DVC

Enables the use of an allow list that specifies which dynamic virtual channels are allowed to be opened in an ICA session.

When disabled, all dynamic virtual channels are allowed.

When enabled, no dynamic virtual channels are allowed. To use dynamic virtual channels (DVC) with this feature, the DVCs must be added to the list. To add a DVC 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.

You may use a wildcard to allow all the listeners supported by the plugin.

You may also use a wildcard to replace a single directory name in the process path, part of a directory name in the process path, replace the executable's name, or replace part of the executable's name.

Changes to this setting will only apply after restarting the session host.

Example:
Client-side plugins: `DvcPlugin1.dll`, `DvcPlugin2.dll`, `DvcPlugin3.dll`

Allow list entry:

```
C:\Program Files\App\run1.2.exe,DvcPlugin1,ListenerName1
C:\Program Files\*\run*.exe,DvcPlugin2,ListenerName1,ListenerName2
C:\Program Files\App\run1.2.exe,DvcPlugin3,*
```

Visual display policy settings

September 6, 2025

The **Visual Display** section includes policy settings for controlling the quality of images that are sent from virtual desktops to the user device.

Preferred color depth for simple graphics

This policy setting is available in VDA versions 7.6 FP3 and later. The 8-bit option is available in VDA versions 7.12 and later.

This setting makes it possible to lower the color depth at which simple graphics are sent over the network. Lowering to 8-bit or 16-bit per pixel potentially improves responsiveness over low bandwidth connections. However, this action might cost slight degradation in image quality. The 8-bit color

© 1997–2026 Citrix Systems, Inc. All rights reserved.

depth is not supported when the Use video codec for compression policy setting is set to **For the entire screen**.

The default preferred color depth is 24-bits per pixel.

VDAs fall back to 24-bit (default) color depth if the 8-bit setting is applied on VDA version 7.11 and earlier.

Target frame rate

This setting specifies the maximum number of frames per second sent from the virtual desktop to the user device.

By default, the maximum is 30 frames per second.

Setting a high number of frames per second (for example, 30) improves the user experience, but requires more bandwidth. Decreasing the number of frames per second (for example, 10) maximizes server scalability at the expense of user experience. For user devices with slower CPUs, specify a lower value to improve the user experience.

The maximum supported frame rate per second is 60.

Visual quality

This setting specifies the desired visual quality for images displayed on the user device.

By default, this setting is Medium.

To specify the quality of images, choose one of the following options:

- **Low** - Recommended for bandwidth-constrained networks where visual quality can be sacrificed for interactivity
- **Medium** - Offers the best performance and bandwidth efficiency in most use cases
- **High** - Recommended if you require visually lossless image quality
- **Build to lossless** - Sends lossy images to the user device during periods of high network activity and lossless images after network activity reduces. This setting improves performance over bandwidth-constrained network connections
- **Always lossless** - When preserving image data is vital, select **Always lossless** to ensure that lossy data is never sent to the user device. For example, when displaying X-ray images where no loss of quality is acceptable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Moving images policy settings

May 5, 2025

The **Moving Images** section contains settings that enable you to remove or alter compression for dynamic images.

Minimum image quality

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting specifies the minimum acceptable image quality for Adaptive Display. The less compression used, the higher the quality of images displayed. Choose from Ultra High, Very High, High, Normal, or Low compression.

By default, this is set to Normal.

Moving image compression

This setting specifies whether or not Adaptive Display is enabled. Adaptive Display automatically adjusts the image quality of videos and transitional slides in slide shows based on available bandwidth. With Adaptive Display enabled, users should see smooth-running presentations with no reduction in quality.

By default, Adaptive Display is enabled.

For VDA versions 7.0 through 7.6, this setting applies only when Legacy graphics mode is enabled. For VDA versions 7.6 FP1 and later, this setting applies when Legacy graphics mode is enabled, or when the legacy graphics mode is disabled and a video codec is not used to compress graphics.

When legacy graphics mode is enabled, the session must be restarted before policy changes take effect. Adaptive Display is mutually exclusive with Progressive Display; enabling Adaptive Display disables Progressive Display and vice versa. However, both Progressive Display and Adaptive Display can be disabled at the same time. Progressive Display, as a legacy feature, is not recommended for XenApp or XenDesktop. Setting Progressive threshold Level will disable Adaptive Display.

Progressive compression level

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This setting provides a less detailed but faster initial display of images.

By default, no progressive compression is applied.

The more detailed image, defined by the normal lossy compression setting, appears when it becomes available. Use Very High or Ultra High compression for improved viewing of bandwidth-intensive graphics such as photographs.

For progressive compression to be effective, its compression level must be higher than the Lossy compression level setting.

Note: The increased level of compression associated with progressive compression also enhances the interactivity of dynamic images over client connections. The quality of a dynamic image, such as a rotating three-dimensional model, is temporarily decreased until the image stops moving, at which time the normal lossy compression setting is applied.

The following policy settings are related:

- Progressive compression threshold value
- Progressive heavyweight compression

Progressive compression threshold value

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection to which progressive compression is applied. This is applied only to client connections under this bandwidth.

By default, the threshold value is 2147483647 kilobits per second.

The following policy settings are related:

- Progressive compression threshold value
- Progressive heavyweight compression

Target minimum frame rate

This setting specifies the minimum frame rate per second the system attempts to maintain, for dynamic images, under low bandwidth conditions.

By default, this is set to 10fps.

For VDA versions 7.0 through 7.6, this setting applies only when Legacy graphics mode is enabled. For VDA versions 7.6 FP1 and later, this setting applies when the Legacy graphics mode is disabled or enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The target minimum framerate policy has been deprecated and is set to 10 fps. This can be changed by end users by using the Quality slider in the Graphic status indicator.

Still images policy settings

September 6, 2025

The **Still Images** section contains settings that enable you to remove or alter compression for static images.

Extra color compression

This setting enables or disables the use of extra color compression on images delivered over client connections that are limited in bandwidth, improving responsiveness by reducing the quality of displayed images.

By default, extra color compression is disabled.

When enabled, extra color compression is applied only when the client connection bandwidth is below the Extra color compression threshold value. When the client connection bandwidth is above the threshold value or Disabled is selected, extra color compression is not applied.

Extra color compression threshold

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection below which extra color compression is applied. If the client connection bandwidth drops below the set value, extra color compression, if enabled, is applied.

By default, the threshold value is 8192 kilobits per second.

Heavyweight compression

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This setting enables or disables reducing bandwidth beyond progressive compression without losing image quality by using a more advanced, but more CPU-intensive, graphical algorithm.

By default, heavyweight compression is disabled.

If enabled, heavyweight compression applies to all lossy compression settings. It is supported on Citrix Workspace™ app but has no effect on other plug-ins.

The following policy settings are related:

- Progressive compression level
- Progressive compression threshold value

Lossy compression level

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting controls the degree of lossy compression used on images delivered over client connections that are limited in bandwidth. In such cases, displaying images without compression can be slow.

By default, medium compression is selected.

For improved responsiveness with bandwidth-intensive images, use high compression. Where preserving image data is vital; for example, when displaying X-ray images where no loss of quality is acceptable, you may not want to use lossy compression.

Related policy setting: Lossy compression threshold value

Lossy compression threshold value

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection to which lossy compression is applied.

By default, the threshold value is 2147483647 kilobits per second.

Adding the Lossy compression level setting to a policy and including no specified threshold can improve the display speed of high-detail bitmaps, such as photographs, over a LAN.

Related policy setting: Lossy compression level

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WebSockets policy settings

September 6, 2025

The **WebSockets** section includes policy settings for accessing virtual desktops and hosted applications using the Citrix Workspace™ app for HTML5. The WebSockets feature increases security and reduces overhead by conducting two-way communication between browser-based applications and servers. The feature does so without opening multiple HTTP connections.

WebSockets connections

This setting allows or prohibits WebSockets connections.

By default, WebSocket connections are prohibited.

WebSockets port number

This setting identifies the port for incoming WebSocket connections.

By default, the value is 8008.

WebSockets trusted origin server list

This setting provides a comma-separated list of trusted origin servers, usually the Citrix Workspace app for Web, expressed as URLs. The server accepts only WebSockets connections originating from one of these addresses.

By default, the wildcard * is used to trust all Citrix Workspace app for Web URLs.

If you choose to type an address in the list, use this syntax:

<protocol>://<Fully qualified domain name of host>:[port]

The protocol must be HTTP or HTTPS. If the port is not specified, port 80 is used for HTTP and port 443 is used for HTTPS.

The wildcard * can be used within the URL, except as part of an IP address (`10.105.*.*`).

WIA devices policy settings

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **WIA devices** section includes policy settings for managing scanner redirection using Windows Image Acquisition (WIA).

WIA redirection

WIA devices, such as digital cameras and scanners, communicate with server-hosted image processing applications by using the WIA framework. This setting allows or prohibits users from accessing WIA devices on the user device. By default, WIA redirection is prohibited.

For information about WIA-compliant devices, see WIA devices.

HDX™ features managed through the registry

May 1, 2026

> **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 the Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

To open the Registry Editor, run `regedit.exe` on the server. Then navigate to the registry key to add or edit the settings.

Devices

Bloomberg keyboards

Citrix Virtual Apps and Desktops™ support the Bloomberg model 4 and model 3 starboard keyboard. By default, the support for the enhanced Bloomberg keyboard is disabled.

To enable support for the Bloomberg keyboard, set the following registry value on the client machine before you start a connection:

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **Value name**: `EnableBloombergHID`
- **Value type**: `DWORD`
- **Value data**:
  - `0` - Disable

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 1 - Enable

For more information, see Bloomberg keyboard.

Mapped client drives

As a security precaution, when a user logs in to Citrix Virtual Apps and Desktops, by default, the server maps client drives without user run permission. To enable users to run executable files residing on mapped client drives, override this default by editing the registry on the server.

To allow access, edit the following registry value (create **CDMSettings** if it doesn't exist):

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **Value name**: `ExecuteFromMappedDrive`
- **Value type**: `DWORD`
- **Value data**:
  - `1` - Allow permission
  - `0` - Deny permission on mapped drives

The change takes effect for sessions connected after you edit the registry.

Citrix Virtual Apps and Desktops 7 2006 is the first version to contain this registry location. Earlier versions of Citrix Virtual Apps and Desktops used a different registry location.

For more information, see Client Drive Mapping.

Microsoft Surface Pro and Surface Book pens

Citrix Virtual Apps and Desktops support standard pen functionality with Windows Ink-based applications. By default, this feature is enabled.

To disable or enable this feature, set the following registry value:

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **Value name**: `DisablePen`
- **Value type**: `DWORD`
- **Value data**:
  - `1` - Disable
  - `0` - Enable

For more information, see Microsoft Surface Pro and Surface Book pens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows Image Acquisition application allow list

This setting lets you control which applications on the VDA can access the Windows Image Acquisition scanner redirection.

By default, no applications have access to Windows Image Acquisition.

To adjust Windows Image Acquisition for applications on the VDA, create the following registry setting:

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **Value name**: `WIAAllowedProcesses`

  Select and right-click **WIAAllowedProcesses**. Choose **New > Multi-String Value** and rename the new value to **AllowProcesses**.
- Value data: Enter the full path and process name for each application that can access Windows Image Acquisition. Provide each application on a new line.

Any changes to this setting take effect the next time you launch a session on the VDA.

General

Secure Connection Port

When TLS/DTLS is enabled on the VDA, the default connection port number is 443. To change the port, modify the following registry value:

- **Key**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Value name**: `SSLPort`
- **Value type**: `DWORD`
- **Value data**: 443 (Decimal)

HDX Reducer

You can configure the version of the HDX compression algorithm (Reducer) that you want to use in the session host.

To enable Reducer V4 in a single-session VDA, set the following registry value:

Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings`

Value name: `ReducerOverrideMask`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Value type: DWORD
Value data: 23 (Decimal)

To enable Reducer V4 in a multi-session VDA, set the following registry value:

- **Key**: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- **Value name**: ReducerOverrideMask
- **Value type**: DWORD
- **Value data**: 23 (Decimal)

Configure Rendezvous version

To configure the version of Rendezvous to use, set the following registry value:

- **Key**: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
- **Value type**: DWORD
- **Value name**: GctRegistration
- **Value data**:
  - 1 - To enable V2
  - 0 - To enable V1

Configure automatic logon to the VDA

This setting lets you enable or disable the **Always prompt for password** Microsoft policy setting on the Windows 10 single-session OS and multi-session OS VDAs.

If **Always prompt for password** is enabled, users must enter credentials on the VDA when they start a remote session. If this setting is disabled, users automatically connect to the remote session without providing credentials on the VDA.

By default, the Microsoft policy setting is disabled. To enable or disable the **Always prompt for password** setting, set the following registry value on the VDA:

- **Key**: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- **Value name**: AutoLogon
- **Value type**: DWORD
- **Value data**:
  - 1 - Disables the Microsoft policy setting and lets users automatically sign in to a remote session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `0` –Enables the Microsoft policy setting and prompts users to provide credentials when they launch a remote session.

Disable timeout warning

By default, users with inactive or idle sessions receive a warning message two minutes before their session automatically disconnects.

This setting disables and removes the warning message for users reaching the idle session timeout limit on the following:

- Windows Server 2004
- Windows 10 multi-session 2004 or later multi-session OS

To remove the warning, set the following registry value on the VDA:

- **Key**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **Value name**: `fEnableTimeoutWarning`
- **Value type**: `DWORD`
- **Value data**:
  - `1` - Disable the warning message
  - `0` - Enable the warning message

To display the warning message, delete the registry value or set it to `0`.

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.

This setting is enabled by default. To disable EDT MTU Discovery, configure the following registry value and restart the session host:

- **Key**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Value name**: `MtuDiscovery`
- **Value type**: `DWORD`
- **Value data**: `0`

To enable MTU Rediscovery, configure the following registry values and restart the session host:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Key:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery
- **Value name:** MtuReDiscovery
- **Value type:** DWORD
- **Value data:** 1
- **Key:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery
- **Value name:** MtuReDiscoveryFrequency
- **Value type:** DWORD
- **Value data:** 1

These settings are machine-wide and affect all sessions connecting from a supported client.

EDT timeout

You can set the EDT timeout in the VDA to any value between 5 and 25 seconds. The default EDT timeout value is 10 seconds.

- **Key**: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters
- **Value type**: DWORD
- **Value name**: edtConnectionTimeout
- **Value data**: time in seconds between 5 and 25 (decimal)

You can also set the EDT timeout for Citrix Workspace app for Windows version 2409.10 and older:

- **Key**: HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT
- **Value type**: String / REG_SZ
- **Value name**: edtConnectionTimeout
- **Value data**: time in seconds between 5 and 25 (decimal)

> **NOTE:**
>
> The timeout setting from the VDA will be used by Citrix Workspace app starting with version 2503, eliminating the need to configure the timeout on the client device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

General content redirection

Add URL types for host to client redirection

By default, we support redirection of the following URL types: HTTP, HTTPS, RTSP, RTSPU, PNM, and MMS. You can add URL types to the list by creating the following registry keys and values on the Windows client.

- **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 this registry setting reject redirection back to the Citrix session. The client must have an application installed and configured to handle the specified URL types.

For more information, see Host to client redirection.

Client folder redirection

Client folder redirection changes the way client-side files are accessible on the host-side session. Consider that you enable client folder redirection on the server and the user configures it on the user device. In this case, the portion of the local volume specified by the user is redirected.

To enable client folder redirection on the server, set the following registry value:

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **Value name**: `CFROnlyModeAvailable`
- **Value type**: `DWORD`
- **Value data**: `1`

For more information, see Client folder redirection.

Host to client redirection for a specific set of websites

To enable host to client redirection for a specific set of websites, set the following registry value on the server VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.example.com

*.example.com

For more information, see Host to client redirection.

Local application behavior on logoff and disconnect

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, set the following registry value in the hosted desktop:

- **Key**: HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies
- **Value name**: Session State
- **Value type**: DWORD
- **Value data**:
  - 1 - Local applications continue to run when a user logs off or disconnects from the virtual desktop. Upon reconnection, local applications are reintegrated if they are available on the virtual desktop.
  - 3 - Local applications close when a user logs off or disconnects from the virtual desktop.

For more information, see Local App Access and URL redirection.

Remove URL types from the default list for host to client redirection

To remove URL types from the default redirection list, create the following registry keys and values on the server VDA.

- **Key**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- **Value name**: DisableServerFTA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Value type**: DWORD
- **Value data**: 1
- **Value name**: NoRedirectClasses
- **Value type**: REG_MULTI_SZ
- **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
```

For more information, see Host to client redirection.

Server VDA default browser configuration

You can enable host to client redirection to supersede any 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.

- Internet Explorer (Default)
  - **Key**: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - **Value name**: Default
  - **Value type**: REG_SZ
  - **Value data**: "c:\program files\internet explorer\iexplore.exe""%1"
  - **Key**: HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - **Value name**: Default
  - **Value type**: REG_SZ
  - **Value data**: "c:\program files\internet explorer\iexplore.exe""%1"
- Google Chrome
  - **Key**: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - **Value name**: Default
  - **Value type**: REG_SZ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Value data**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`
    - **Key**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
    - **Value name**: `Default`
    - **Value type**: `REG_SZ`
    - **Value data**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`
- Microsoft Edge
    - **Key**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
    - **Value name**: `Default`
    - **Value type**: `REG_SZ`
    - **Value data**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`
    - **Key**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
    - **Value name**: `Default`
    - **Value type**: `REG_SZ`
    - **Value data**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`

The Local App Access for published applications

Local App Access seamlessly integrates locally installed Windows applications into a hosted desktop environment without switching from one desktop to another. To provide access to published applications, set the following registry value on the server:

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **Value name**: `ClientHostedAppsEnabled`
- **Value type**: `DWORD`
- **Value data**:
    - `1` - Enable
    - `0` - Disable

For more information, see Local App Access and URL redirection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Graphics

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 following registry setting:

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **Value name**: `CUDA`
- **Value type**: `DWORD`
- **Value data**: `00000001`

To use the OpenCL acceleration POC features, enable the following registry setting:

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **Value name**: `OpenCL`
- **Value type**: `DWORD`
- **Value data**: `00000001`

For more information, see GPU acceleration for Windows multi-session OS

Progressive mode

Progressive mode is disabled by default. You can change the progressive mode state with the following registry value:

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **Value type**: `REG_DWORD`
- **Value name**: `ProgressiveDisplay`
- **Value data**:
  - `0` - Always off (Disables progressive mode. This value is the default.)
  - `1` - Automatic (Toggle based on network conditions.)
  - 2 = Always on

For more information, see Progressive mode.

> **Note:**
>
> Progressive mode has been deprecated. Thinwire is an alternative option that optimizes image

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> delivery and maintains cache efficiency while providing nearly all of the benefits of the progressive mode.

Windows Presentation Foundation (WPF) rendering

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 Windows Presentation Foundation (WPF) rendering to the server's GPU, graphics rendering does not slow the server's CPU.

To enable WPF application rendering using the server's GPU, create the following setting in the registry of the server running Windows multi-session OS:

1. Open the Registry Editor on the VDA and go to the following key:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. Create or edit the following registry values:

   - [REG_DWORD] AdapterHandle = 0x00000001
   - [REG_DWORD] DevicePath = 0x00000001
   - [REG_DWORD] Flag = 0x00000412
   - [REG_DWORD] WPF = 0x00000001

3. Create a sub-key with the executable name of your WPF app. For example, if your app is called "mywpfapp.exe", create the following key:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`

4. Reboot the server for the setting to take effect.

For more information, see GPU acceleration for Windows multi-session OS and the blog on Getting the best out of WPF apps on Windows multi-session OS.

Multimedia

Avoid echo during multimedia conferences

Citrix Virtual Apps and Desktops provide an echo cancellation option that minimizes any echo. This feature is enabled by default. To disable echo cancellation, you can change one of the following registry settings:

- **Key**:
  - 32-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 64-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio

- **Value name**: EchoCancellation
- **Value type**: String/REG_SZ
- **Value data**: False

For more information, see Audio features.

Audio 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 following registry key on the RDS machine and then restart the machine:

- **Key**: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig
- **Value name**: EnableSvchostMitigationPolicy
- **Value type**: DWORD
- **Value data**: 0

For more information, see Audio features.

High-definition webcam resolution

If the media type negotiation fails, HDX falls back to the default VGA resolution (640 x 480 pixels). You can use registry keys on the client to configure the default resolution. Before setting the following registry keys, ensure that the camera supports the specified resolution.

- **Key**: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Width
    - **Value name**: DefaultWidth
    - **Value type**: DWORD
    - **Value data**: desired width in decimal (for example: 1280)
- Height
    - **Value name**: DefaultHeight
    - **Value type**: DWORD
    - **Value data**: desired height in decimal (for example 720)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Teams 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, such as webcam redirection and client audio and microphone redirection. If you are using a Workspace app version/platform OS that does not support Microsoft Teams optimization, fallback registry keys do not apply.

To control the fallback mechanism, set one of the following registry values on the VDA:

- **Key** (only one needed):
  - **Computer setting:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **User setting:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`
- **Value name**: `DisableFallback`
- **Value type**: `DWORD`
- Value data:
  - 1 - Disable fallback mode
  - 2 - Enable audio only

If the value isn't present or is set to 0, fallback mode is enabled. This feature requires Microsoft Teams version 1.3.0.13565 or later. For more information, see Optimization for Microsoft Teams.

Optimization for Microsoft Teams with Citrix App Layering™

If using Citrix App Layering to manage VDA and Microsoft Teams installations in different layers, create an empty registry key named **PortICA** on Windows before installing Microsoft Teams with the `ALLUSER=1` flag from the command line. Leave the default value name, type, and data.

- Key for 32-bit Version of Registry Editor: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- Key for 64-bit Version of Registry Editor: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

For more information, see Optimization for Microsoft Teams.

Webcam software compression

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 values to the client:

- **Key**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Value name**: `DeepCompress_ForceSWEncode`
- **Value type**: `DWORD`
- **Value data**: `1`

For more information, see HDX webcam video compression.

Webcam video compression

HDX webcam video compression sends the H.264 video directly to the video conferencing application running in 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 following registry value in the VDA.

- **Key**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **Value name**: `OfferH264ToApp`
- **Value type**: `DWORD`
- **Value data**: `0`

For more information, see HDX webcam video compression.

Webcam video compression frame rate

To adjust the preferred video frame rate, edit the following registry value on the client:

- **Key**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **Value name**: `FramesPerSecond`
- **Value type**: `DWORD`
- **Value data**: `15`

If the webcam doesn't support the specified frame rate, the application uses 15 FPS by default.

For more information, see HDX webcam video compression.

Load management policy settings

May 5, 2025

The **Load Management** section includes policy settings for enabling and configuring load management between servers delivering Windows Multi-session OS machines.

For information about calculating the load evaluator index, see CTX202150.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Concurrent logon tolerance

This setting specifies the maximum number of concurrent logons that a server can accept.

By default, this value is set to 2.

When this setting is enabled, load balancing tries to avoid having more than the specified number of logons active on a Server VDA at the same time. However, the limit is not strictly enforced. To enforce the limit (and cause concurrent logons that exceed the specified number to fail), create the following registry key:

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
> Type: DWORD
> Value: 1

CPU usage

This setting specifies the level of CPU usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and CPU usage is excluded from load calculations.

CPU usage excluded process priority

> **Note:**
>
> In scenarios where Workspace Environment Management manages machines, using this setting along with the CPU Priority settings can have unintended results. We recommend that you disable this setting if you choose to use the CPU Priority settings.

This setting specifies the priority level at which a process'CPU usage is excluded from the CPU Usage load index.

By default, this value is set to **Below Normal** or **Low**.

Disk usage

This setting specifies the disk queue length at which the server reports a 75% full load. When enabled, the default value for disk queue length is 8.

By default, this setting is disabled and disk usage is excluded from load calculations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Maximum number of sessions

This setting specifies the maximum number of sessions a server can host. When enabled, the default setting for the maximum number of sessions a server can host is 250.

By default, this setting is enabled.

Memory usage

This setting specifies the level of memory usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and memory usage is excluded from load calculations.

Memory usage base load

This setting specifies an approximation of the base operating system's memory usage. Also, defines, in MB, the memory usage below which a server is considered to have zero load.

By default, this value is set to 768 MB.

Profile Management policy settings

May 5, 2025

This section contains policy settings for enabling and configuring Profile Management.

For other information, such as the following, see Profile Management policies:

- Names of the equivalent .ini file setting
- Which version of Profile Management is required for a policy setting

Advanced policy settings

November 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Number of retries when accessing locked files

Sets the number of retries when accessing locked files.

If this policy is disabled, the default value of five retries is used. If this policy isn't configured here, the value from the .ini file is used. If this policy isn't configured here or in the .ini file, the default value is used.

Process Internet cookie files on logoff

Some deployments leave extra Internet cookies that `Index.dat` does not reference. The extra cookies left in the file system after sustained browsing can lead to profile bloat. This policy lets you enable Profile Management to force processing of Index.dat and remove the extra cookies. The policy increases logoff times, so enable it only after you experience this issue.

Configuration precedence:

1. If this policy isn't configured here, the value from the .ini file is used.
2. If this policy isn't configured here or in the .ini file, no processing of Index.dat takes place.

Disable automatic configuration

Profile Management examines any Citrix Virtual Desktops™ environment, for example for the presence of personal vDisks, and configures Group Policy accordingly. Only Profile Management policies in the Not Configured state are adjusted, so any customizations you have made are preserved.

This policy lets you speed up deployment and simplifies optimization. You do not need to configure this policy. However, you can disable automatic configuration when doing one of the following:

- Upgrading to retain settings from earlier versions
- Troubleshooting

You can regard automatic configuration as a dynamic configuration checker that automatically configures the default policy settings according to environments at runtime. It eliminates the need to configure the settings manually. Runtime environments include:

- Windows OS
- Windows OS versions
- Presence of Citrix Virtual Desktops
- Presence of personal vDisks

Automatic configuration might change the following policies if the environment changes:

- Active write-back

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Always cache
- Delete locally cached profiles on logoff
- Delay before deleting cached profiles
- Profile streaming

See the following table for the default status of the policies on different OSs:

	Multi-session OS	Single-session OS
Active write back	Enabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.
Always cache	Disabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.
Delete locally cached profiles on logoff	Enabled	*Disabled* if one of the following situations occurs: Personal vDisk is in use, Citrix Virtual Desktops is assigned, or Citrix Virtual Desktops isn't installed; otherwise, enabled.
Delay before deleting cached profiles	0 seconds	60 seconds if user changes are not persistent; otherwise, 0 seconds.
Profile streaming	Enabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.

However, with automatic configuration disabled, all policies above default to **Disabled**.

> **Important:**
>
> Personal vDisk is deprecated. For details, see Remove PVD, AppDisks, and unsupported hosts.

Starting with Profile Management 1909, you can have an improved experience with the Start menu on Windows 10 (version 1607 and later). This improvement is achieved through automatic configuration of the following policies:

- Add `Appdata\Local\Microsoft\Windows\Caches` and `Appdata\Local\Packages` to **Folders to Mirror**.
- Add `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` to **Files to synchronize**.

Configuration precedence:

1. If this setting isn't configured here, the value from the .ini file is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. If this setting isn't configured here or in the .ini file, automatic configuration is turned on. In this case, Profile Management settings might change if the environment changes.

Log off user if a problem is encountered

Lets you specify whether Profile Management logs off users if a problem is encountered.

If this policy is disabled or not configured, Profile Management gives a temporary profile to users if a problem is encountered. For example, the user store is unavailable.

If it is enabled, an error message is displayed and users are logged off. This setup can simplify troubleshooting of the problem.

Configuration precedence:

1. If this setting isn't configured here, the value from the .ini file is used.
2. If this setting isn't configured here or in the .ini file, a temporary profile is provided.

Customer Experience Improvement Program

By default, the Customer Experience Improvement Program is enabled to help improve the quality and performance of Citrix® products by collecting anonymous statistics and usage data.

If this setting isn't configured here, the value from the .ini file is used.

Enable search index roaming for Outlook

Allow user-based Outlook search experience by automatically roaming Outlook search data along with user profile. This feature requires extra spaces in the user store to store search indexes for Outlook.

Log off and then log on again for this policy to take effect.

Outlook search index database –backup and restore

Lets you specify what Profile Management does during logon when the Enable search index roaming for Outlook policy is enabled.

If this policy is enabled, Profile Management backs up the search index database each time the database is mounted successfully on logon. Profile Management treats the backup as the good copy of the search index database. When an attempt to mount the search index database fails due to database corruption, Profile Management reverts the search index database to the last-known good copy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Note:
>
> Profile Management deletes the previously saved backup after a new backup is saved successfully. The backup consumes the available VHDX storage.

Enable concurrent session support for Outlook search data roaming

Lets Profile Management provide native Outlook search experience in concurrent sessions of the same user. Use this policy with the Search index roaming for Outlook policy.

With this policy enabled, each concurrent session uses a separate Outlook OST file.

By default, only two VHDX disks can be used to store Outlook OST files (one file per disk). If the user starts more sessions, their Outlook OST files are stored in the local user profile. You can specify the maximum number of VHDX disks for storing Outlook OST files.

Enable OneDrive container

Lets OneDrive folders roam with users.

The OneDrive container is a VHDX-based folder roaming solution. Profile Management creates a VHDX file per user on a file share and stores the users' OneDrive folders into the VHDX files. The VHDX files are attached when users log on and detached when users log off.

UWP app roaming

Lets you enable UWP (Universal Windows Platform) apps to roam with users. As a result, users can access the same UWP apps from different devices.

With this policy enabled, Profile Management lets UWP apps roam with users by storing the apps on separate VHDX disks. Those disks are attached during user logons and detached during user logoffs.

Configuration precedence:

1. If this setting isn't configured here, the value from the .ini file is used.
2. If this setting isn't configured here or in the .ini file, this feature is disabled.

Enable UWP app load acceleration

Enable UWP app load acceleration. Lets you accelerate the loading of UWP apps and improve their consistency in non-persistent environments. By default, Windows stores UWP App registration information locally on each machine, which can be lost upon restart in non-persistent environments. With

© 1997–2026 Citrix Systems, Inc. All rights reserved.

this policy enabled, Profile Management creates a VHDX container for each machine to store the UWP app registration data, speeding up user logon and preventing data loss on restarts.

Configuration precedence:

1. If this setting isn't configured using a GPO, Studio, or Workspace Experience Management (WEM), the value from the .ini file is used.
2. If this setting isn't configured anywhere, this feature is disabled.

Enable asynchronous processing for user Group Policy on logon

Windows provides two processing modes for user Group Policy: synchronous and asynchronous. Windows uses a registry value to determine the processing mode for the next user logon. If the registry value doesn't exist, synchronous mode is applied. The registry value is a machine-level setting and doesn't roam with users. Thus, asynchronous mode will not be applied as expected if users:

- Log on to different machines.
- Log on to the same machine where the Delete locally cached profiles on logoff policy is enabled.

With this policy enabled, the registry value roams with users. As a result, processing mode is applied each time users log on.

Free space ratio to trigger VHD disk compaction

Applicable when Enable VHD disk compaction is enabled. Lets you specify the free space ratio to trigger VHD disk compaction. When the free space ratio exceeds the specified value on user logoff, disk compaction is triggered.

Free space ratio = (current VHD file size –required minimum VHD file size*) ÷ current VHD file size

* Obtained using the GetSupportedSize method of the `MSFT_Partition` class from the Microsoft Windows operating system.

Number of logoffs to trigger VHD disk compaction

Applicable when Enable VHD disk compaction is enabled. Lets you specify the number of user logoffs to trigger VHD disk compaction.

When the number of logoffs since the last compaction reaches the specified value, disk compaction is triggered again.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disable defragmentation for VHD disk compaction

Applicable when Enable VHD disk compaction is enabled. Lets you specify whether to disable file defragmentation for VHD disk compaction.

When VHD disk compaction is enabled, the VHD disk file is first automatically defragmented using the Windows built-in `defrag` tool, and then compacted. VHD disk defragmentation produces better compaction results while disabling it can save system resources.

Enable multi-session write-back for profile containers

Enables write-back for profile containers in multi-session scenarios. If enabled, changes in all sessions are written back to profile containers. Otherwise, only changes in the first session are saved because only the first session is in read/write mode in profile containers. Citrix Profile Management profile containers are supported starting with Citrix Profile Management 2103. FSLogix Profile Container is supported starting with Citrix Profile Management 2003.

To use this policy for the FSLogix Profile Container, ensure that the following prerequisites are met:

- The FSLogix Profile Container feature is installed and enabled.
- The profile type is set to **Try for read-write profile and fallback to read-only** in FSLogix.

Replicate user stores

Lets you replicate the remote user profile store to multiple paths on each logon and logoff. Doing so lets Profile Management provide profile redundancy for user logons.

Enabling the policy increases system I/O and might prolong logoffs.

> **Note:**
>
> This feature is available for both the file-based and container-based profile solutions.

Enable credential-based access to user stores

By default, Citrix Profile Management impersonates the current user to access the user store. Enable this feature if you do not want Profile Management to impersonate the current user when accessing the user store. You can put user stores in storage repositories (for example, Azure Files) that the current user has no permission to access.

To ensure that Profile Management can access user stores, save the profile storage server's credentials in Workspace Environment Management™ (WEM) or Windows Credential Manager. We recommend

© 1997–2026 Citrix Systems, Inc. All rights reserved.

you use Workspace Environment Management to eliminate the need of configuring the same credentials for each machine where Profile Management runs. If you use the Windows Credential Manager, use the Local System account to securely save the credentials.

> **Note:**
>
> This policy is available both for file-based and VHDX-based user stores. For Profile Management versions earlier than 2212, this policy is available only for VHDX-based user stores.

Configuration precedence:

1. If this setting isn't configured here, the value from the .ini file is used.
2. If this setting isn't configured here or in the .ini file, it is disabled by default.

Customize storage path for VHDX files

Profile Management provides the following VHDX-based policies: Profile container, Search index roaming for Outlook, and Accelerate folder mirroring. By default, VHDX files are stored in the user store. This policy lets you specify a separate path to store them.

Default capacity of VHD containers

Lets you specify the default storage capacity (in GB) of VHD containers.

Configuration precedence:

1. If this policy isn't configured here, the value from the .ini file is used.
2. If this policy isn't configured here or in the .ini file, the default is 50 (GB).

Automatically reattach VHDX disks in sessions

With this policy enabled, Profile Management ensures a high level of stability of VHDX-based policies. By default, this policy is enabled.

When this policy is enabled, Profile Management monitors VHDX disks that are in use by VHDX-based policies. If any of the disks is detached, Profile Management reattaches the disk automatically.

Profile container auto-expansion threshold

Lets you specify the utilization percentage of storage capacity at which profile containers trigger auto-expansion.

Configuration precedence:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If this policy isn't configured here, the value from the .ini file is used.
- If this policy isn't configured here or in the .ini file, the default is 90 (%) of storage capacity.

Profile container auto-expansion increment

Lets you specify the amount of storage capacity (in GB) by which profile containers automatically expand when auto-expansion is triggered.

Configuration precedence:

- If this policy isn't configured here, the value from the .ini file is used.
- If this policy isn't configured here or in the .ini file, the default is 10 (GB).

Profile container auto-expansion limit

Lets you specify the maximum storage capacity (in GB) to which profile containers can automatically expand when auto-expansion is triggered.

Configuration precedence:

- If this policy isn't configured here, the value from the .ini file is used.
- If this policy isn't configured here or in the .ini file, the default is 80 (GB).

Enable user-level policy settings

With this policy enabled, machine-level policy settings can work at the user level, and user-level settings override machine-level settings.

Configuration precedence:

1. If this policy isn't configured here, the value from the .ini file is used.
2. If this policy isn't configured here or in the .ini file, it is disabled.

Set priority order for user groups

Lets you specify the priority order for user groups. The order determines which group takes precedence when a user belongs to multiple groups with different policy settings.

When a user belongs to multiple groups with conflicting policy settings, consider the following:

- If the user belongs to one or more groups defined in this policy, the group with the highest priority takes precedence.
- If the user doesn't belong to any of the groups defined in this policy, the group with the SID listed earliest in alphabetical order takes precedence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User store selection method

Lets you specify the user store selection method when multiple user stores are available. Options include:

- **Configuration order.** Profile Management selects the earliest configured store.
- **Access performance.** Profile Management selects the store with the best access performance.

Configuration precedence:

1. If this setting isn't configured here, the value from the .ini file is used.
2. If this setting isn't configured here or in the .ini file, **Configuration order** is used.

Enable in-session profile container failover among user stores

By default, when multiple user stores are deployed, profile container failover occurs only at user logon. As a result, profile redundancy is available only at user logon. This policy lets you expand the failover scope to the entire session, ensuring profile redundancy throughout the session. With the policy enabled, if Profile Management loses connection to the active profile container during a session, it automatically switches to another available one.

Configuration precedence:

1. If this policy isn't configured here, the value from the .ini file is used.
2. If this policy isn't configured here or in the .ini file, the setting is disabled.

Profile load timeout

Lets you enable the profile load timeout feature and configure the timeout duration. Citrix Profile Management waits for the specified timeout for a user profile to load before switching to a temporary profile.
By default, the **Profile load timeout** setting is 45 seconds, with a valid range of 0–1800 seconds. To bypass profile loading and use a temporary profile, set the timeout to 0 seconds.

Configuration precedence:

1. If this policy isn't configured here, the value from the .ini file is used.
2. If this policy isn't configured either here or in the .ini file, the policy is disabled by default.

Limit profile synchronization during logoff

Lets you specify how many user stores are synced on user logoff.
By default, Citrix Profile Management syncs all user stores during logoff, and the logoff isn't completed

© 1997–2026 Citrix Systems, Inc. All rights reserved.

until the profile has been synced across all stores.
Reducing the number of stores synced speeds up logoff. For non-persistent machines, the unsynced stores will be updated during the next user session while for persistent machines, the unsynced stores will be synced in the background.

Configuration precedence:

1. If this policy is not configured here, the value from the .ini file is used.
2. If this policy is not configured either here or in the .ini file, the policy is disabled by default.\n\nNote: This setting applies only when the Replicate user stores policy is enabled.

Notify user when profile size exceeds quota

Lets you set a quota for the user profile and notify users when their profile size exceeds it.

Configuration precedence:

1. If this policy isn't configured here, the value from the .ini file is used.
2. If this policy isn't configured here or in the .ini file, the setting is disabled.

Notification message when profile size exceeds quota

Applicable when the **Notify user when profile size exceeds quota** policy is enabled. Lets you set the notification message users receive.

Configuration precedence:

1. If this policy isn't configured here, the value from the .ini file is used.
2. If this policy isn't configured here or in the .ini file, the setting is disabled.

Basic policy settings

September 6, 2025

This section contains policy settings relating to the basic configuration of Profile Management.

Enable Profile Management

By default, to facilitate deployment, Profile Management does not process logons or logoffs. Enable Profile Management only after carrying out all other setup tasks and testing how Citrix® user profiles perform in your environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, Profile Management does not process Windows user profiles in any way.

Processed groups

Both computer-local groups and domain groups (local, global, and universal) can be used. Domain groups must be specified in the format: DOMAIN NAME\GROUP NAME.

If this policy is configured here, Profile Management processes only members of these user groups. If this policy is disabled, Profile Management processes all users. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, members of all user groups are processed.

Excluded groups

You can use computer local groups and domain groups (local, global, and universal) to prevent particular user profiles from being processed. Specify domain groups in the form DOMAIN NAME\ GROUP NAME.

If this setting is configured here, Profile Management excludes members of these user groups. If this setting is disabled, Profile Management does not exclude any users. If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no members of any groups are excluded.

Process logons of local administrators

Specifies whether logons of members of the BUILTIN\Administrators group are processed. Consider this policy is disabled or not configured on multi-session operating systems, such as Citrix Virtual Apps environments. In this case, Profile Management assumes that logons by domain users, but not local administrators, must be processed. On single-session operating systems (such as Citrix Virtual Desktops environments), local administrator logons are processed. This policy allows domain users with local administrator rights, typically Citrix Virtual Desktops users with assigned virtual desktops, to:

- Bypass any processing
- Log on
- Troubleshoot the desktop-experiencing problems with Profile Management

Note: Domain users' logons might be subject to restrictions imposed by group membership, typically to ensure compliance with product licensing.
If this policy is disabled, Profile Management does not process logons by local administrators. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, administrators are not processed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Path to user store

Sets the path to the directory (the user store) in which the user settings (registry changes and synchronized files) are saved.

The path can be:

- A relative path. It must be relative to the home directory (which is typically configured as the #homeDirectory# attribute for a user in the Active Directory).
- A UNC path. It typically specifies a server share or a DFS namespace.
- Disabled or unconfigured. In this case, a value of #homeDirectory#\Windows is assumed.

The following types of variables can be used for this policy:

- System environment variables enclosed in percent signs (for example, %ProfVer%). System environment variables generally require extra setup.
- Attributes of the Active Directory user object enclosed in hashes (for example, #sAMAccountName#).
- Profile Management variables. For more information, see the Profile Management variables product document.

User environment variables cannot be used, except for %username% and %userdomain%. You can also create custom attributes to define organizational variables such as location or users fully. Attributes are case-sensitive.

Examples:

- \server\share#sAMAccountName# stores the user settings to the UNC path \server\share\JohnSmith (if #sAMAccountName# resolves to JohnSmith for the current user)
- \server\profiles$\%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS! might expand to \server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64

Important: Whichever attributes or variables you use, check that this policy expands to the folder one level higher than the folder containing NTUSER.DAT. For example, if this file is contained in \server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile, set the path to the user store as \server\profiles$\JohnSmith.Finance\Win8x64 (not the \UPM_Profile subfolder).

For more information on using variables when specifying the path to the user store, see the following topics:

- Share Citrix user profiles on multiple file servers
- Administer profiles within and across OUs
- High availability and disaster recovery with Profile Management

If Path to user store is disabled, the user settings are saved in the Windows subdirectory of the home directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If this policy is disabled, the user settings are saved in the Windows subdirectory of the home directory. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the Windows directory on the home drive is used.

Migrate user store

Specifies the path to the folder where the user settings (registry changes and synchronized files) were previously saved (the user store path that you previously used).

If this setting is configured, the user settings that are stored in the previous user store are migrated to the current user store specified in the "Path to user store"policy.

The path can be an absolute UNC path or a path relative to the home directory.

In both cases, you can use the following types of variables:

- System environment variables enclosed in percent signs
- Attributes of the Active Directory user object enclosed in hash signs

Examples:

- The folder `Windows\\%ProfileVer%` stores the user settings in a subfolder called `Windows\W2K3` of the user store (if %ProfileVer% is a system environment variable that resolves to W2K3).
- `\\server\share\\#SAMAccountName#` stores the user settings to the UNC path `\\server\share\<JohnSmith>` (if `#SAMAccountName#` resolves to JohnSmith for the current user).

In the path, you can use user environment variables except `%username%` and `%userdomain%`.

If this setting is disabled, the user settings are saved in the current user store.

If this setting is not configured here, the corresponding setting from the .ini file is used.

If this setting is not configured here or in the .ini file, the user settings are saved in the current user store.

Active write back

Files and folders (but not registry entries) that are modified can be synchronized to the user store in the middle of a session, before logoff.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, it is enabled.

Offline profile support

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This policy allows profiles to synchronize with the user store at the earliest possible opportunity. It is aimed at laptop or mobile device users who roam. When a network disconnection occurs, profiles remain intact on the laptop or device even after rebooting or hibernating. As mobile users work, their profiles are updated locally. Also, eventually synchronized with the user store when the network connection is re-established.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, offline profiles are disabled.

Active write back registry

Use this policy along with "Active write back."Registry entries that are modified can be synchronized to the user store in the middle of a session.

If you do not configure this setting here, the value from the .ini file is used.

If you do not configure this setting here or in the .ini file, the active write back registry is disabled.

Active write back on session lock and disconnection

With both this policy and the **Active write back** policy enabled, profile files and folders are written back only when a session is locked or disconnected.

With this policy and both the **Active write back** and **Active write back registry** policies enabled, registry entries are written back only when a session is locked or disconnected.

Offline profile support

Enables the offline profiles feature. This feature is intended for computers that are commonly removed from networks. For example, laptops or mobile devices not servers or desktops.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, offline profile support is disabled.

Cross-platform policy settings

September 6, 2025

This section contains policy settings relating to configuring the **Profile Management cross-platform** settings feature.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable cross-platform settings

By default, to facilitate deployment, cross-platform settings are disabled. Turn on processing by enabling this policy but only after thorough planning and testing of this feature.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no cross-platform settings are applied.

Cross-platform settings user groups

Enter one or more Windows user groups. For example, you might use this policy to process only the profiles from a test user group. If this policy is configured, the cross-platform settings feature of Profile Management processes only members of these user groups. If this policy is disabled, the feature processes all users specified by the Processed groups policy.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, all user groups are processed.

Path to cross-platform definitions

Identifies the network location of the definition files that you copied from the download package. This path must be a UNC path. Users must have read access to this location, and administrators must have write access to it. The location must be a Server Message Block (SMB) or Common Internet File System (CIFS) file share.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no cross-platform settings are applied.

Path to cross-platform settings store

Sets the path to the cross-platform settings store, the folder in which users'cross-platform settings are saved. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory.

This area is the common area of the user store where profile data shared by multiple platforms is located. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory. You can use the same variables as for the **Path to user store**.

If this policy is disabled, the path Windows\PM_CP is used. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Source for creating cross-platform settings

Specifies a platform as the base platform if this policy is enabled in that platform's OU. This policy migrates data from the base platform's profiles to the cross-platform settings store.

Each platform's own set of profiles are stored in a separate OU. You must decide which platform's profile data to use to seed the cross-platform settings store. It is referred to as the base platform. Consider the cross-platform settings store contains a definition file with no data, or the cached data in a single-platform profile is newer than the definition's data in the store. In this case, the Profile Management migrates the data from the single-platform profile to the store unless you disable this policy.

> **Important:**
>
> If this policy is enabled in multiple OUs, or multiple user or machine objects, the platform that the first user logs on to becomes the base profile.
> By default this policy is Enabled.

File system policy settings

May 5, 2025

This section contains policies that set the following:

- Which files in a user profile are synchronized between the system where the profile is installed and the user store
- Which directories in a user profile are synchronized between the system where the profile is installed and the user store

Exclusions policy settings

September 6, 2025

This section describes policy settings for configuring which files and directories in a users profile are excluded from the synchronization process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exclusion list - files

List of files that are ignored during synchronization. File names must be paths relative to the user profile (%USERPROFILE%). Wildcards are supported in file names and in folder names, but only wildcards in file names are applied recursively.

Examples:

- `Desktop\Desktop.ini` ignores the file `Desktop.ini` in the `Desktop` folder
- `%USERPROFILE%\*.tmp` ignores all files with the extension `.tmp` in the entire profile
- `AppData\Roaming\MyApp\*.tmp` ignores all files with the extension `.tmp` in one part of the profile
- `Downloads\*\a.txt` ignores `a.txt` in any immediate subfolder of the `Downloads` folder.

If this policy is disabled, no files are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no files are excluded.

Enable Default Exclusion List - directories

Default list of directories ignored during synchronization. Use this policy to specify GPO exclusion directories without having to fill them in manually.

If you disable this policy, Profile Management does not exclude any directories by default.

If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not exclude any directories by default.

Exclusion list - directories

List of folders that are ignored during synchronization. Folder names must be specified as paths relative to the user profile (%USERPROFILE%). Wildcards in folder names are supported but are not applied recursively.

Example:

- `Desktop` ignores the `Desktop` folder in the user profile

If this policy is disabled, no folders are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no folders are excluded.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logon Exclusion Check

This setting configures what Profile Management does if a profile in the user store contains excluded files or folders. The possible policy settings and the corresponding actions are listed in the following table:

Policy setting	Action
Setting is disabled or the value of "Synchronize excluded files or folders on logon"is set to default	Profile Management synchronizes excluded files or folders from the user store to the local profile when a user logs on.
Setting is set to "Ignore excluded files or folders on logon"	Profile Management ignores the excluded files or folders in the user store when a user logs on.
Setting is set to "Delete excluded files or folder on logon"	Profile Management deletes the excluded files or folders in the user store when a user logs on.
Setting is not configured in the Web Studio	The value from the .ini file is used
Setting is not configured in the Web Studio or in the .ini file	The excluded files or folders are synchronized from the user store to a local profile when a user logs on.

Large File Handling - Files to be created as symbolic links

To improve logon performance and to process large-size files, Profile Management creates a symbolic link instead of copying files in this list.

You can use wildcards in policies that refer to files; for example, `!ctx_localappdata!\Microsoft\Outlook\*.OST`.

To process the offline folder file (`*.ost`) of Microsoft Outlook, make sure that the **Outlook** folder is not excluded for Profile Management.

Those files cannot be accessed in multiple sessions simultaneously.

Synchronization policy settings

May 5, 2025

The **Synchronization** section describes policy settings for specifying which files and folders in a users profile are synchronized between the system where the profile is installed and the user store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Directories to synchronize

Be default, Profile Management synchronizes the user profile between the system it is installed on and the user store. If you exclude a folder from the synchronization, this policy lets you include the subfolders of the excluded folder back to the synchronization.

Paths on this list must be relative to the user profile. Wildcards in folder names are supported but are not applied recursively.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, only non-excluded folders in the user profile are synchronized.

Files to synchronize

Be default, Profile Management synchronizes the user profile between the system it is installed on and the user store. If you exclude a folder from the synchronization, this policy lets you include the files inside the excluded folder back to the synchronization.

Paths on this list must be relative to the user profile. Wildcards are supported in file names and in folder names, but only wildcards in file names are applied recursively. Wildcards cannot be nested.

Examples:

- `AppData\Local\Microsoft\Office\Access.qat` specifies a file below a folder that is excluded in the default configuration
- `AppData\Local\MyApp\*.cfg` specifies all files with the extension `.cfg` in the profile folder `AppData\Local\MyApp` and its subfolders

Disabling this policy has the same effect as enabling it and configuring an empty list.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, only non-excluded files in the user profile are synchronized.

Folders to mirror

This policy lets you solve issues involving any transactional folder (also known as a referential folder). That folder contains interdependent files, where one file references the other.

Mirroring folders enables Profile Management to process a transactional folder and its contents as a single entity, avoiding profile bloat. For example, you can mirror the **Internet Explorer cookies** folder so that Index.dat is synchronized with the cookies that it indexes. In these situations the "last write wins."So files in mirrored folders that have been modified in more than one session are overwritten by the last update, resulting in loss of profile changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, the following table describes how Index.dat references cookies while a user browses the Internet:

Scenario	How Index.dat references cookies	
A user has two Internet Explorer sessions, each on a different server, and they visit different sites in each session.	Cookies from each site are added to the appropriate server.	Cookies from each site are added to the appropriate server.
User logs off from the first session or in the middle of a session (if the active write back feature is configured)	Cookies from the second session must replace those cookies from the first session.	
First and second sessions are merged and the references to the cookies in Index.dat become out of date	Further browsing in new sessions results in repeated merging and a bloated cookie folder	

Mirroring the cookie folder solves the issue. In this case, the cookies are overwritten with those cookies from the last session each time the user logs off. So Index.dat stays up to date.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no folders are mirrored.

Accelerate folder mirroring

With both this policy and the **Folders to mirror** policy enabled, **Profile Management stores mirrored** folders on a VHDX-based virtual disk. It attaches the virtual disk during logons and detaches it during logoffs. Enabling this policy eliminates the need to copy the folders between the user store and local profiles and accelerates folder mirroring.

Folder redirection policy settings

May 5, 2025

This section contains policy settings that specify whether to redirect folders that commonly appear in profiles to a shared network location.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Grant administrator access

This setting enables an administrator to access the contents of a user's redirected folders.

> **Note:**
>
> This setting grants permissions to administrators who have complete and unrestricted access to the domain.

By default, this setting is disabled and users are granted exclusive access to the contents of their redirected folders.

Include domain name

This setting enables the inclusion of the `%userdomain%` environment variable as part of the UNC path. This UNC path is specified for redirected folders.

By default, this setting is disabled. And the `%userdomain%` environment variable is not included as part of the UNC path that is specified for redirected folders.

AppData(Roaming) policy settings

May 5, 2025

This section contains policy settings for redirecting the contents of the **AppData(Roaming)** folder to a shared network location.

AppData(Roaming) path

This setting specifies the network location to which the contents of the **AppData(Roaming)** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for AppData(Roaming)

This setting specifies how to redirect the contents of the **AppData(Roaming)** folder.

By default, contents are redirected to a UNC path. For more information, see the Path to user store section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Contacts policy settings

May 5, 2025

This section contains policy settings for redirecting the contents of the **Contacts** folder to a shared network location.

Contacts path

This setting specifies the network location to which the contents of the **Contacts** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Contacts

This setting specifies how to redirect the contents of the **Contacts** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Desktop policy settings

May 5, 2025

This section contains policy settings for redirecting the contents of the `Desktop` folder to a shared network location.

Desktop path

This setting specifies the network location to which the contents of the **Desktop** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Redirection settings for Desktop

This setting specifies how to redirect the contents of the **Desktop** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Documents policy settings

May 5, 2025

This section contains policy settings for redirecting the contents of the **Documents** folder to a shared network location.

Documents path

This setting specifies the network location to which files in the **Documents** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

The **Documents path** setting must be enabled not only to redirect files to the **Documents** folder, but also to redirect files to the **Music**, **Pictures**, and **Videos** folders.

Redirection settings for Documents

This setting specifies how to redirect the contents of the **Documents** folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the **Documents** folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Documents path policy setting.
- Redirect to the users home directory. Redirects content to the users home directory, typically configured as the #homeDirectory# attribute for a user in the Active Directory.

If this setting is not configured here, Profile Management does not redirect the specified folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Downloads policy settings

September 6, 2025

This section contains policy settings for redirecting the contents of the **Downloads** folder to a shared network location.

Downloads path

This setting specifies the network location to which files in the **Downloads** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Downloads

This setting specifies how to redirect the contents of the **Downloads** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Favorites policy settings

May 5, 2025

This section contains policy settings for redirecting the contents of the **Favorites** folder to a shared network location.

Favorites path

This setting specifies the network location to which the contents of the **Favorites** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Redirection settings for Favorites

This setting specifies how to redirect the contents of the **Favorites** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Links policy settings

May 5, 2025

This section contains policy settings for redirecting the contents of the **Links** folder to a shared network location.

Links path

This setting specifies the network location to which the contents of the **Links** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Links

This setting specifies how to redirect the contents of the **Links** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Music policy settings

September 6, 2025

This section contains policy settings for redirecting the contents of the **Music** folder to a shared network location.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Music path

This setting specifies the network location to which the contents of the **Music** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Redirection settings for Music

This setting specifies how to redirect the contents of the **Music** folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the **Music** folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Music path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the **Documents** folder, the **Documents path** setting must be enabled.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Pictures policy settings

September 6, 2025

This section contains policy settings for redirecting the contents of the **Pictures** folder to a shared network location.

Pictures path

This setting specifies the network location to which the contents of the **Pictures** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Redirection settings for Pictures

This setting specifies how to redirect the contents of the **Pictures** folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the **Pictures** folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Pictures path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the **Documents** folder, the **Documents path** setting must be enabled.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Saved Games policy settings

September 6, 2025

This section contains policy settings for redirecting the contents of the **Saved Games** folder to a shared network location.

Redirection settings for Saved Games

This setting specifies how to redirect the contents of the **Saved Games** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Saved Games path

This setting specifies the network location to which the contents of the **Saved Games** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Start menu policy settings

September 6, 2025

This section contains policy settings for redirecting the contents of the **Start Menu** folder to a shared network location.

Redirection settings for Start Menu

This setting specifies how to redirect the contents of the **Start Menu** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Start Menu path

This setting specifies the network location to which the contents of the **Start Menu** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Searches policy settings

May 5, 2025

This section contains policy settings for redirecting the contents of the **Searches** folder to a shared network location.

Redirection settings for Searches

This setting specifies how to redirect the contents of the **Searches** folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile Management does not redirect the specified folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Searches path

This setting specifies the network location to which the contents of the **Searches** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Video policy settings

September 6, 2025

This section contains policy settings for redirecting the contents of the **Video** folder to a shared network location.

Redirection settings for Video

This setting specifies how to redirect the contents of the **Video** folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the **Video** folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Video path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the **Documents** folder, the **Documents path** setting must be enabled.

If this setting is not configured here, Profile Management does not redirect the specified folder.

Video path

This setting specifies the network location to which the contents of the **Video** folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile Management does not redirect the specified folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log policy settings

September 6, 2025

This section contains policy settings that configure Profile Management logging.

Active Directory actions

This setting enables or disables verbose logging of actions performed in the Active Directory.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured in the Web Studio, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

Common information

This setting enables or disables verbose logging of common information.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

Common warnings

This setting enables or disables verbose logging of common warnings.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Errors
- General information

Enable logging

This setting enables or disables Profile Management logging in debug (verbose logging) mode. In debug mode, extensive status information is logged in the log files located in "%SystemRoot%\System32\Logfiles\UserProfileManager".

By default, this setting is disabled and only errors are logged.

Citrix® recommends enabling this setting only if you are troubleshooting Profile Management.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, only errors are logged.

File system actions

This setting enables or disables verbose logging of actions performed in the file system.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

File system notifications

This setting enables or disables verbose logging of file systems notifications.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logoff

This setting enables or disables verbose logging of user logoffs.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

Logon

This setting enables or disables verbose logging of user logons.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

Maximum size of the log file

This setting specifies the maximum permitted size for the Profile Management log file, in bytes.

By default, this value is set to 1048576 bytes (1 MB).

Citrix recommends increasing the size of this file to 5 MB or more, if you have sufficient disk space. If the log file grows beyond the maximum size:

- An existing backup of the file (.bak) is deleted
- The log file is renamed to .bak
- A new log file is created

The log file is created in %SystemRoot%\System32\Logfiles\UserProfileManager.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Path to log file

This setting specifies an alternative path to save the Profile Management log file.

By default, this setting is disabled and log files are saved in the default location: %SystemRoot%\System32\Logfiles\UserProfileManager.

The path can point to a local drive or a remote network-based drive (UNC path). Remote paths can be useful in large distributed environments but they might create significant network traffic, which might be inappropriate for log files. For provisioned, virtual machines with a persistent hard drive, set a local path to that drive. This setting ensures that the log files are preserved when the machine restarts. For virtual machines without a persistent hard drive, setting a UNC path allows you to retain the log files. However, the system account for the machines must have write access to the UNC share. Use a local path for any laptops managed by the offline profiles feature.

If a UNC path is used for log files, Citrix recommends that an appropriate access control list is applied to the log file folder. This setting ensures that only authorized user or computer accounts can access the stored files.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default location %SystemRoot%\System32\Logfiles\UserPr
is used.

Personalized user information

This setting enables or disables verbose logging of personalized user information.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

Policy values at logon and logoff

This setting enables or disables verbose logging of policy values when a user logs on and off.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

Registry actions

This setting enables or disables verbose logging of actions performed in the registry.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

Registry differences at logoff

This setting enables or disables verbose logging of any differences in the registry when a user logs off.

By default, this setting is disabled.

When enabling this setting, make sure the **Enable logging** setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured in the Web Studio or in the .ini file, the following is logged:

- Errors
- General information

Profile handling policy settings

September 6, 2025

This section includes policy settings that specify how Profile Management handles user profiles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Delay before deleting cached profiles

This setting specifies an optional extension to the delay, in minutes, before Profile Management deletes locally cached profiles at logoff.

A value of 0 deletes the profiles immediately at the end of the logoff process. Profile Management checks for logoffs every minute. As as result, a value of 60 ensures that profiles are deleted between one and two minutes after users log off. This action depends on when the last check occurred. Extending the delay is useful if you know that a process keeps files or the user registry hive open during logoff. With large profiles, this process can also speed up logoff.

By default, this value is set to 0 and Profile Management deletes locally cached profiles immediately.

When enabling this setting, ensure the Delete locally cached profiles on logoff is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, profiles are deleted immediately.

Delete locally cached profiles on logoff

This setting specifies whether locally cached profiles are deleted after a user logs off.

When this setting is enabled, a user's local profile cache is deleted after they have logged off. Citrix® recommends enabling this setting for terminal servers.

By default, this setting is disabled and a users local profile cache is retained after they log off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, cached profiles are not deleted.

Local profile conflict handling

This setting configures how Profile Management behaves if a user profile exists in both of the following:

- User store
- Local Windows user profile (not a Citrix user profile)

By default, Profile Management uses the local Windows profile, but does not change it in any way.

To control how Profile Management behaves, choose one of the following options:

- Use local profile. Profile Management uses the local profile, but does not change it in any way.
- Delete local profile. Profile Management deletes the local Windows user profile, and then imports the Citrix user profile from the user store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Rename local profile. Profile Management renames the local Windows user profile (for backup purposes) and then imports the Citrix user profile from the user store.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local profiles are used.

Migration of existing profiles

This setting specifies the types of profile migrated to the user store during logon if a user has no current profile in the user store.

Profile Management can migrate existing profiles "on the fly" during logon if a user has no profile in the user store. After that, the user store profile is used by Profile Management in both of the following:

- Current session
- Any other session configured with the path to the same user store

By default, both local and roaming profiles are migrated to the user store during logon.

To specify the types of profile migrated to the user store during logon, choose one of the following options:

- Local and roaming profiles
- Local
- Roaming
- None (Disabled)

If you select **None**, the system uses the existing Windows mechanism to create profiles, as if in an environment where Profile Management is not installed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local and roaming profiles are migrated.

Automatic migration of existing application profiles

This setting enables or disables the automatic migration of existing application profiles across different operating systems. The application profiles include both the application data in the `AppData` folder and the registry entries under `HKEY_CURRENT_USER\SOFTWARE`. This setting can be useful in cases where you want to migrate your application profiles across different operating systems.

For example, suppose you upgrade your operating system (OS) from Windows 10 version 1803 to Windows 10 version 1809. If this setting is enabled, Profile Management automatically migrates the existing application settings to Windows 10 version 1809 the first time each user

© 1997–2026 Citrix Systems, Inc. All rights reserved.

logs on. As a result, the application data in the AppData folder and the registry entries under HKEY_CURRENT_USER\SOFTWARE are migrated.

If there are multiple existing application profiles, Profile Management performs the migration in the following order of priority:

1. Profiles of the same OS type (single-session OS to single-session OS and multi-session OS to multi-session OS).
2. Profiles of the same Windows OS family; for example, Windows 10 to Windows 10, or Windows Server 2016 to Windows Server 2016).
3. Profiles of an earlier version of the OS; for example, Windows 7 to Windows 10, or Windows Server 2012 to Windows 2016.
4. Profiles of the closest OS.

Note: You must specify the short name of the OS by including the variable "!CTX_OSNAME!"in the user store path. Doing so lets Profile Management locate the existing application profiles.

If this setting is not configured here, the setting from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled by default.

Path to the template profile

This setting specifies the path to the profile that you want Profile Management to use as a template to create user profiles.

The specified path must be the full path to the folder containing the NTUSER.DAT registry file and any other folders and files required for the template profile.

Note: Do not include NTUSER.DAT in the path. For example, with the file \\myservername\myprofiles\template\ntu set the location as \\myservername\myprofiles\template.

Use absolute paths, which can be either UNC paths or paths on the local machine. Use the latter, for example, to specify a template profile permanently on a Citrix Provisioning™ Services image. Relative paths are not supported.

Note: This setting does not support expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.

By default, this setting is disabled and new user profiles are created from the default user profile on the device where a user first logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Template profile overrides local profile

This setting enables the template profile to override the local profile when creating user profiles.

Consider that a user has no Citrix user profile, but has a local Windows user profile. In this case, by default the local profile is used and migrated to the user store, if this value is enabled. Enabling this policy setting allows the template profile to override the local profile used when creating user profiles.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Template profile overrides roaming profile

This setting enables the template profile to override a roaming profile when creating user profiles.

Consider that a user has no Citrix user profile, but has a roaming Windows user profile. In this case, by default the roaming profile is used and migrated to the user store, if this value is enabled. Enabling this policy setting allows the template profile to override the roaming profile used when creating user profiles.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Template profile used as a Citrix mandatory profile for all logons

This setting enables Profile Management to use the template profile as the default profile for creating all user profiles.

By default, this setting is disabled and new user profiles are created from the default user profile on the device where a user first logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

Registry policy settings

September 6, 2025

This section contains policy settings that specify which registry keys are included or excluded from Profile Management processing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exclusion list

List of registry keys in the HKCU hive which are ignored during logoff.

Example: Software\Policies

If this policy is disabled, no registry keys are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no registry keys are excluded.

Inclusion list

List of registry keys in the HKCU hive that are processed during logoff.

Example: Software\Adobe.

If this policy is enabled, only keys on this list are processed. If this policy is disabled, the complete HKCU hive is processed. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, all of HKCU is processed.

Enable Default Exclusion List - Profile Management 5.5

Default list of registry keys in the HKCU hive that are not synchronized to the user's profile. Use this policy to specify GPO exclusion files without having to fill them in manually.

If you disable this policy, Profile Management does not exclude any registry keys by default. If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not exclude any registry keys by default.

NTUSER.DAT backup

Enables a backup of the last known good copy of NTUSER.DAT and rollback in there is corruption.

If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not back up NTUSER.DAT.

Streamed user profiles policy settings

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This section contains policy settings that specify how Profile Management processes streamed user profiles.

Always cache

This setting specifies whether Profile Management caches streamed files as soon as possible after a user logs on. Caching files after a user logs on saves network bandwidth, enhancing the user experience.

Use this setting with the **Profile streaming** setting.

By default, this setting is disabled and streamed files aren't cached as soon as possible after a user logs on.

If this setting isn't configured here, the value from the .ini file is used.

If this setting is configured neither here nor in the .ini file, it is disabled.

Always cache size

This setting specifies a lower limit, in MB, on the size of files that are streamed. Profile Management caches any files in this size or larger as soon as possible after a user logs on.

By default, the value is set to 0 (zero) and the cache entire profile feature is used. When the cache entire profile feature is enabled, Profile Management fetches all profile contents in the user store, after a user logs on, as a background task.

If this setting isn't configured here, the value from the .ini file is used.

If this setting is configured neither here nor in the .ini file, it is disabled.

Profile streaming

This setting enables and disables the Citrix® streamed user profiles feature. When enabled, profile files and folders are fetched from the user store to the local computer only when users access them after logon. Registry entries and files in the pending area are fetched immediately.

By default, profile streaming is disabled.

If this setting isn't configured here, the value from the .ini file is used.

If this setting is configured neither here nor in the .ini file, it is disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Streamed user profile groups

This setting specifies which user profiles within an OU are streamed, based on Windows user groups.

When enabled, only user profiles within the specified user groups are streamed. All other user profiles are processed normally.

By default, this setting is disabled and all user profiles within an OU are processed normally.

If this setting isn't configured here, the value from the .ini file is used.

If this setting is configured neither here nor in the .ini file, all user profiles are processed.

Enable profile streaming exclusion

When profile streaming exclusion is enabled:

- Profile Management does not stream folders in the exclusion list
- All the folders are fetched immediately from the user store to the local computer when a user logs on

For more information, see Stream user profiles.

Timeout for pending area lock files

This setting specifies the number of days after which users' files are written back to the user store from the pending area, if the user store remains locked when its storage server becomes unresponsive. This behavior prevents bloat in the pending area and ensures that the user store always contains the most up-to-date files.

By default, this setting is set to 1 (one) day.

If this setting isn't configured here, the value from the .ini file is used.

If this setting is configured neither here nor in the .ini file, the default value is used.

Enable profile streaming for pending area

Lets you enable the profile streaming feature for files and folders in the pending area.

The pending area is used to ensure profile consistency while profile streaming is enabled. It temporarily stores profile files and folders changed in concurrent sessions.

By default, this policy is disabled, and all files and folders in the pending area are fetched to the local profile on logon. With this policy enabled, files in the pending area are fetched to the local profile only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

when they are requested. Use the policy with the Profile streaming policy to ensure optimal logon experience in concurrent session scenarios.

The policy applies to folders in the pending area when the Enable profile streaming for folders policy is enabled.

User personalization layer policy settings

September 6, 2025

To enable the mounting of user layers within the Virtual Delivery Agents, use the configuration parameters to specify:

- Where on the network to access the user layers.
- How large any new user layer disks can grow.

To do so, these two policies appear in the list of available policies:

- User Layer Repository Path - Enter a path in the format '\server name or address\folder name' in the Value field.
- User Layer Size GB - The default user layer size of 10 GB is the minimum that Citrix® recommends. A user layer is a thin-provisioned disk that expands to the set size as space is used. User layers never decrease in size.

> **Note:**
>
> Increasing the User Layer Size affects new user layers and expands existing ones. Decreasing the layer size only affects new user layers. Existing user layers never decrease in size.

For more information, see User personalization layer.

Virtual Delivery Agent policy settings

September 6, 2025

The Virtual Delivery Agent (VDA) section contains policy settings that control communication between the VDA and controllers for a site.

Important: The VDA requires information provided by these settings to register with a Delivery Controller™, if you are not using the auto-update feature. Because this information is required for registration, you must configure the following settings using the Group Policy Editor, unless you provide this information during the VDA installation:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Controller registration IPv6 netmask
- Controller registration port
- Controller SIDs
- Controllers
- Only use IPv6 controller registration
- Site GUID

Controller registration IPv6 netmask

This policy setting allows administrators to restrict the VDA to only a preferred subnet (rather than a global IP, if one is registered). This setting specifies the IPv6 address and network where the VDA register. The VDA register only on the first address that matches the specified netmask. This setting is valid only if the Only use IPv6 controller registration policy setting is enabled.

By default this setting is blank.

Controller registration port

Use this setting only if the **Enable auto update of controllers** setting is disabled.

This setting specifies the TCP/IP port number that the VDA uses to register with a Controller when using registry-based registration.

By default, the port number is set to 80.

Controller SIDs

Use this setting only if the **Enable auto update of controllers** setting is disabled.

This setting specifies a space-separated list of controller Security Identifiers (SIDs) the VDA uses to register with a Controller when using registry-based registration. This setting is an optional and might be used with the **Controllers** setting to restrict the list of Controllers used for registration.

By default, this setting is blank.

Controllers

Use this setting only if the **Enable auto update of controllers** setting is disabled.

This setting specifies a space-separated list of controller Fully Qualified Domain Names (FQDNs) the VDA uses to register with a Controller when using registry-based registration. This setting is an optional and might be used with the **Controller SIDs** setting.

By default, this setting is blank.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable auto update of controllers

This setting enables the VDA to register with a Controller automatically after installation.

After the VDA registers, the Controller with which it registered sends a list of the current controller FQDNs and SIDs to the VDA. The VDA writes this list to persistent storage. Each Controller also checks the Site database every 90 minutes for Controller information. The Controller sends updated lists to its registered VDAs if one of the following occurs:

- A Controller has been added or removed since the last check
- A policy change has occurred

The VDA accepts connections from all the Controllers in the most recent list that it received.

By default, this setting is enabled.

Only use IPv6 controller registration

This setting controls which form of address the VDA uses to register with the Controller:

- When enabled, the VDA registers with the Controller using the machine's IPv6 address. When the VDA communicates with the Controller, it uses the following address order: global IP address, Unique Local Address (ULA), link-local address (if no other IPv6 addresses are available).
- When disabled, the VDA registers and communicates with the Controller using the machine's IPv4 address.

By default, this setting is disabled.

Site GUID

Use this setting only if the **Enable auto update of controllers** setting is disabled.

This setting specifies the Globally Unique Identifier (GUID) of the site that the VDA uses to register with a Controller when using Active Directory-based registration.

By default, this setting is blank.

HDX™ 3D Pro policy settings

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The HDX 3D Pro section includes policy settings for enabling and configuring the image quality configuration tool for users. This tool enables users to optimize the use of available bandwidth. For this optimization, the balance between image quality and responsiveness is adjusted in real time.

Enable lossless

This setting specifies whether users can enable and disable lossless compression using the image quality configuration tool. By default, users are not given the option to enable lossless compression.

Consider that a user enables lossless compression. In this case, the image quality is automatically set to the maximum value available in the image configuration tool. By default, either GPU or CPU-based compression can be used, according to the capabilities of the user device and the host computer.

HDX 3D Pro quality settings

This setting specifies the minimum and maximum values available to users in the image quality configuration tool. Using these values, uses can define the range of image quality adjustment in the image quality configuration tool.

Specify image quality values of between 0 and 100, inclusive. The maximum value must be greater than or equal to the minimum value.

Monitoring policy settings

September 6, 2025

The **Monitoring** section includes policy settings for process, resource monitoring, and application failure monitoring.

The scope of these policies can be defined based on the following:

- Site
- Delivery group
- Type of delivery group
- Organizational unit
- Tags

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policies for process and resource monitoring

Each data point for CPU, memory, and processes is collected from the VDA and stored on the Monitoring database. Sending the data points from the VDA consumes network bandwidth and storing them consumes considerable space in the monitoring database. Consider that you do not want to monitor either resource data or process data or both for a specific scope. For example, a specific delivery group or organizational unit. In this case, it is recommended to disable the policy.

Enable process monitoring

Enable this setting to allow monitoring of processes running on machines with VDAs. Statistics such as CPU and memory use are sent to the Monitoring Service. The statistics are used for real-time notifications and historical reporting in the Director.

The default for this setting is Disabled.

Enable resource monitoring

Enable this setting to allow monitoring of critical performance counters on machines with VDAs. Statistics (such as CPU and memory use, IOPS, and disk latency data) are sent to the Monitoring Service. The statistics are used for real-time notification and historical reporting in the Director.

The default for this setting is Enabled.

Scalability

The CPU and memory data is pushed to the database from each VDA at 5-minute intervals. Process data (if enabled) is pushed to the database at 10-minute intervals. IOPS and disk latency data is pushed to the database at 1-hour intervals.

CPU and memory data

CPU and memory data is **enabled** by default. The data retention values are as follows (Platinum license):

Data granularity	Number of Days
5 Minute Data	1 Day
10 Minute Data	7 Days

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data granularity	Number of Days
Hourly Data	30 Days
Daily Data	90 Days

IOPS and disk latency data

IOPS and disk latency data is **Enabled** by default. The data retention values are as follows (Platinum license):

Data granularity	Number of Days
Hourly Data	3 Days
Daily Data	90 Days

With the data retention settings, approximately 276 KB of disk space is required to store the following for one VDA over a period of one year:

- CPU
- Memory
- IOPS
- Disk latency data

Number of machines	Approximate storage required
1	276 KB
1K	270 MB
40K	10.6 GB

Process data

Process data is **Disabled** by default. It is recommended to enable process data on a subset of machines on a need basis. The default data retention settings for the process data are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data granularity	Number of Days
10-minute Data	1 Day
Hourly Data	7 Days

If process data is enabled with the default retention settings, process data would consume approximately 1.5 MB per VDA and 3 MB per Terminal Services VDA (TS VDA) over a period of one year.

Number of machines	Approximate storage required VDA	Approximate storage required TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

> **Note:**
>
> The numbers provided earlier do not include the Index space. And all the calculations are approximate and vary depending on the deployment.

Optional Configurations

You can modify the default retention settings to suit your needs. However, this configuration consumes extra storage. By enabling the settings below you can gain more accuracy in the process utilization data. The configurations which can be enabled are:

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

These Configurations can be enabled from the Monitoring PowerShell cmdlet: Set-MonitorConfiguration

Policies for application failure monitoring

The **Application Failure** tab, by default, displays only application faults from Multi-session OS VDAs. Settings of Application failure monitoring can be modified with the following Monitoring policies:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable monitoring of application failures

Use this setting to configure application failure monitoring to monitor either application errors or faults (crashes and unhandled exceptions), or both.
Disable application failure monitoring by setting the **Value** to **None**.
The default for this setting is Application faults only.

Enable monitoring of application failures on Single-session OS VDAs

By default, failures only from applications hosted on the Multi-session OS VDAs are monitored. To monitor Single-session OS VDAs, set the policy to **Allowed**.
The default for this setting is **Prohibited**.

List of applications excluded from failure monitoring

Specify a list of applications that are not to be monitored for failure.
By default this list is empty.

Policy for collecting data for Analytics

VDA Data Collection for Analytics

Use the policy to enable or disable the Monitor service from collecting performance and security related metrics of the VDAs for Performance and Security Analytics. By default, the policy is **Allowed**. Set the policy to **Prohibited** to stop the collection of data from the VDAs.

Clipboard place metadata collection for Security monitoring

Use the policy to enable or disable the clipboard place metadata collection by Broker service for Security monitoring, auditing, and compliance. By default, the policy is **Enabled**. Set the policy to **Disabled** to stop the collection of data from the VDAs.

Diagnostic data collection for performance monitoring

Use this policy to enable the monitoring service to gather diagnostic data such as session information, UPM/EUEM service states, Microsoft Teams optimization, and connection protocols. By default, the policy is **Enabled**. Set the policy to **Disabled** to stop the collection of data from the VDAs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Storage planning tips

Group policy. If you are not interested in monitoring the Resource Data or Process Data, either or both can be turned off using the group policy. For more information, see the **Group Policy** section of Create policies.

Data grooming. The default data retention settings can be modified to groom the data early and free up storage space. For more information on grooming settings, see Data granularity and retention in Accessing data using the API.

Virtual IP policy settings

September 6, 2025

> **Important:**
>
> - Windows 10 Enterprise multi-session doesn't support Remote Desktop IP Virtualization (Virtual IP) and we don't support Remote Desktop IP Virtualization or virtual loopback on Windows 10 Enterprise multi-session.
> - Remote Desktop IP Virtualization (Virtual IP) isn't supported on cloud-hosted machines. For more information, see Microsoft documentation.

The **Virtual IP** section includes policy settings that control whether sessions have their own virtual loopback address.

Virtual IP loopback support

When this setting is enabled, each session has its own virtual loopback address. When disabled, sessions do not have individual loopback addresses.

By default, this setting is disabled.

Virtual IP virtual loopback programs list

This setting specifies the application executables that can use virtual loopback addresses. When adding programs to the list, specify only the executable name. You do not need to specify the entire path.

By default, no executables are specified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual IP loopback port exclusion

When an application calls the loopback address on any ports specified in this setting, virtual loopback does not change the call to the session-specific loopback address

Workspace Environment Management™ policy settings

September 6, 2025

The **Workspace Environment Management** (WEM) section includes policy settings that help you manage how WEM agents work.

Citrix Cloud™ Connectors

This setting lets you configure Citrix Cloud Connector™ machines to which Workspace Environment Management agents can connect. To ensure high availability, we recommend at least two Cloud Connectors in each resource location. Make sure that Cloud Connector machines and agent machines reside in the same AD domain.

Configure COM Port and LPT Port Redirection settings using the registry

September 6, 2025

In VDA versions 7.0 through 7.8, **COM Port and LPT Port** settings are only configurable using the registry. For VDA versions earlier than 7.0 and for VDA versions 7.9 and later, these settings are configurable in Web Studio. For more information, see Port redirection policy settings and Bandwidth policy settings.

Policy settings for COM Port and LPT Port Redirection are located under HKLM\Software\Citrix\GroupPolicy\Default on the VDA image or machine.

To enable COM port and LPT port redirection, add new registry keys of type REG_DWORD, as follows:

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 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.

Registry key	Description	Permitted values
AllowComPortRedirection	Allow or prohibit COM port redirection	1 (Allow) or 0 (Prohibit)
LimitComBw	Bandwidth limit for COM port redirection channel	Numeric value
LimitComBWPercent	Bandwidth limit for COM port redirection channel as a percentage of total session bandwidth	Numeric value between 0 and 100
AutoConnectClientComPorts	Automatically connect COM ports from the user device	1 (Allow) or 0 (Prohibit)
AllowLptPortRedirection	Allow or prohibit LPT port redirection	1 (Allow) or 0 (Prohibit)
LimitLptBw	Bandwidth limit for LPT port redirection channel	Numeric value
LimitLptBwPercent	Bandwidth limit for LPT port redirection channel as a percentage of total session bandwidth	Numeric value between 0 and 100
AutoConnectClientLptPorts	Automatically connect LPT ports from the user device	1 (Allow) or 0 (Prohibit)

After configuring these settings, change your machine catalogs to use the new master image or updated physical machine. Desktops are updated with the new settings that the next time users log off.

Policy changes

March 27, 2026

The following table lists policy updates in Citrix Virtual Apps and Desktops™ 7 2507, including additions, removals, name changes, and default state changes.

Policy setting	Changes
ICA > End User Monitoring > Endpoint location data collection	The default state of this policy setting is changed from **Enabled** to **Disabled**. Learn more.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy setting	Changes
ICA > End User Monitoring > Endpoint network latency measurement interval Client printers policy settings > Retained and restored client printers	The default state of this policy setting is changed from **Enabled** to **Disabled**. Learn more. Deprecated since 2402

> **Note:**
>
> Delete all deprecated settings before upgrading. If any deprecated settings remain in use, the upgrade can fail with an error.

Manage

September 13, 2025

Managing a Citrix Virtual Apps and Desktops™ site covers various items and tasks.

Licensing

A valid connection to the Citrix License Server is required when you create a site. Later, you can complete several licensing tasks from Studio, including adding licenses, changing license types or models, and managing license administrators. You can also access the License Administration Console from Studio.

Applications

Manage applications in Delivery Groups and optionally, Application Groups.

Zones

In a geographically disperse deployment, you can use zones to keep applications and desktops closer to end users, which can improve performance. When you install and configure a site, all Controllers, machine catalogs, and host connections are in one primary zone. Later, you can use Studio to create satellite zones containing those items. After your site has more than one zone, you will be able to indicate in which zone any newly created machine catalogs, host connections, or added Controllers will be placed. You can also move items between zones.

Connections and resources

If you are using a hypervisor or other service to host machines that deliver applications and desktops to users, you create your first connection to that hypervisor or other service when you create a site. The storage and network details for that connection form its resources. Later, you can change that

© 1997–2026 Citrix Systems, Inc. All rights reserved.

connection and its resources, and create more connections. You can also manage the machines that use a configured connection.

Local Host Cache

Local Host Cache allows connection brokering operations in a site to continue when the connection between a Delivery Controller™ and the site database fails.

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. The Citrix virtual loopback feature allows you to configure applications that depend on communications with localhost to use a unique virtual loopback address in the localhost range.

Delivery Controllers

This article contains considerations and procedures when adding and removing Controllers from a site. It also describes how to move Controllers to another zone or site, and how to move a VDA to another site.

VDA registration with Controllers

Before a VDA can help deliver applications and desktops, it must register (establish communication) with a Controller. Controller addresses can be specified in several ways, which are described in this article. It is critical that VDAs have current information as Controllers are added, moved, and removed in the site.

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.

- Session reliability
- Auto Client Reconnect
- ICA® Keep-Alive
- Workspace control
- Session roaming

Use search in Studio

When you want to view information about machines, sessions, machine catalogs, applications, or Delivery Groups in Studio, use the flexible search feature.

Tags

Use tags to identify items such as machines, applications, groups, and policies. You can then tailor certain operations to apply on to items with a specific tag.

IPv4/IPv6

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

User profiles

By default, Citrix Profile Management is installed automatically when you install a VDA. If you use this profile solution, review this article for general information. See the Profile Management documentation for details.

Collect Citrix Diagnostic Facility (CDF) traces

The CDFControl utility is an event tracing controller or consumer for capturing Citrix Diagnostic Facility (CDF) trace messages displayed from various Citrix tracing providers. It is made to troubleshoot complex Citrix related issues, parse filter support, and collect performance data.

Citrix Insight Services

Citrix Insight Services (CIS) is a Citrix platform for instrumentation, telemetry, and business insight generation.

Citrix Scout

Citrix Scout collects diagnostics and runs health checks. You can use the results for proactive maintenance in your Citrix Virtual Apps and Desktops deployment. Citrix offers comprehensive, automated analysis of diagnostics collections through Citrix Insight Services. You can also use Scout to troubleshoot issues, on your own or with Citrix Support guidance.

Applications

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Introduction

If your deployment uses only delivery groups (and not application groups), you add applications to the delivery groups. If you also have application groups, generally you add applications to the application

© 1997–2026 Citrix Systems, Inc. All rights reserved.

groups instead. This guidance provides easier administration. An application must always belong to 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 Web 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.

For details, see:

- Create delivery groups
- Create application groups
- Tags

Add applications

You can add applications when you create a delivery group or application group. Those procedures are detailed in Create delivery groups and Create application groups. 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.

To add one or more applications:

1. Select **Applications** in the left pane and then select **Add Applications** in the action bar.
2. The Add Applications wizard launches with an **Introduction** page, which you can remove from future launches of this wizard.
3. The wizard guides you through the **Groups**, **Applications**, and **Summary** pages. When you are done with each page, click **Next** until you reach the **Summary** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alternatives to step 1 if you want to add applications to a single delivery group or application group:

- **To add applications to only one delivery group:** In step 1, select **Delivery Groups** in the Web Studio left pane, select a delivery group in the middle pane, and then select **Add Applications** in the action bar. The wizard does not display the **Groups** page.
- **To add applications to only one application group:** In step 1, select **Applications** in the Web Studio left pane, select an application group in the middle pane, and then select the **Add Applications** entry under the application group's name in the action bar. The wizard does not display the **Groups** page.

Groups page

This page lists all the delivery groups in the site. If you have also created application groups, the page lists the application groups and delivery groups. You can choose from either group, but not from both groups. In other words, you cannot add applications to an application group and a delivery group at the same time. Generally, if you are using application groups, add applications to application groups, rather than delivery groups.

When adding an application, select the check box next to at least one delivery group (or application group, if available). Every application must always be associated with at least one group.

Applications page

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 check boxes of applications to add, and then click **OK**.

  This source cannot be selected if you (1) selected application groups with no associated delivery groups, (2) selected application groups with associated delivery groups that contain no machines, or (3) selected a delivery group containing no machines.

- **Manually:** Applications located 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 click **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**. For more information, see Deploy and deliver App packages.

- **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 check boxes 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.

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` already exists in the **Applications** folder, and you attempt to add another application named `app` to that folder, the new name `app_1` is offered.

Summary page

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.

Review the summary information and then click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 (1) the delivery group contains shared machines and was created with a XenDesktop 7.x version earlier than 7.9, and (2) you have `Edit delivery group` permission. The delivery group type is automatically converted to `desktops and applications` when the properties dialog is committed.

1. Sign in to Web Studio, select **Applications** in the left pane, and then select the application.
2. Select **Properties** in the action bar.
3. Select the **Groups** page.
    - 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 group association would result 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.

Duplicate, enable or disable, rename, or delete an application

The following actions are available:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 in the middle pane and then select the appropriate task in the action bar.
3. Confirm the action, when prompted.

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.
2. Select a delivery group. In the lower middle pane, on the **Applications** tab, select the application you want to remove.
3. Select **Remove Application** 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 in the middle pane, and then select one or more applications.
3. Select **Remove from Application Group** in the action bar.
4. Confirm the removal.

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 **Edit Application Properties** in the action bar.
3. Select the page containing the property you want to change.
4. When you are finished, click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

In the following list, the page is shown in parentheses.

Property	Page
Category/folder where application appears in Citrix Workspace app	Delivery
Command line arguments; see Pass parameters to published applications	Location
Delivery groups and application groups where the application is available	Groups
Description	Identification
File name extensions and file type association: which extensions the application opens automatically	File Type Association
Icon	Delivery
Keywords for StoreFront™	Identification
Limits; see Configure application limits	Delivery
Name: Names seen by the user and by the administrator	Identification

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Property	Page
Path to executable; see Pass parameters to published applications	Location
Shortcut on user's desktop: enable or disable	Delivery
Visibility: Limits which users can see the application in Citrix Workspace app. An invisible application can still be started. To make it unavailable and invisible, add it to a different group.	Limit Visibility
Working directory	Location

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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- **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 will be allowed to continue until their users close them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 **Edit Application Properties** in the action bar.
3. On the **Delivery** page, choose one of the following options.
    - **Allow unlimited use of the application**. 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
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
  ```

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 validation. If you do not see these symbols in a command line for the application, add them manually.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 executed, 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

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]\LogoffCheckerBloc` to determine if any processes are blocking a graceful sign-out when a published application is closed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 [ID] 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:

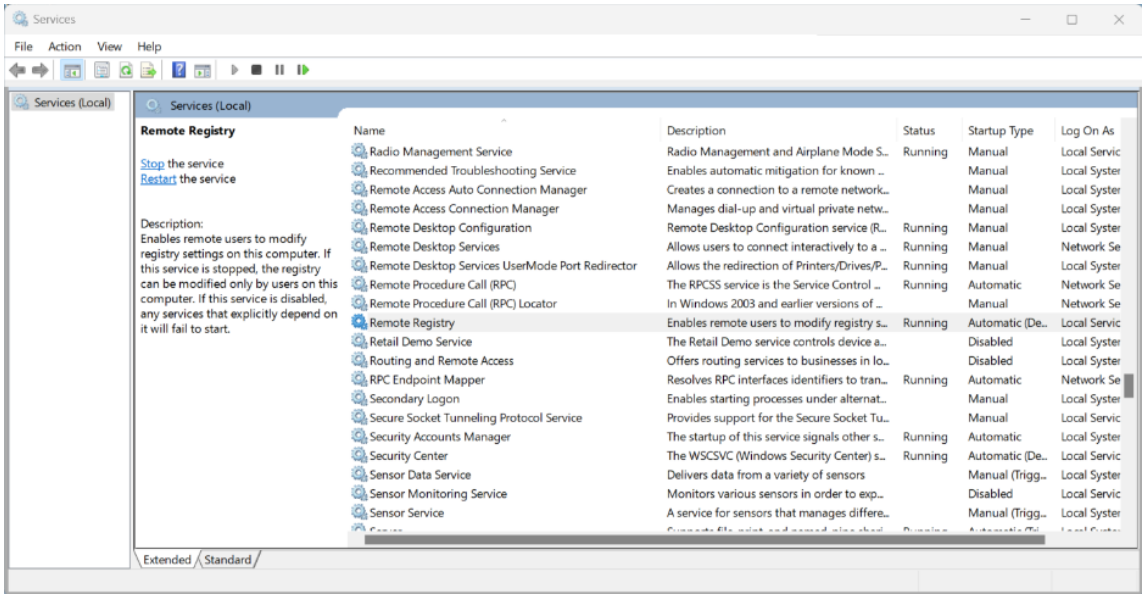
```
Add the process file name to the following registry key:
Caution! Refer to the Disclaimer at the end of this article before
   using the Registry Editor.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI
Value Name:LogoffCheckSysModules
Type:REG_SZ
String:MyAppName.exe
```

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**.

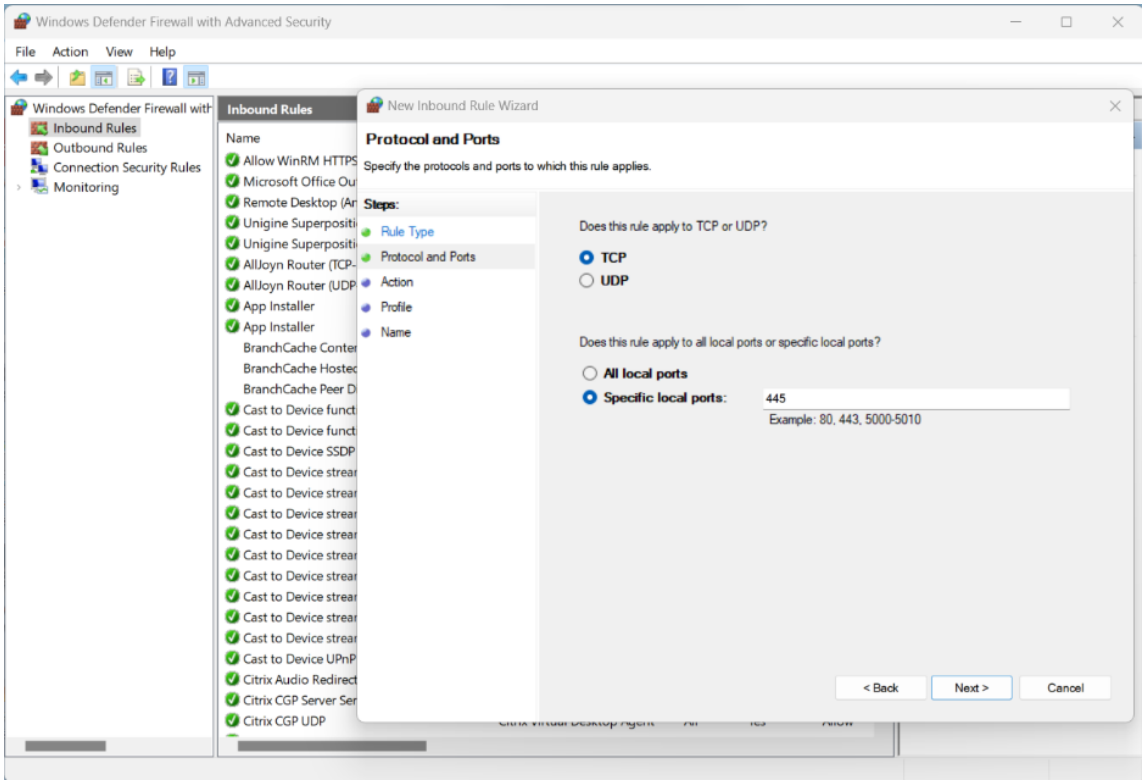
    d) On the **Protocols and Ports** page, select **TCP and Specific Local Ports**. Enter 445 as the local port.

    e) Select **Allow Connection** on the **Action** page.

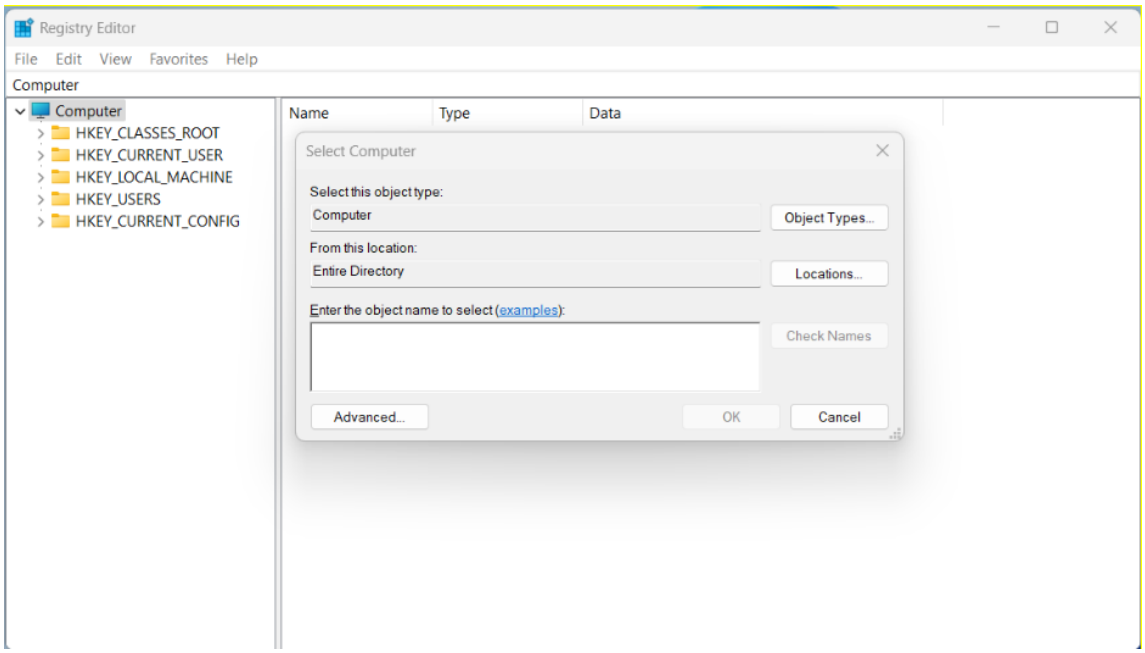
    f) Select the firewall profiles that you want to apply the new inbound rule.

    g) Name the firewall rule and select **Finish** to exit **New Inbound Rule wizard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

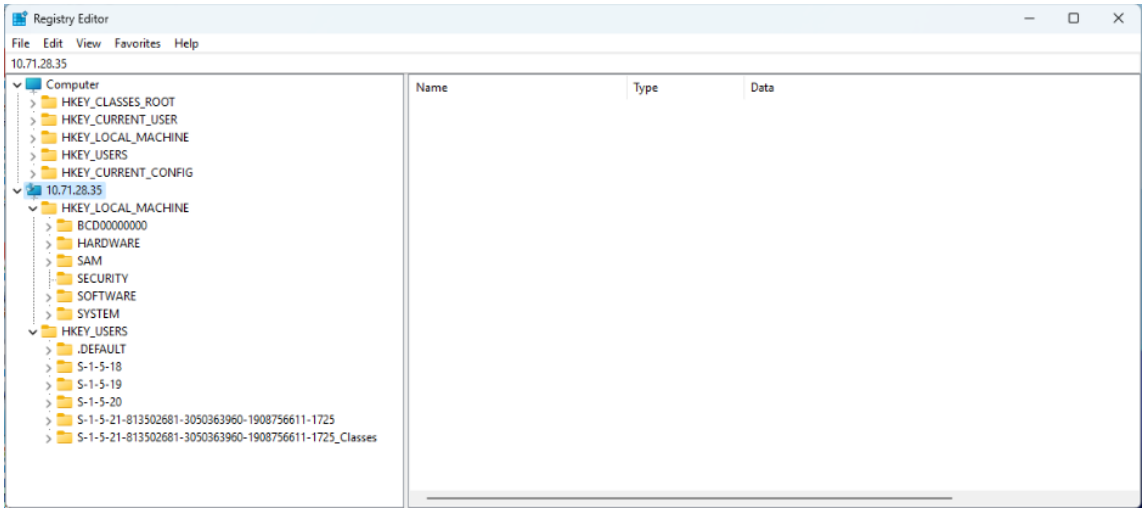


3. From another VM on the same domain (it could be DC, DDC, or another VDA), run `Regedit` and connect to a remote registry.

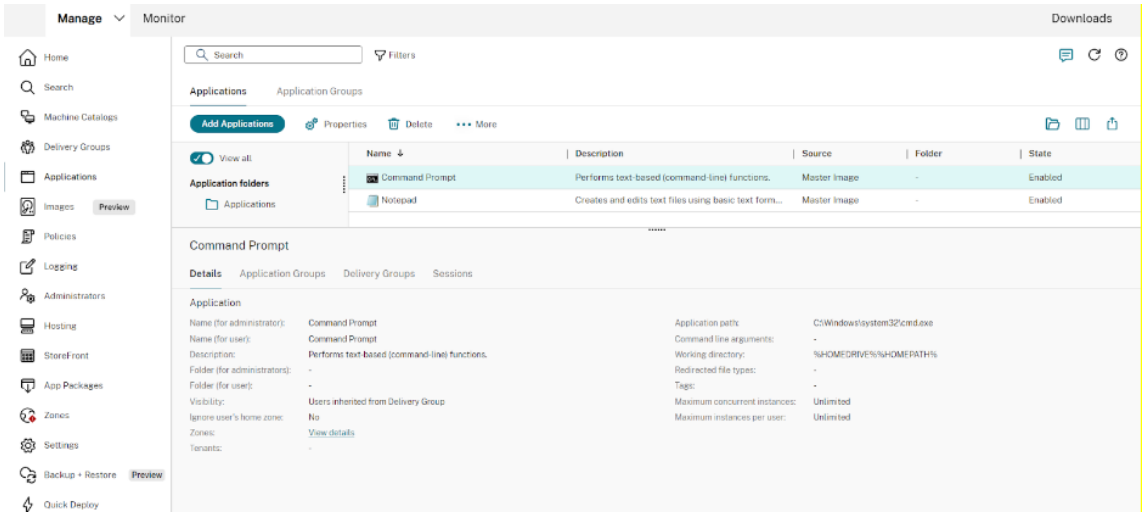


4. Enter the IP address of the VDA under test and click **OK**. The `regedit` tree must display branches for the VDA under test.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

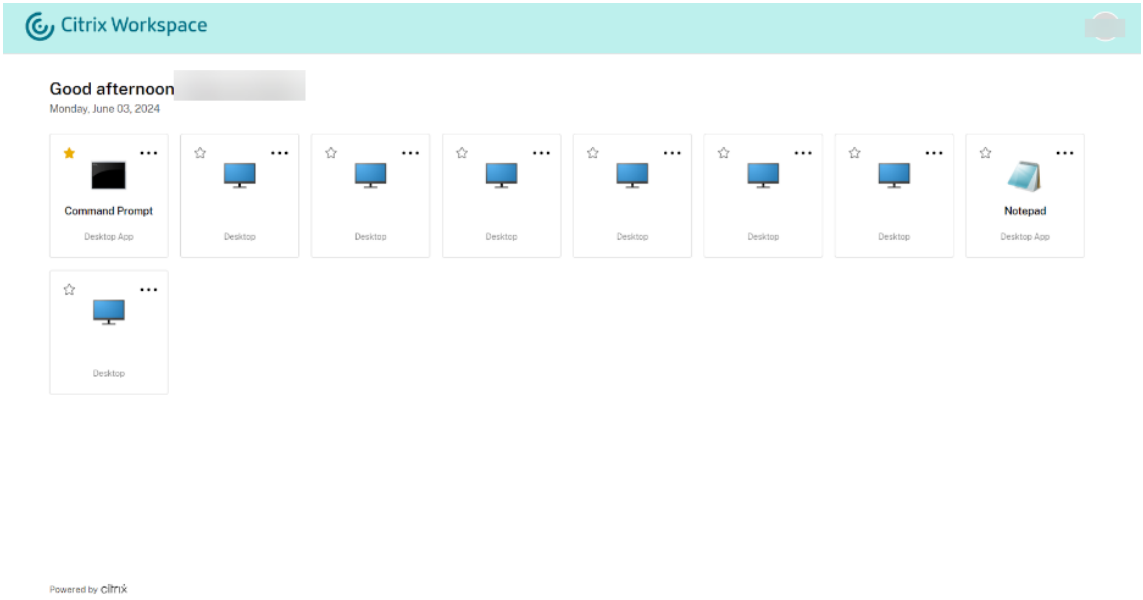


5. Open the **Command Prompt** published application.



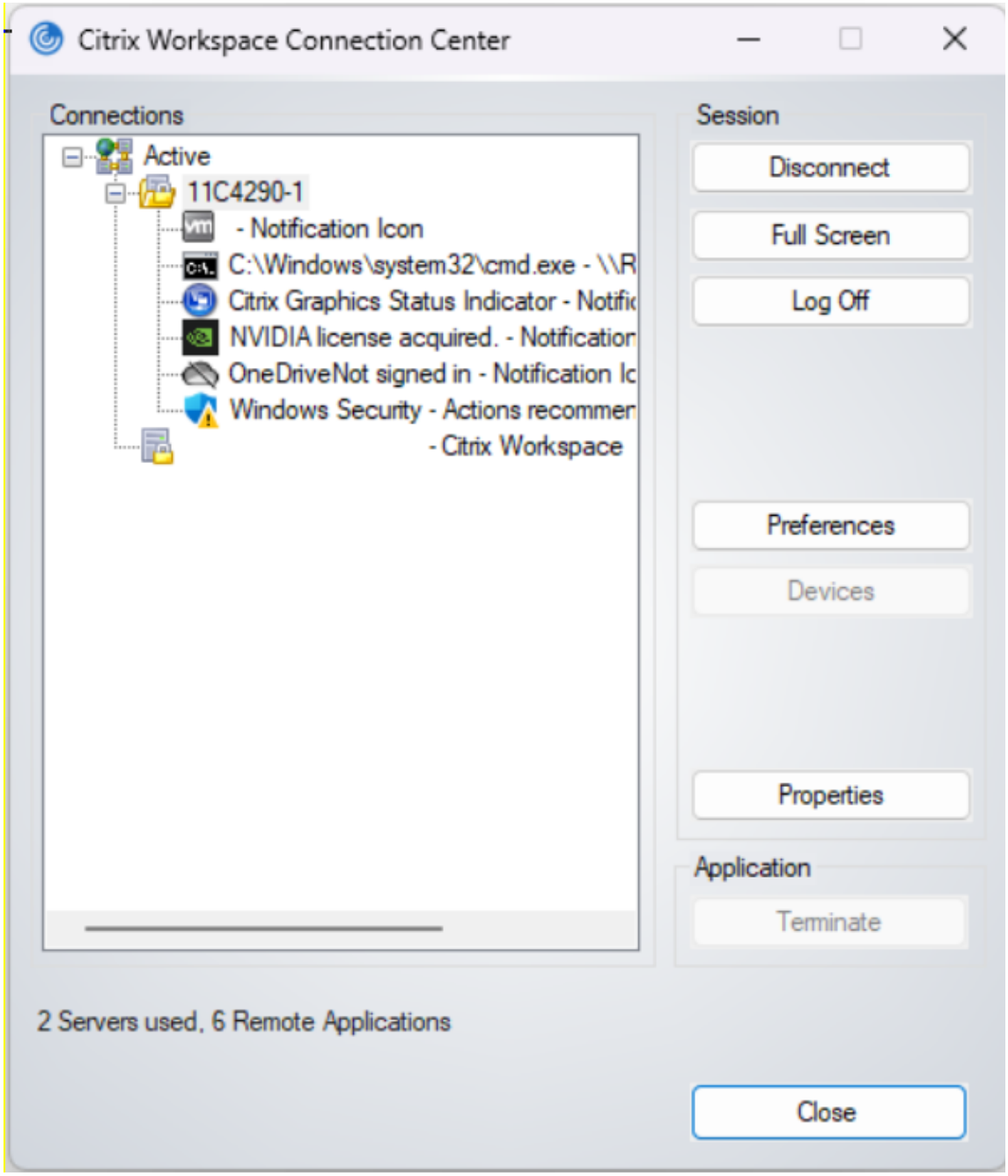
The **Command Prompt** app is displayed on Citrix Workspace.

© 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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\`

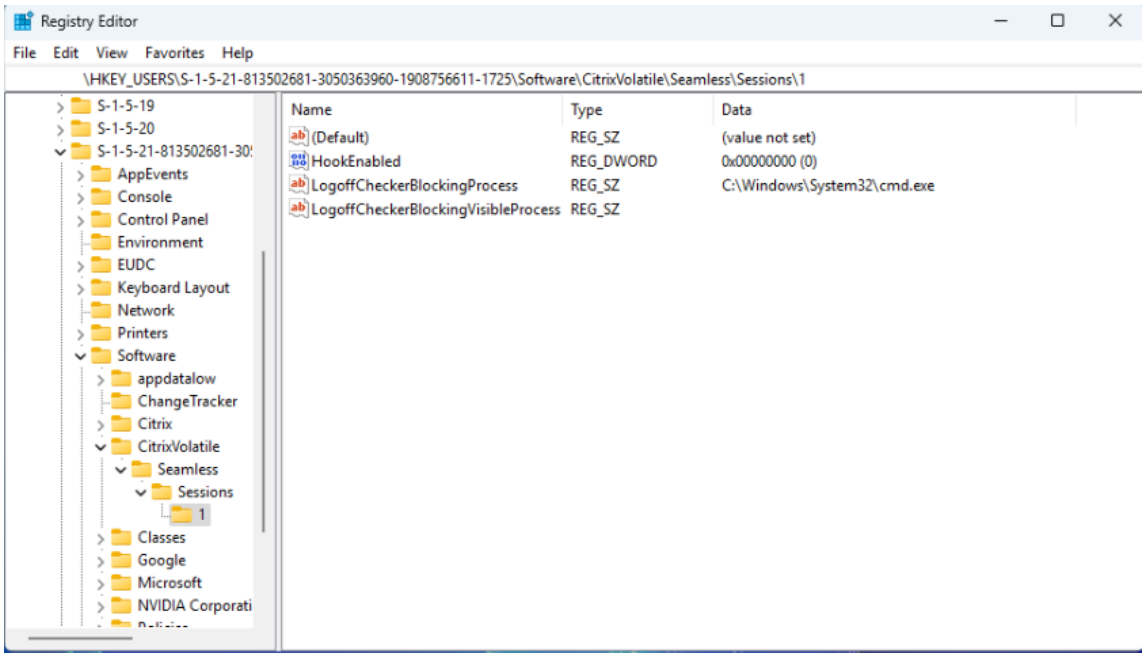
   > **Note:**
   >
   > This path changes every time you open a new session.

8. There are two keys to read here (do not change them here): **LogoffCheckBlockingProcess** and **LogoffCheckerBlockingVisibleProcess**. These keys display any programs that are blocking

© 1997–2026 Citrix Systems, Inc. All rights reserved.

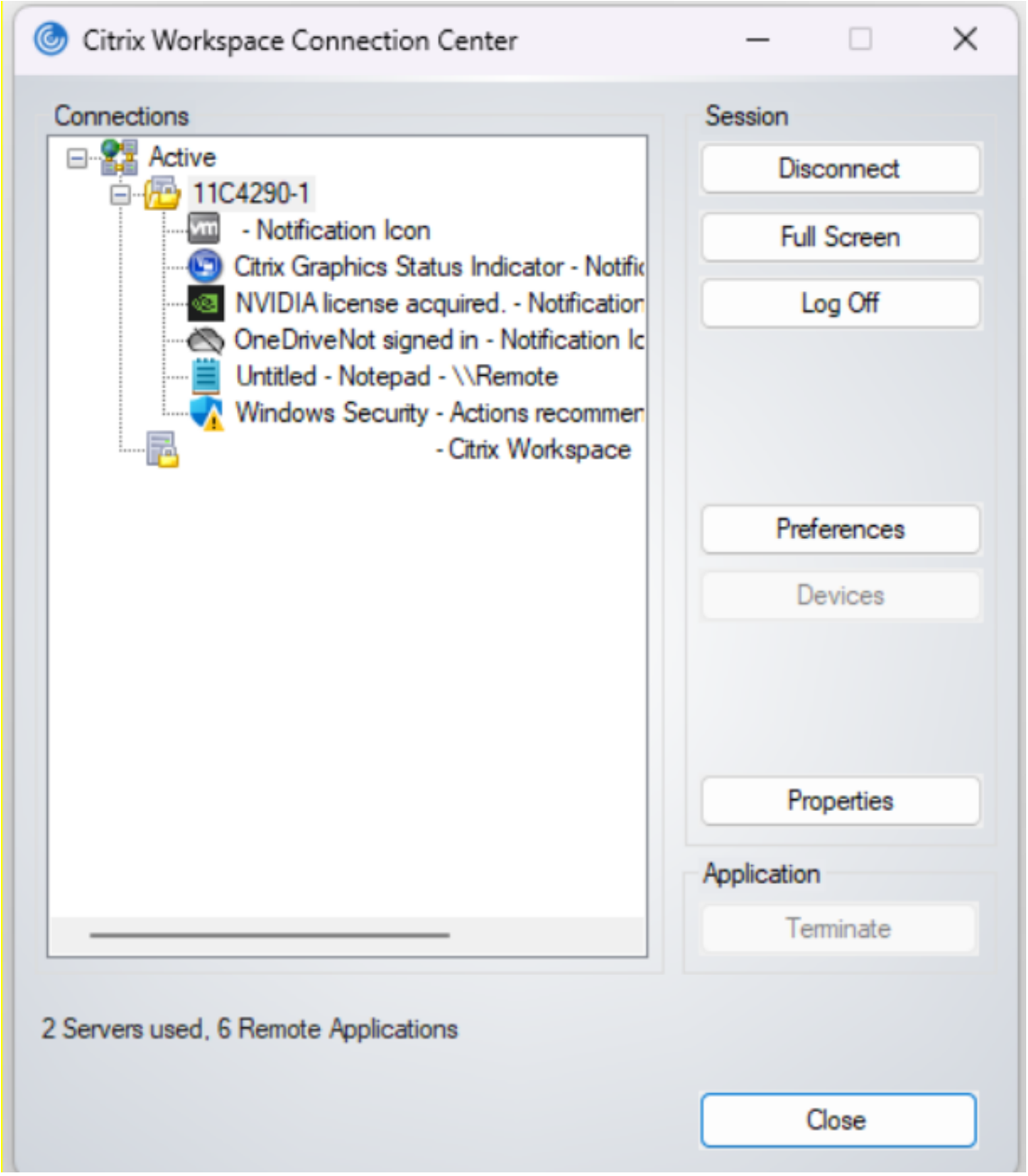
sign-out. The first one must display `C:\Windows\System32\cmd.exe` since that was open and has not been closed yet.

> **Note:**
>
> **LogoffCheckBlockingProcess** and **LogoffCheckerBlockingVisibleProcess** must not be manually edited. Manually editing these registry values could 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.

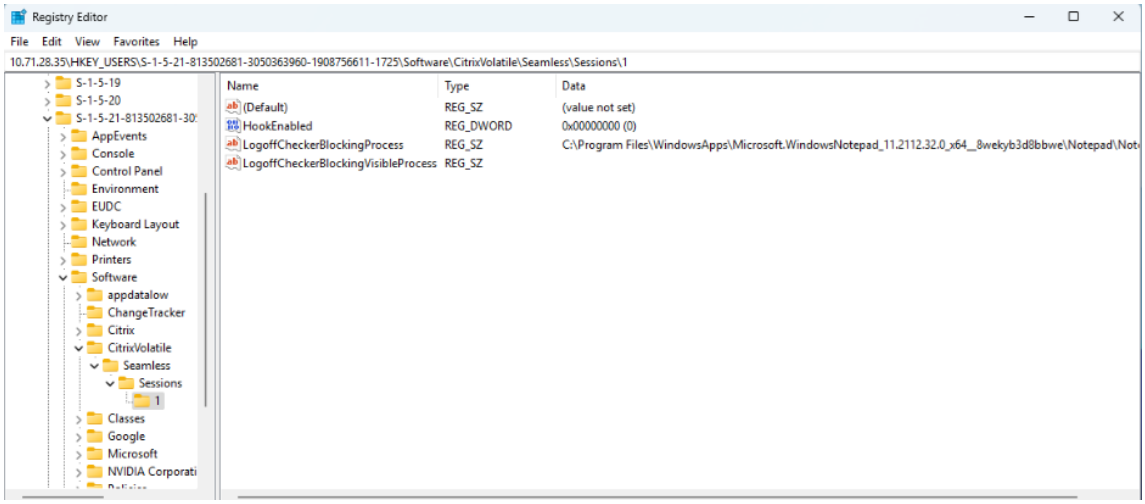
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

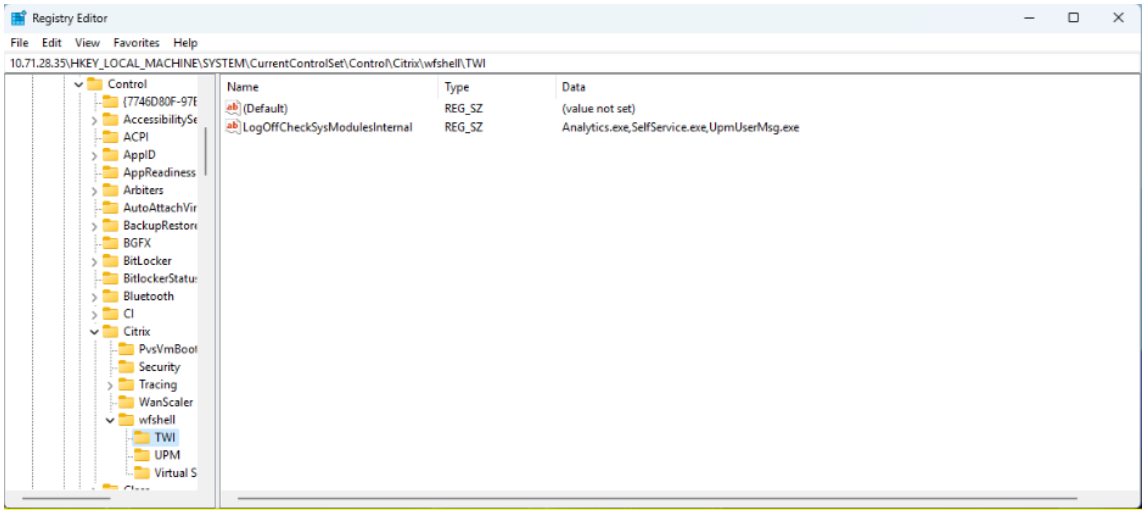
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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\TWILogoffCheckSysModulesInternal`
    - 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.
15. Repeat steps 9-16 until the session is signed out automatically within 30 seconds of closing the Remote Application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

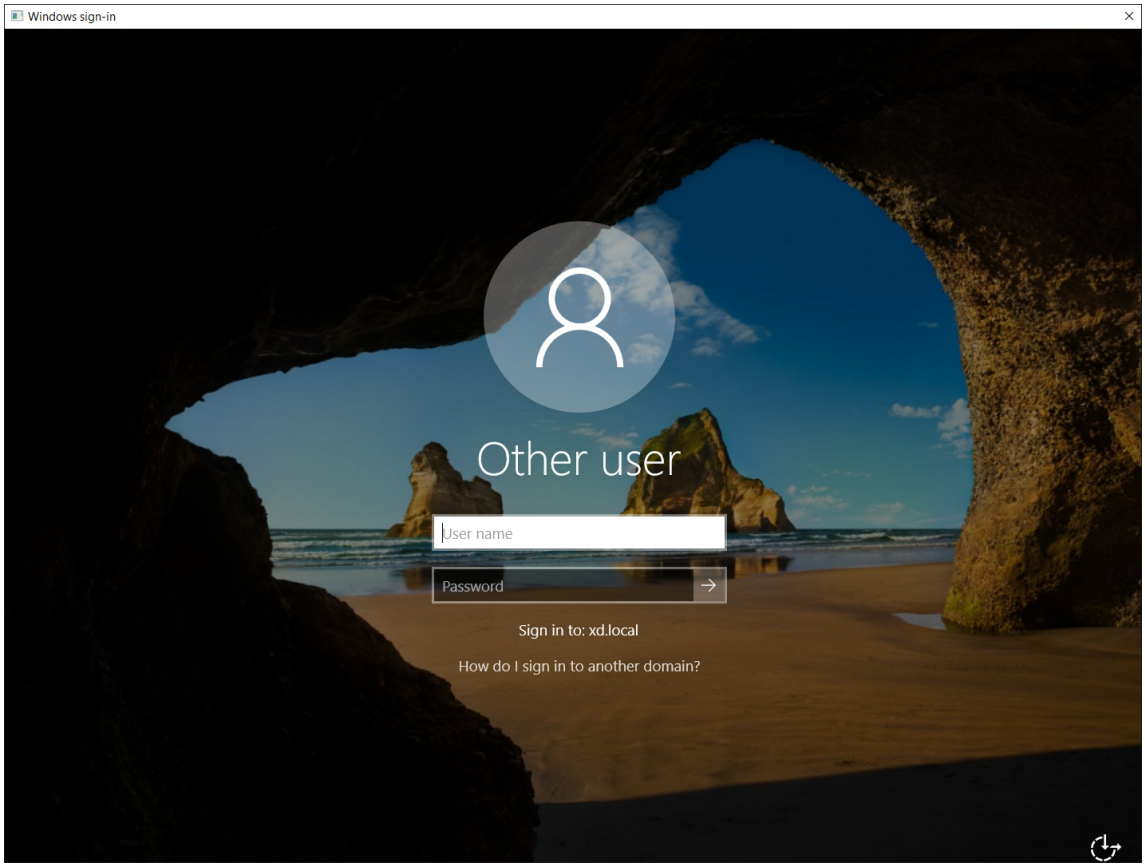
By default, the **LogonUI** window includes a title bar with a close button which enables the end user to disconnect from the session if needed.

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 Web 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.
- **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

App packages

January 5, 2026

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix supports the following packaging technologies for delivering applications to users:

- App-V applications
- MSIX and MSIX app attach applications
- FlexApp applications

This article walks you through how to deploy and deliver these packaged applications in your Citrix Virtual Apps and Desktops™ environment.

> **Note:**
>
> - You can manage your Citrix Virtual Apps and Desktops deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.
> - We don't recommend using Web Studio and Citrix Studio interchangeably for deploying and delivering app packages. Each uses different mechanisms, which can lead to discrepancies, such as App-V server information appearing correctly in one but not the other. Also, note that Citrix Studio supports only App-V.

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 Virtual Apps and Desktops 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.
- **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,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

  1. User SID
  2. Username
  3. AD Group SID (First found wins)
  4. AD Group Name (First found wins)
  5. 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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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:

   ```
   1 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.

Methods

You can use the following methods to deliver and manage App-V packages:

- **Dual Admin**: In this method, Citrix Virtual Apps and Desktops and App-V servers work together to deliver and manage packages. This method requires Citrix Virtual Apps and Desktops to periodically refresh the snapshot view of the App-V server's state. It incurs hardware, infrastructure, and administration overhead. Citrix Virtual Apps and Desktops 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Virtual Apps and Desktops 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.

> **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 sources. 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 Virtual Apps and Desktops 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about MSIX and MSIX app attach, see the Microsoft documentation: MSIX documentation and App Attach in Azure Virtual Desktop respectively.

> **Note:**
>
> - We support native MSIX Packages on Desktop and server VDAs and MSIX app attach on `.vhd`, `.vhdx`, 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.

Deploy and deliver app packages

Prerequisites

To support the delivery of App-V, MSIX, MSIX app attach and FlexApp packages, 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, and FlexApp 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In the installation wizard, go to the **Additional Components** page and then select the **App Packages Delivery Component** checkbox.
- 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.

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.

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.
4. To enable automatic delivery of interdependent App-V packages, create isolation groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
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:
    - The connecting entity must be a user account, not a machine account, as Azure AD 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Virtual Apps and Desktops 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:
    - 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
- 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 **Sources** tab, click the **Add Source** button. The **Add Source** page appears.
3. In the **Name** field, enter a descriptive name for the package source.
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** or **Network share** based on where you store the packages, and then complete the corresponding settings:
   - If you select **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.
     - 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\`
     - Select the package types that you want to upload. Options include App-V, MSIX, MSIX app attach, and FlexApp.
     - 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.
6. Click **Add Source**.

   The **Add Source** page closes and the newly added source appears in the source list. Citrix Virtual Apps and Desktops uploads the packages to your environment 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 source location and import them to your environment, select the location in the source list and click **Check for Package Updates**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the action bar, click **Add Delivery Groups**. The **Assign Applications to Delivery Groups** page appears.
4. Select one or more applications in the package as needed, and then click **Next**.
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.

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 source needed (for example, App-V Single Admin). All packages of this type appear.
   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 Mi-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> crosoft 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.

When a user starts an App-V application marked as *Explicit* in an isolation group, Citrix Virtual Apps and Desktops 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.
- 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

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 Virtual Apps and Desktops ISO on the path mentioned in step 1.

2. The package discovery module must be from the ISO of a Citrix Virtual Apps and Desktops 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
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 Virtual Apps and Desktops 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.

Universal Windows Platform Apps

September 13, 2025

For information about Universal Windows Platform (UWP) apps, see the following Microsoft documentation:

- What's a Universal Windows Platform (UWP) app?
- Windows Package Manager

Requirements and limitations

Citrix Virtual Apps and Desktops™ supports the use of UWP apps with VDAs on the following Windows machines:

- Windows 10 and later versions
- Windows Server 2016 and later versions

VDAs must be minimum version 7.11.

The following Citrix Virtual Apps and Desktops features are either not supported or limited when using UWP apps:

- File type association is not supported.
- Local App Access is not supported.
- Dynamic preview: If apps running in the session overlap, the preview shows the default icon. The Win32 APIs used for Dynamic Preview are not supported in UWP apps.
- Action Center remoting: UWP apps can use the Action Center for displaying the messages in the session. These messages are currently not redirected to the endpoint to be displayed to the user.

Launching UWP apps and non-UWP apps from the same server is not supported. Instead, place UWP apps and non-UWP apps in separate delivery groups or application groups.

Because all UWP apps installed on the machine are enumerated, Citrix® recommends disabling user access to the Windows Store. This precludes the UWP apps installed by one user from being accessed by a different user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

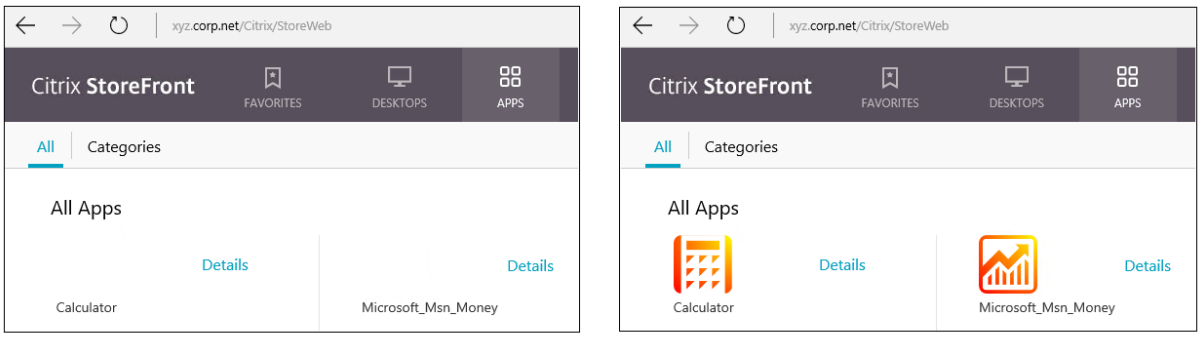
During sideloading, the UWP app is installed on the machine and is available for use by other users. When another user launches the app, then it is installed, and the OS updates its AppX database to indicate "as installed"by that user.

A graceful logoff started from a published UWP app that was launched in a fixed or seamless window might prevent the VDA session from closing and forcibly log off the user. When this occurs, several processes remaining in the VDA session prevent it from properly closing. To resolve this, determine which process is preventing the VDA session from closing, and then add it to the "LogoffCheckSysModules"registry key value, following the guidance in CTX891671.

Application Display Names and Descriptions for UWP apps might not have correct names. Edit and correct these properties when adding the applications to the delivery group.

Check Known issues for any additional issues.

Currently, several UWP apps have white icons with transparency enabled, which results in the icon not being visible against the white background of the StoreFront display. To avoid this issue, you can change the background. For example, on the StoreFront machine, edit the file `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`. At the end of the file, add `.storeapp-icon { background-image: radial-gradient( circle at top right, yellow, red ); }`. The following graphic illustrates the before-and-after for this example.



On Windows Server 2016 and later versions, the Server Manager might also launch when a UWP app is launched. To prevent this from occurring, you can disable Server Manager from auto-starting during logon with the `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon` registry key. For details, see https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/.

Install and publish UWP apps

Support for UWP apps is enabled by default.

To install one or more UWP apps on VDAs (or a master image), use one of the following methods:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Complete an offline install from the Windows Store for Business, using a tool such as Deployment Image Servicing and Management (DISM) to deploy the apps to the desktop image. For more information, see Windows Package Manager.
- Sideload the apps. For more information, see Sideload line of business (LOB) apps in Windows client devices.
- Install the UWP apps for each intended user directly from the Windows Store for Business.

To add (publish) one or more UWP apps in Citrix Virtual Apps or Citrix Virtual Desktops™:

1. After the UWP apps are installed on the machine, add the UWP apps to a delivery group or application group. You can do this when you create a group, or later. On the **Applications** page, in the **Add** menu, select **From Start menu**.
2. When the applications list appears, select the UWP apps you want to publish.
3. Continue with the wizard or close the edit dialog.

To disable the use of Universal Apps on a VDA, add the registry setting **EnableUWASeamlessSupport** in `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` and set to **0**.

Uninstall UWP apps

When you uninstall a UWP app with a command such as `Remove-AppXPackage`, the item is uninstalled only for administrators. To remove the app from the machines of users who may have launched and used the app, run the removal command on each machine. You cannot uninstall the AppX package from all users' machines with one command.

Backup or Migrate your configuration

September 6, 2025

This feature helps you take a backup of your 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 Web Studio.
2. Automated Configuration Tool (ACT)
    a) Powershell-based tool. Install the tool to use it. See Download Automated Configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Web Studio
DaaS and on-premises	On-demand and scheduled backups	ACT	User keeps the backup	Backup and Restore using Automated 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Environment	Use Case	Recommended Tool	Special Considerations	Link
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 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

September 6, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

  > **Note:**
  >
  > You can now backup host connections. 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 to restore different components. For example, if you want to restore Applications, Delivery groups, and Group policies, you must follow the order:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Delivery groups
- Applications
- Group policies

- You cannot back up or restore MCS machine catalogs.

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 Web Studio

September 6, 2025

This article describes the actions that you can perform on the **Backup and Restore** node available in the left pane of your console.

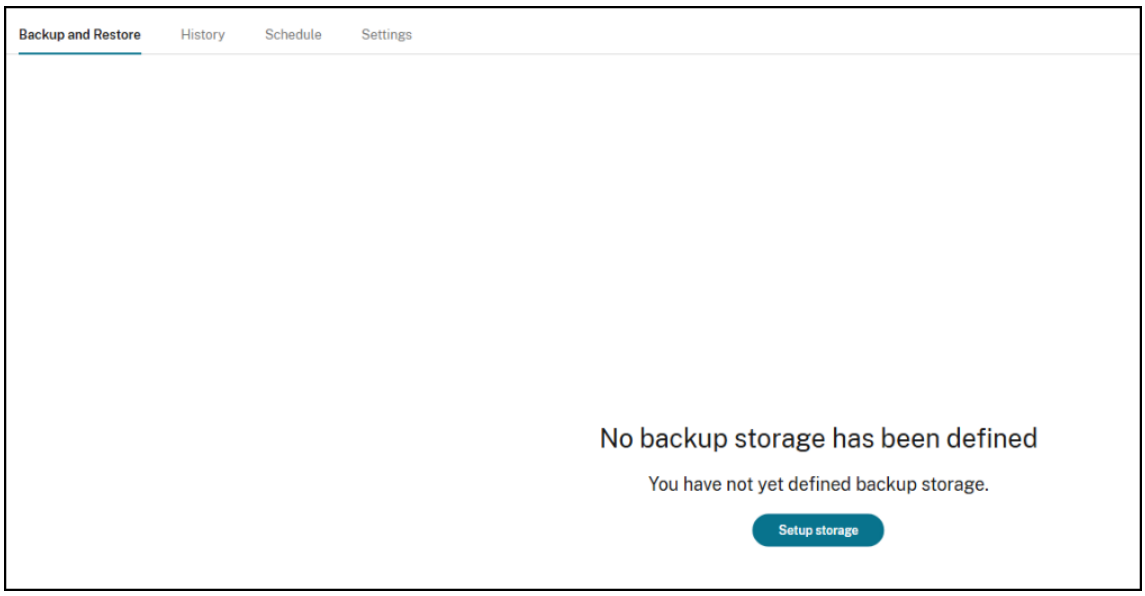
Backup and Restore allows the administrator to take backups from the Web Studio.

Set up storage location

Before creating backups, you must set up a storage location to store backups.

1. From Web Studio, click **Manage**.
2. From the left-menu, select **Backup+Restore**.
3. Within the **Backup and Restore** tab, click **Setup storage**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. From the drop-down list, select a **Storage type**. The Storage type can be a File Storage or an Azure Storage.

   > **Note:**
   >
   > - The location must be accessible to all Delivery Controllers.
   > - If access to the folder requires a username and password, make sure that corporate password policies do not limit the lifespan of the password.

5. Select the following:

   - Maximum backups
   - Maximum pinned backups
   - Maximum auto-pinned backups

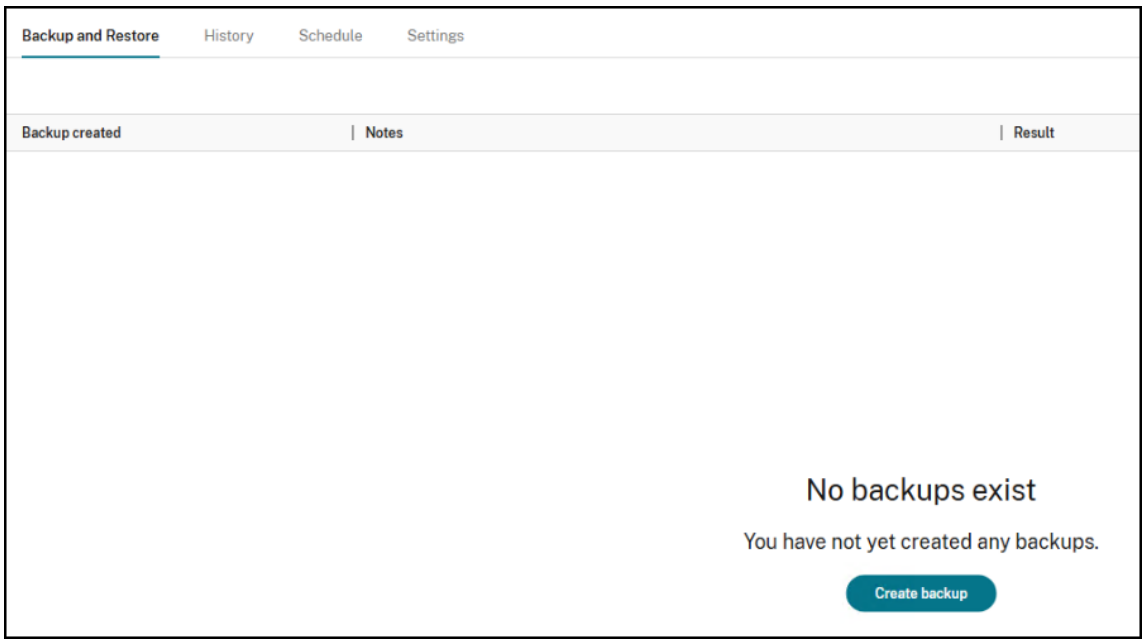
6. Click **Save** to save the storage location or **Save and create backup** to save the storage location and create backups.

After you set up a storage location, you can create backups.

Create on-demand backups

1. From Web Studio, click **Manage**.
2. From the left-menu, select **Backup and Restore**.
3. If the storage location is set up but no backup exists, you are prompted to create a backup.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If there are existing backups, you can click **Create backup**.

4. 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.

5. After the backup completes successfully, it is listed as a line item under the **Backup and Restore** tab.
6. Select a particular backup to see more information on the backup in the **Details** tab.
7. To delete a backup, right-click a backup and click **Delete backup**.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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 that 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select a scheduled backup for auto-pinning.
3. Switch the toggle to enable auto-pinned schedules.
4. Select a schedule and click **Save**.

Edit backup storage

You can edit the backup storage settings to change the storage type and location, maximum backups, maximum pinned backups, and maximum auto-pinned backups.

1. Go to the **Settings** tab of the **Backup and Restore** node.
2. Click **Change** in **Storage** box.
3. Change the storage settings in the **Edit backup storage** dialog.

Restore

This feature allows the administrators to restore the site configurations from the backups. We allow you to restore one component at a time.

> **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, in Azure, enter the alphanumeric application secret used to create the connection.

1. From Web Studio, click **Manage**.
2. From the left menu, select **Backup and Restore**.
3. Click a specific backup from the list.
4. Click **Restore Backup**.
5. 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 **Detail > Components**. Select a component and click **View component members**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.

  > **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.

6. 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Backup and Restore using the Automated Configuration tool

September 13, 2025

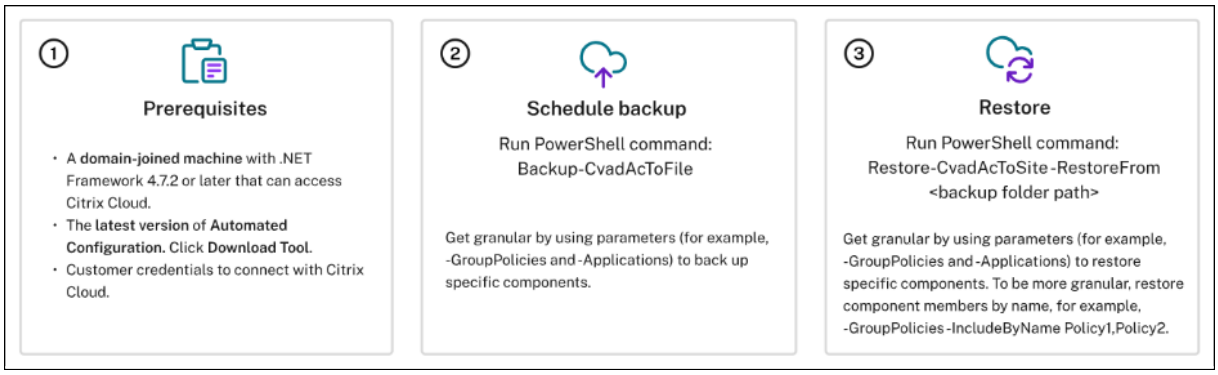
Automated Configuration tool allows you to take on-demand and scheduled backups in the following environments:

- 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)

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 Web Studio.

Back up

1. Install Automated Configuration. For more information, see Download Automated Configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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>
```

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The `CvadAcSecurity.yml` file with information on host connections.

1. Install Automated Configuration. For more information, 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`

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
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 Web 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Best practices for backup and restore

August 11, 2025

This article provides several recommendations that can help in better planning of backup and restore.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Can we download backups?

Currently, use ACT to download backups. 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.

Migrate configuration to Citrix Cloud™

September 13, 2025

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.

This is an embedded video. Click the link to watch the video

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
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.

```
1 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.
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:

```
1 New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6-46
    CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaaw==
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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-2
    CFE30CC398E
```

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
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft Azure
    - Subscription ID
    - 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.
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
    - 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 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

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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> `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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `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-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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

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.

Merging multiple sites into a single site

September 13, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prefixes and suffixes can be assigned for each of the following components on a per-on-premises-site basis.

- `AdminScope`
- `AdminRole`
- `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.

Prefixing and suffixing 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,"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:**
>
> 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.

Direct file share

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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 located 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.
- A different machine.

Automated Configuration must be installed on the machine accessing the cloud. Neither the on-premises PowerShell SDK, Delivery Controllers, nor Active Directory are used, so the cloud accessing execution requirements are simpler than the export requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To merge the East Delivery Controllers 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 Controllers 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_"
          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 instead
          ApplicationFolderRoot: "Western"
          ApplicationGroupPrefix: "Western "
          ApplicationUserPrefix: "Western "
          DeliveryGroupPrefix: "Western "
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
38            GroupPolicyPrefix: "Western "
39            HostConnectionPrefix: "Western "
40            MachineCatalogPrefix: "Western "
41            StoreFrontPrefix: "Western "
42            TagPrefix: "Western "
43            AdminScopeSuffix: ""
44            AdminRoleSuffix: ""
45            ApplicationAdminSuffix: ""
46            ApplicationFolderSuffix: ""
47            ApplicationGroupSuffix: ""
48            ApplicationUserSuffix: ""
49            DeliveryGroupSuffix: ""
50            GroupPolicySuffix: ""
51            HostConnectionSuffix: ""
52            MachineCatalogSuffix: ""
53            StoreFrontSuffix: ""
54            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
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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_"
          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 "
          ApplicationFolderPrefix: "" # Note that a new parent root
             folder is used instead
          ApplicationFolderRoot: "Western"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
35            ApplicationGroupPrefix: "Western "
36            ApplicationUserPrefix: "Western "
37            DeliveryGroupPrefix: "Western "
38            GroupPolicyPrefix: "Western "
39            HostConnectionPrefix: "Western "
40            MachineCatalogPrefix: "Western "
41            StoreFrontPrefix: "Western "
42            TagPrefix: "Western "
43            AdminScopeSuffix: ""
44            AdminRoleSuffix: ""
45            ApplicationAdminSuffix: ""
46            ApplicationFolderSuffix: ""
47            ApplicationGroupSuffix: ""
48            ApplicationUserSuffix: ""
49            DeliveryGroupSuffix: ""
50            GroupPolicySuffix: ""
51            HostConnectionSuffix: ""
52            MachineCatalogSuffix: ""
53            StoreFrontSuffix: ""
54            TagSuffix: ""
```

If a central file share method is not used and the import, merge, or add is done from the individual Delivery Controllers, then 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

1. `Remove-CvadAcFromSite –GroupPolicies –IncludeByName “Western *”`
2. `Remove-CvadAcFromSite –Applications –IncludeByName “Western *”`
3. `Remove-CvadAcFromSite – ApplicationGroups –IncludeByName “Western *”`
4. `Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”`
5. `Remove-CvadAcFromSite –MachineCatalogs –IncludeByName “Western *”`
6. `Remove-CvadAcFromSite –HostConnections –IncludeByName “Western *”`
7. `Remove-CvadAcFromSite –Tags –IncludeByName “Western *”`

To remove group policies of the East components, use the suffix:

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName “*_east”
```

Migrating from cloud to cloud

September 6, 2025

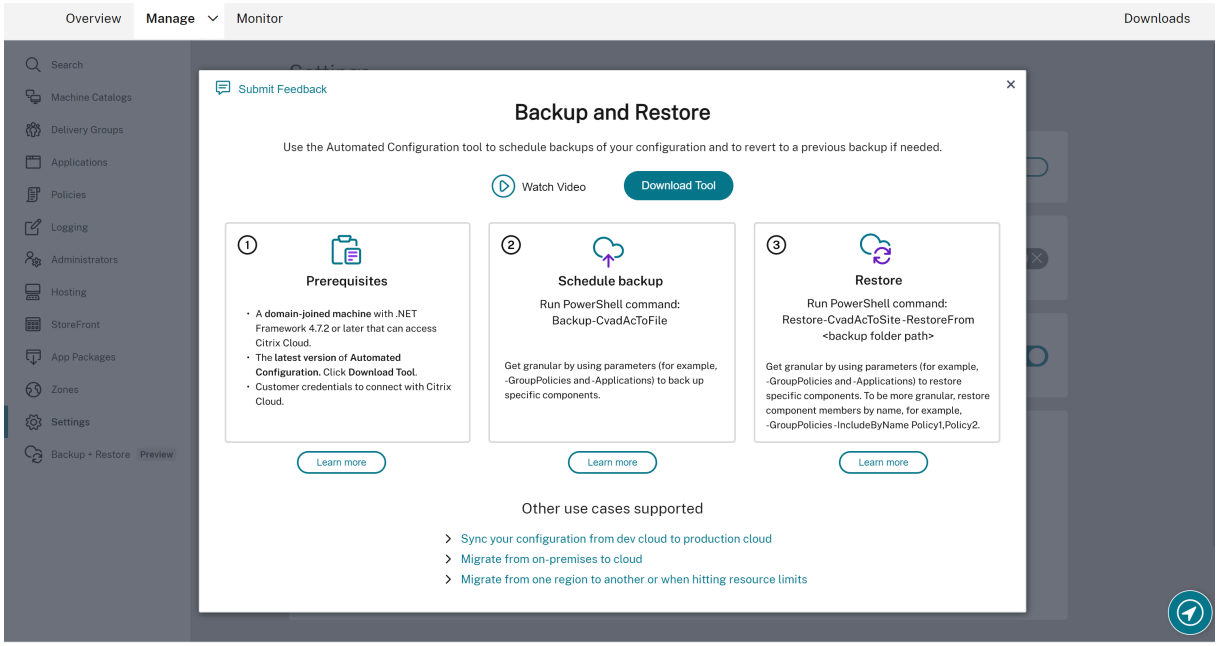
Automated Configuration allows you to automate moving your cloud configuration to another cloud site or allowing you to restore your own cloud site.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

   > **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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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

September 13, 2025

This article describes backing up and migrating your Cloud configurations to on-premises sites.

Prerequisites 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-premises site, we recommend ACT be installed on the Delivery Controller. ACT can be started via the desktop icon.
> - If ACT is intended to be used from the standard Powershell window then the following command must be executed:
>
> ```
> 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. Run `New-CvadAcCustomerInfoFile` to create a **CustomerInfo.yml** file. For more information, see Populate customer info file..
3. Run the command `Backup-CvadAcToFile` to take a backup of your Cloud configurations.

> **Note:**
>
> - 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.
> - 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
CvadAcSecurity.yml	Hypervisor: ConnectionType: “Username: “ Password: “	Add the hypervisor username and passwords.	If the hypervisor is XenServer,XenServer: ConnectionType: ‘XenServer’Username: ‘root’Password: “

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Migrate on-premises configurations to on-premises site

September 6, 2025

This article describes the steps to migrate your on-premises configurations from one site to another on-premises site using Automated Configuration Tool (ACT).

Requirements

- Both on-premises sites must be domain joined to the same domain.
- Use Citrix Virtual Apps and Desktops™ version 2305 or later.

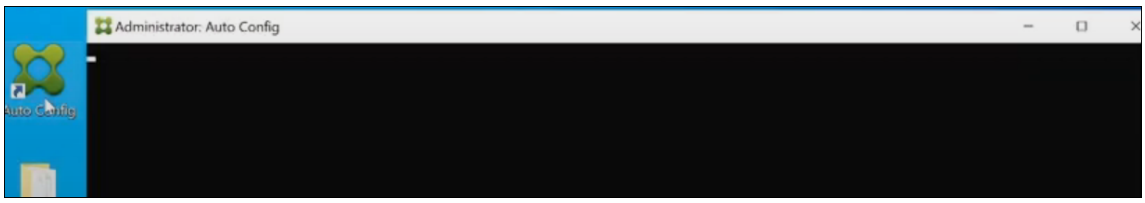
Steps

1. Download the Automated Configuration Tool and review the system requirements. See Download Automated Configuration.
2. Open ACT and export your on-premises site using the following the command.

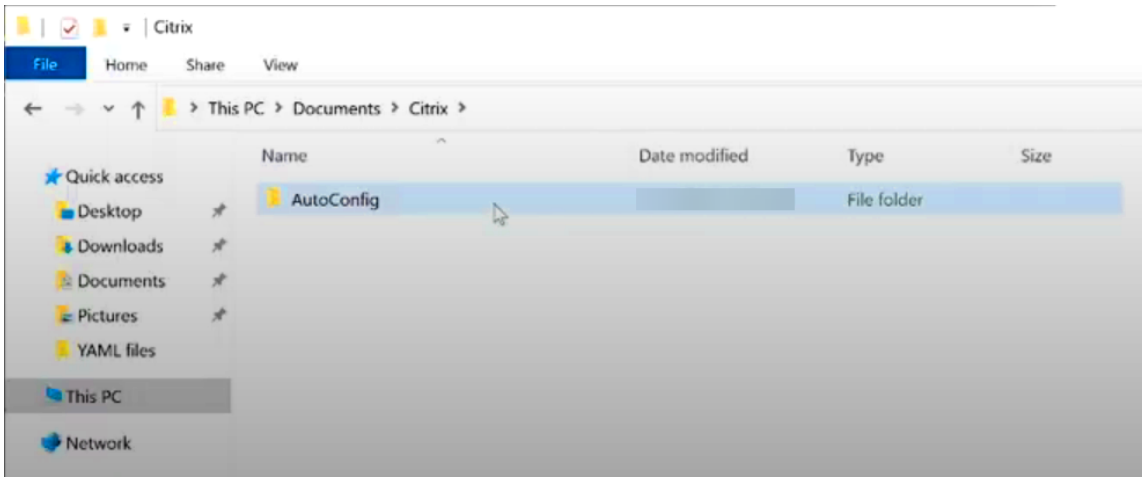
    ```
    1 Export-CvadAcToFile
    ```

    See Supported migration objects for the list of components supported for migration. For information on the steps to export, see Export on-premises configuration. The parent folder `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` always contains the exported files from the most recent export.
3. Launch the ACT on the target site. You must see an `AutoConfig` folder created in `%HOMEPATH%\\Documents\\Citrix`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



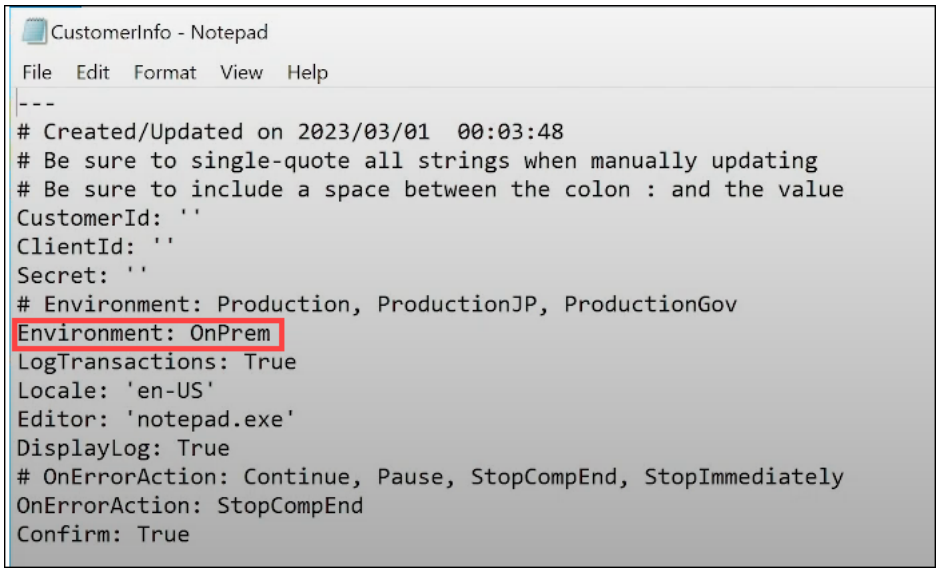
4. Copy the `.yml` files from the **Export** folder in the source site to the target site's `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` folder.



5. Specify the environment that you are working in using the `Set-CvadAcCustomerInfoFile` command. For example:

```
Set-CvadAcCustomerInfoFile -Environment OnPrem
```

This command updates the **CustomerInfo** file with the environment.



6. Migrate the configuration files using the following command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Import-CvadAcToFile
```

If you want to import from a different folder rather than the `AutoConfig` folder, run the following:

```
Import-CvadAcToFile -Sourcefolder PATH
```

> **Note:**
>
> If you are migrating host connections, then update the `CvadAcSecurity.yml` file with the connection information for each host type. See Update the security file for host connections.

If you encounter any errors or exceptions, see the Fixups section in the log file.

7. Verify that your configurations are migrated on your target site using Web Studio.

Automated configuration tool cmdlets for migration

September 6, 2025

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Cmdlet	Description
	`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.
	`Remove-CvadAcFromSite`	Remove component members from cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Cmdlet	Description
	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.
	`Find-CvadAcConnector`	Locates existing connectors and determines their running state.
	`Get-CvadAcCustomerSites`	Returns the list of all the customer sites.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Cmdlet	Description
	`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.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 machines that are not in Active Directory might result in import failures.		`$true` or `$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:

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 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 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 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
`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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Description	Required?	Type
`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

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%\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`
`OnErrorAction`	See OnErrorAction parameter.		String

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Description	Required?	Type

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
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 `$false`
`AddOnly`	When set to `$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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Description	Required?	Type
`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.

  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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Returns:

- 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 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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Description	Required?	Type
`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

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 `$false` to suppress the log display.		`$true` or `$false`

Returns:

- See Cmdlet return values

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
`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.

- * 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

`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`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 using this parameter.	Conditionally	String
`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:

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

© 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

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.
- `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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
`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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

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 supported in names.		List of strings
`Unique`	Report only unique-found members.		SwitchParameter
`IncludeYaml`	Include the member specific YAML.		SwitchParameter
`FindSourceFolder`	The folder find begins searching in.		String

© 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.		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
`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

© 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`

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 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 `$false` to suppress the log display.		`$true or $false`

Returns:

- See Cmdlet return values

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Description	Required?	Type
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:

  - 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; ApplicationFolderPrefi 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `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; `ApplicationFolderSuffi` can be combined with `ApplicationFolderRoot`.
- `ApplicationGroupSuffix` –the suffix for application groups.
- `ApplicationUserSuffix` –the suffix to apply to the application name the user sees.
- `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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migration mode parameters

Cmdlets modifying the cloud site configuration (`Import`, `Restore`, `Merge`, `New`, and `Sync`) support the following extra parameters to provide further flexibility.

- `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.

```
1             public class ActionResult
2             {
3
4                 public bool                          Overall_Success;
5                 public Dictionary<string, string>    Individual_Success;
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
6                   public object                       CustomResult;
7               }
```

`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.

```
1                   public class EvaluationResultData
2                   {
3
4                       public Dictionary<string, Dictionary<string,
                           ActionResultValues >> EvaluationResults;
5                       public int                  Added;
6                       public int                  Updated;
7                       public int                  Deleted;
8                       public int                  NoChange;
9                       public int                  TotalChanged;
10                      public EvaluationResults     OverallResult;
11                      public string               CloudBackupFolder;
12                      public string               SourceBackupFolder;
13                   }
14
15                  Where:
16                  public enum ActionResultValues
17                  {
18
19                      Add,
20                      Update,
21                      Delete,
22                      Identical,
23                      DoNothing
24                   }
25
26                  public enum EvaluationResults
27                  {
28
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
29                      Success,
30                      Failure,
31                      Skipped
32                  }
```

`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.

`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

September 6, 2025

This page lists all the cmdlets and parameters supported by the tool to trigger the backup and restore APIs that Web Studio uses.

Backup storage cmdlets

Get-BckRstrStorage

This cmdlet is applicable to only on-premises. Gets details for the storage where backups are saved.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 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.
`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
`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:

© 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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.
`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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ApplicationGroups
- ApplicationFolders
- 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.
`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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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.

© 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.

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.

© 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.
`BackupName`	The name of backup. The `.zip` extension is optional.

Remove backup cmdlet

Remove-BckRstrBackup

Removes one or more 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: 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.
`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.
`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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
`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
`Enabled`	The parameter to enable this backup schedule. `True` when enabled and **`false`** when disabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter	Description
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.
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter	Description
`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.
`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.

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.
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.

© 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.
`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.

© 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.
`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: 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.

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.
`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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot Automated configuration and additional information

September 6, 2025

> **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:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 autoconfig operation and the date and timestamp of the cmdlet execution. Logs do not auto-delete.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

`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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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*.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
```

> **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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.)

   ```
   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.

Autoscale™

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This feature is available only in Web Studio.

Autoscale is a feature that provides a consistent, high-performance solution to proactively power manage your machines. It aims to balance costs and user experience.

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)
- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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 Virtual Apps and Desktops supports. This includes various infrastructure platforms including XenServer, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere, and many more. For a complete list of supported platforms, see System requirements for Citrix Virtual Apps and Desktops.

> **Note:**
>
> When adding public cloud host connections to your deployment, you need Hybrid Rights License. For information about Hybrid Rights License, see Transition and Trade-Up (TTU) with Hybrid Rights. For information about adding a license, see Create a site.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

Watch a 2-minute video

The following video provides a quick tour of Autoscale.

This is an embedded video. Click the link to watch the video

Get started with Autoscale™

December 4, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Load index
- Autoscale and maintenance mode
- Machine cost
- Scale up a delivery group
- Scale down a Delivery Group
- Drain state

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, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 > Trends > Machine usage**.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Registered as available or is waiting to register after starting up
5. Drained and has no active sessions
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.

- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

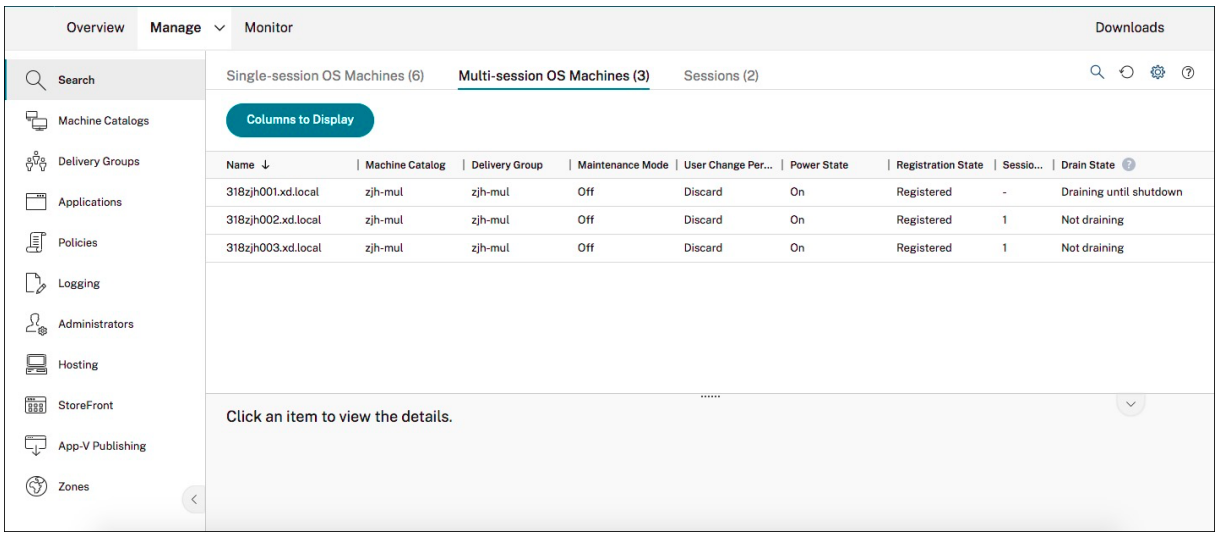
In Studio, you can display machines that are in drain state, letting you know which machines are about to shut down. Complete the following steps:

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

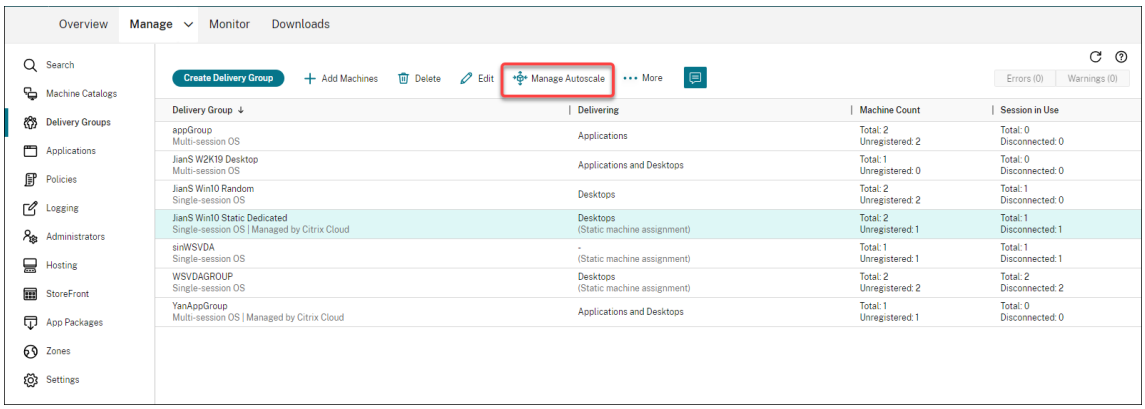


Enable Autoscale for a delivery group

Autoscale is disabled by default when you create a delivery group. To enable and configure Autoscale for a delivery group using Web Studio, follow these steps:

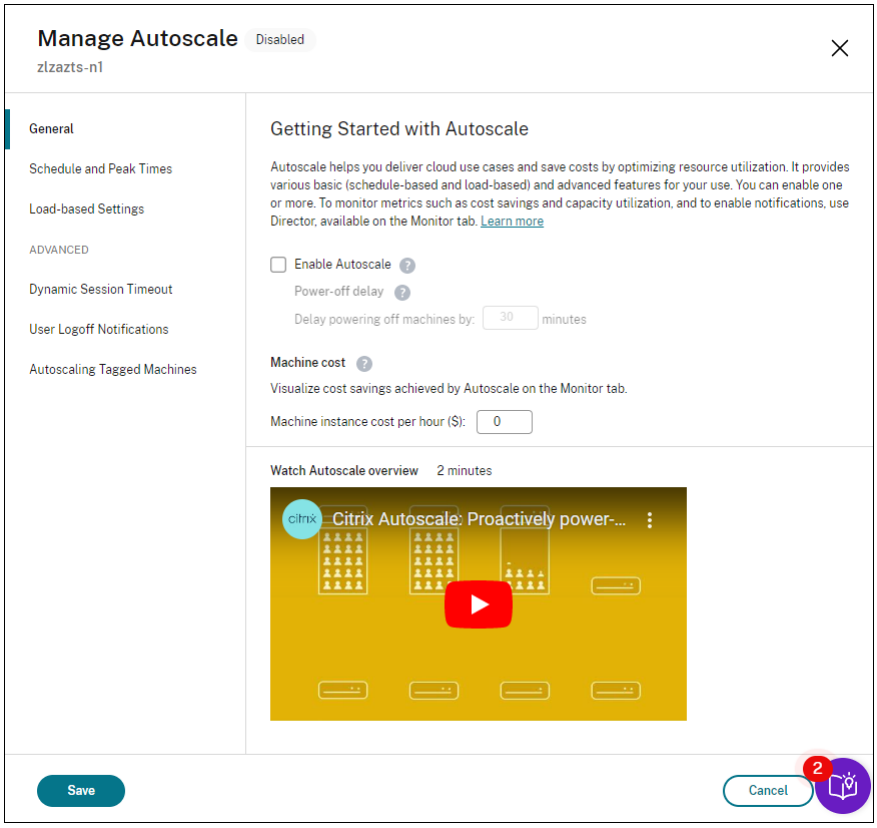
You can also use PowerShell commands to enable and configure Autoscale for a delivery group. For more information, see Broker PowerShell SDK commands.

1. 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** check box 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** check box. The options on the page turn gray to indicate that Autoscale is disabled for the selected delivery group.

> **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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exclude draining machines from autoscale calculations

This feature allows you to prevent machines, which are draining due to reboot schedules, from counting towards Autoscale capacity targets. By excluding these machines, you optimize resource provisioning and avoid over-provisioning.
For example: You have a delivery group of multi-session OS machines configured with Autoscale and regular reboot schedules. When machines enter a draining state for reboot, Autoscale typically still counts them as available capacity. This might trigger the provisioning of additional machines unnecessarily. By enabling this feature, you instruct Autoscale to ignore these draining machines when calculating capacity. This ensures that only actively available machines contribute to the target, which leads to more efficient resource utilization and reduced operational costs.

Applicability:
This feature applies to delivery groups containing **multi-session OS machines (RDS)**.
Limitations:

- This feature does not apply to single-session OS machines.
- When you configure Autoscale based on the "Number of machines"(rather than "Percentage"), the system does not exclude machines in a draining state from Autoscale calculations.

Important considerations:

- The property `ExcludeNaturalRebootDrainingFromAutoscale` is configured at the delivery group.
- The default value for the `ExcludeNaturalRebootDrainingFromAutoscale` property is `False`. This means draining machines are included in Autoscale calculations by default.

Prerequisites:

- You must configure a multi-session OS delivery group.
- You must enable and configure Autoscale for the target delivery group. Preferably, you use "Percentage of machines"for scaling.
- You must configure Restart Schedules for the delivery group to induce machines into a draining state.
  **How to configure:

You configure this feature at the delivery group level using a PowerShell command.

1. Ensure the feature toggle `ExcludeNaturalRebootDrainingFromAutoscale` is enabled. You can verify this by running `Get-ConfigEnabledFeature` in PowerShell and checking for the toggle in the output list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> If the toggle is disabled, you cannot modify the delivery group property.

2. Set the delivery group property to exclude draining machines**.

   a) **Open PowerShell** with administrative privileges.

   b) **Identify your multi-session OS delivery group**.

   c) **Set the `ExcludeNaturalRebootDrainingFromAutoscale` property to `$True`** for your delivery group using the `Set-BrokerDesktopGroup` cmdlet:

   ```
   Set-BrokerDesktopGroup -Name "<YourDeliveryGroupName>" -
       ExcludeNaturalRebootDrainingFromAutoscale $True
   ```

   Replace <`YourDeliveryGroupName`> with the actual name of your delivery group.

   d) **Verify the property is set to `True`** by running:

   ```
   Get-BrokerDesktopGroup -Name "<YourDeliveryGroupName>" |
       Select Name, ExcludeNaturalRebootDrainingFromAutoscale
   ```

   The output should show `ExcludeNaturalRebootDrainingFromAutoscale : True`.

3. Configure Autoscale and restart schedules (if not already configured)**
   Ensure your delivery group has Autoscale enabled and a Restart Schedule configured to cause machines to enter a draining state.

   a) In Citrix Studio, edit your delivery group.
   b) Go to **Manage Autoscale** and configure peak/off-peak schedules, ensuring Autoscale is enabled. If you intend for draining machines to be excluded, set your schedule based on "Percentage of machines".
   c) Go to **Restart Schedule** and create or edit a schedule that causes machines to enter a draining state (e.g., use "Graceful restart"for Cloud or "Re-start all machines after draining session"for On-prem deployments).

Monitoring and Troubleshooting:
Problem: Sessions occasionally launch onto draining machines even when you enable the feature.
Cause: This is expected behavior. Machines in a draining state are still available for session launches as a "last resort"if no other suitable non-draining machines are available. The feature primarily affects Autoscale calculations for provisioning/deprovisioning. It does not affect the broker's session launch logic itself.
Solution: This is not an issue but an intended design. To minimize sessions going to draining machines, ensure your Autoscale buffer and capacity are sufficient to keep enough non-draining machines available to meet demand.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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:

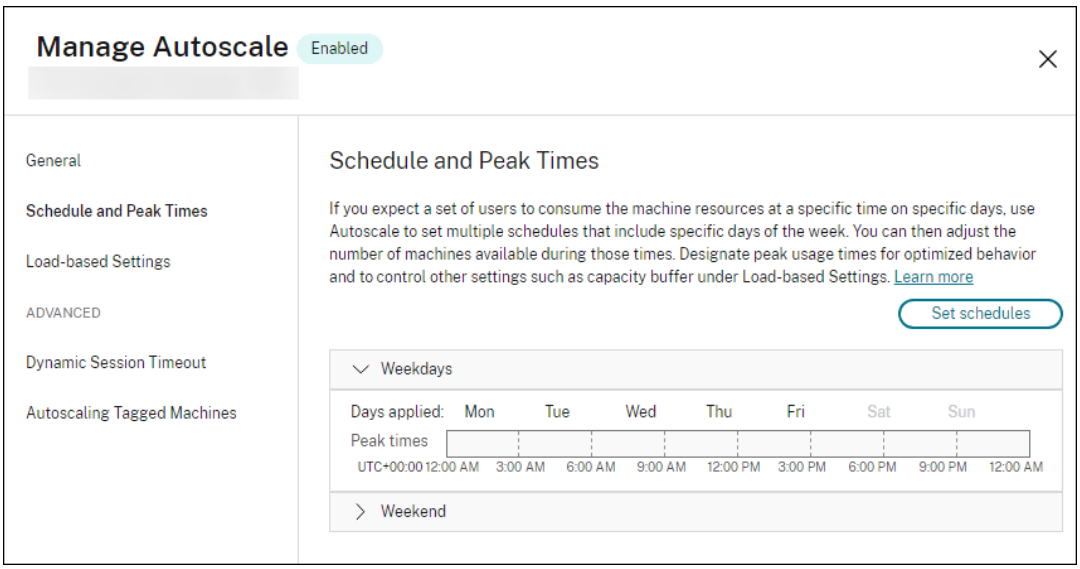
```
Set-BrokerDesktopGroup "Desktop Group Name" -
    AutomaticPowerOnForAssigned $True
```

- 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:

```
1 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 Director.

- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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 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.

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 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

September 6, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 10% during peak and off-peak times. By default, the **Weekend** schedule keeps no machines powered on.

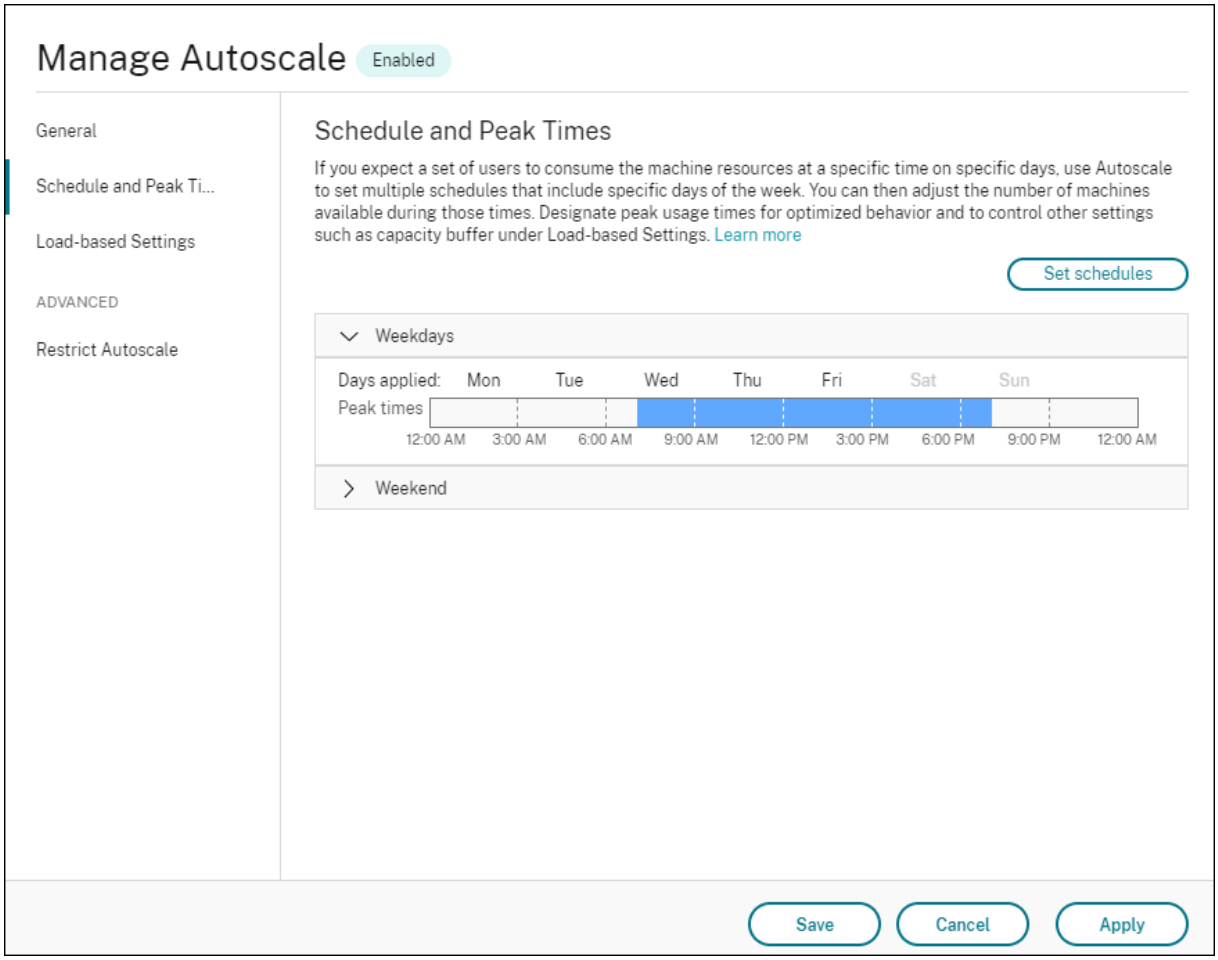
> **Note:**
>
> Autoscale treats only those machines that are registered with the site as part of the available capacity in the calculations it makes. "Registered" means that the machine is available for use or already in use. Doing so ensures that only machines that can accept user sessions are included in the capacity for the delivery group.

User interfaces

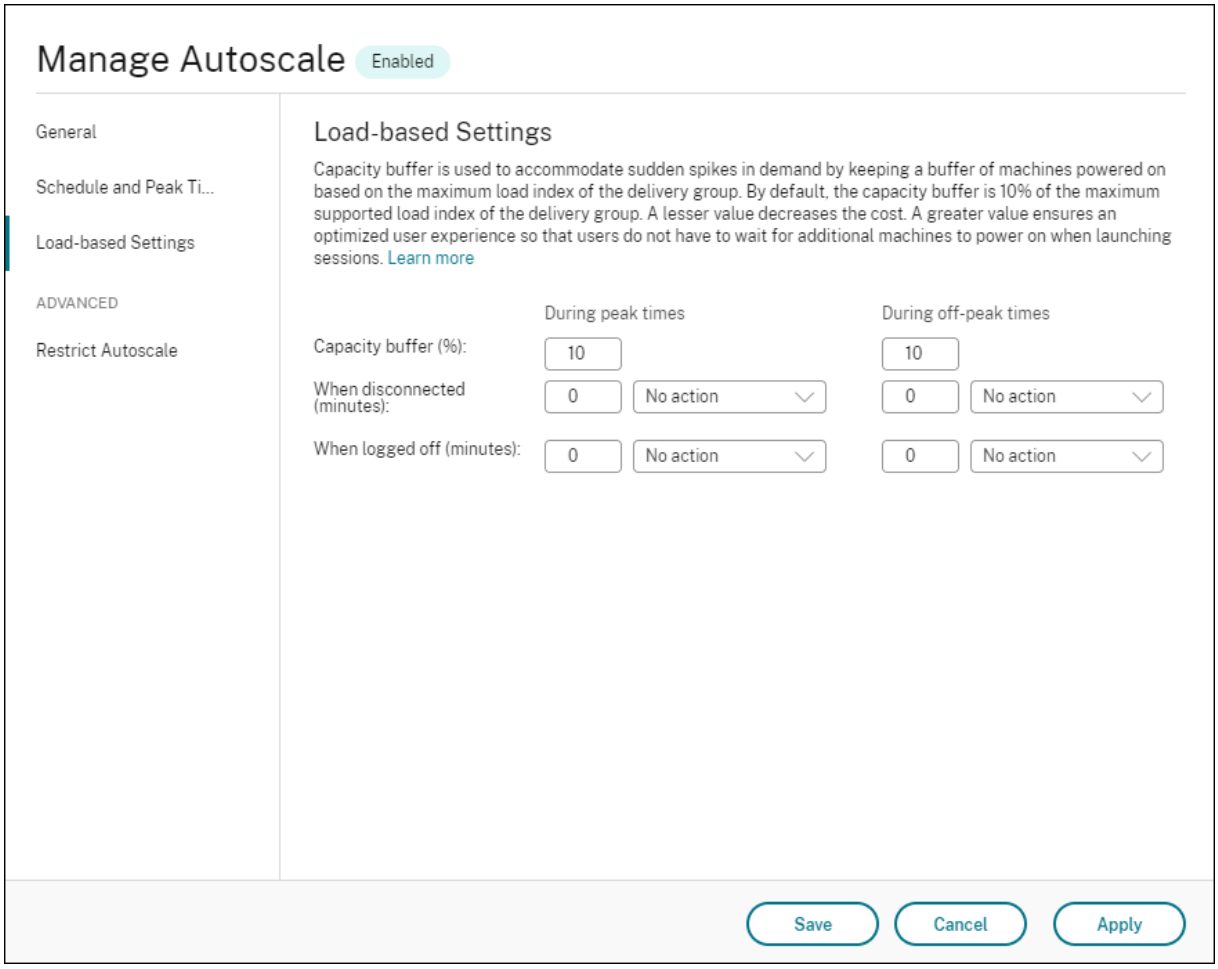
There are three types of user interfaces to be aware of.

User interface for *single-session OS static delivery groups*:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

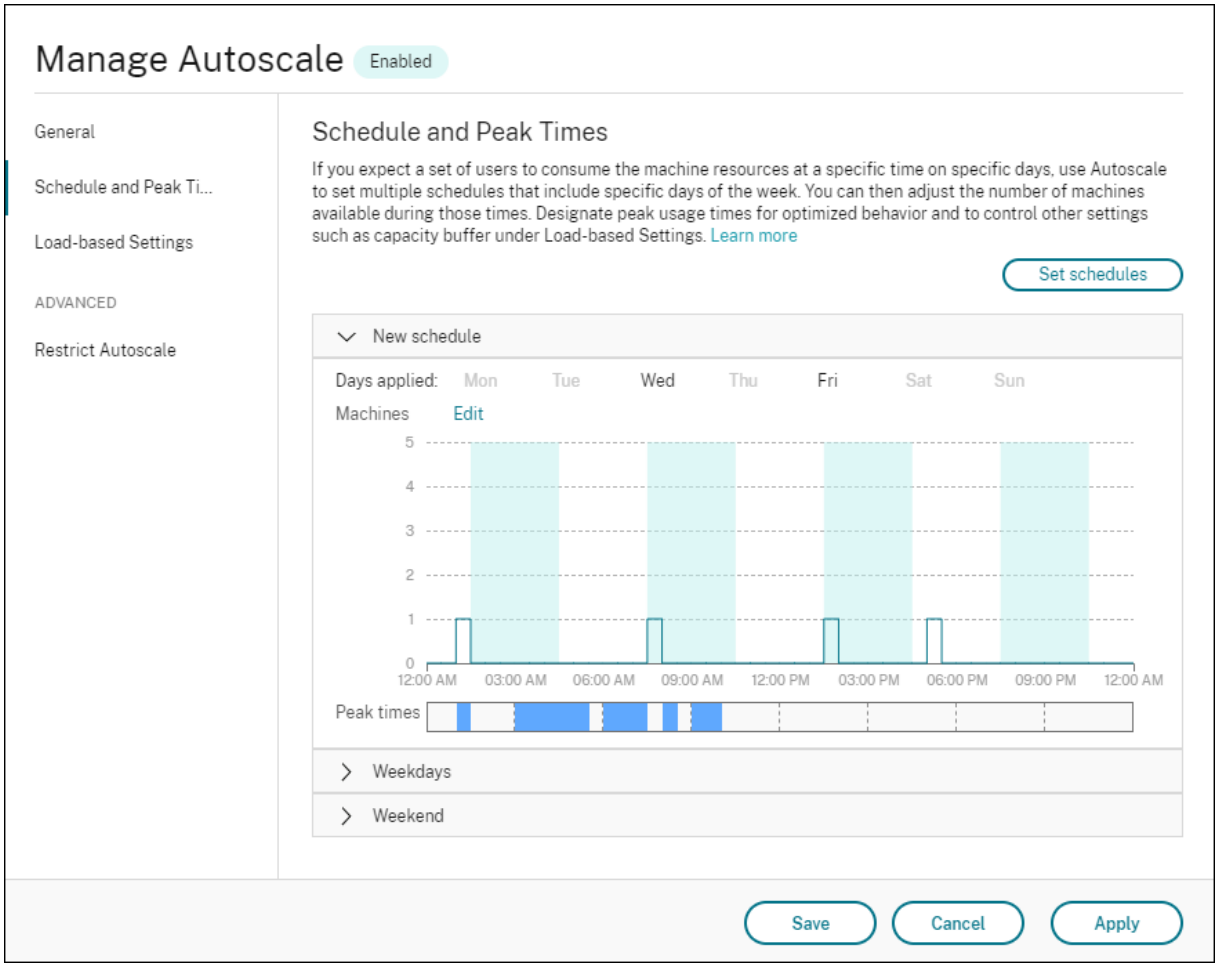


© 1997–2026 Citrix Systems, Inc. All rights reserved.

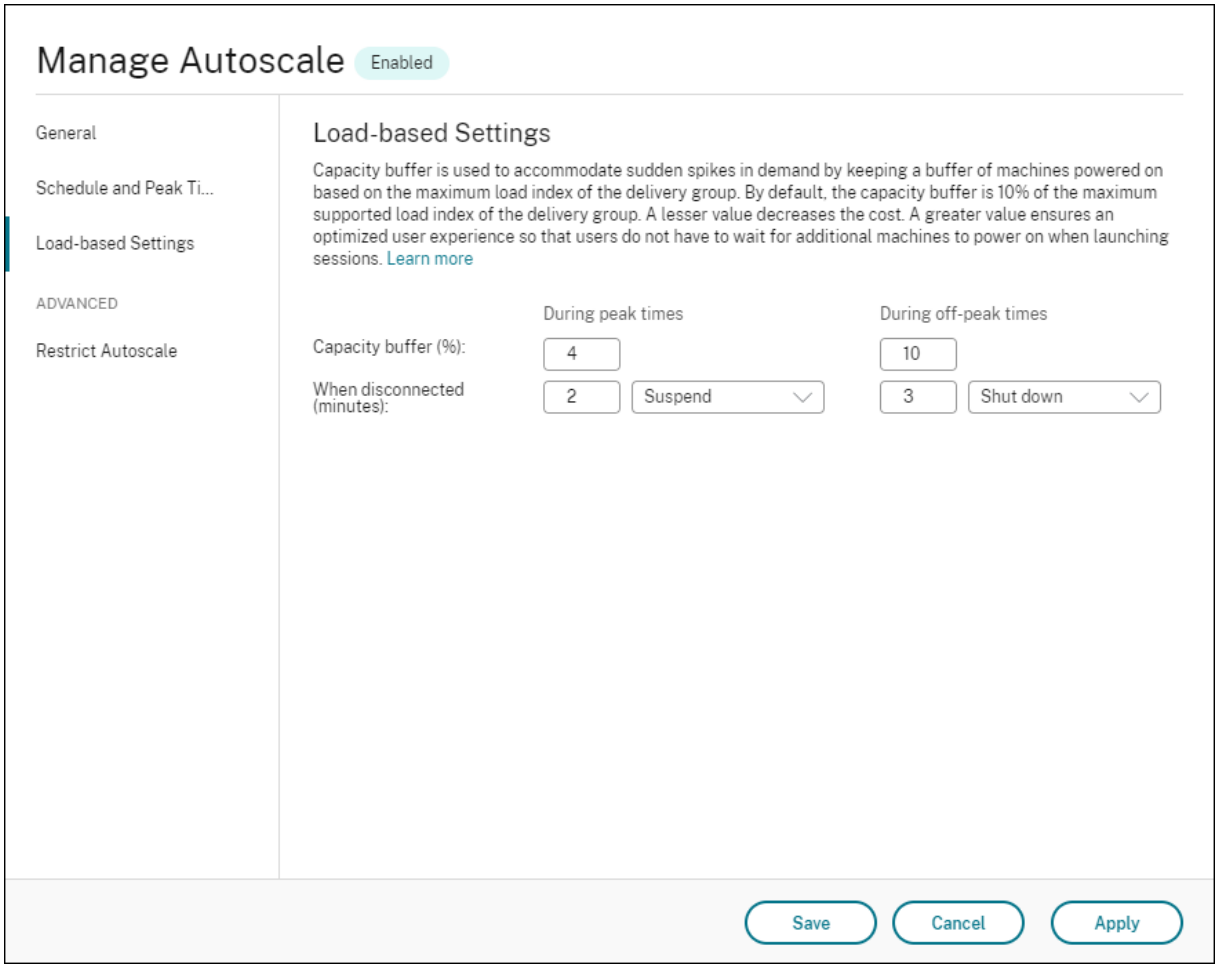


Autoscale user interface for *single-session OS random delivery groups*:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

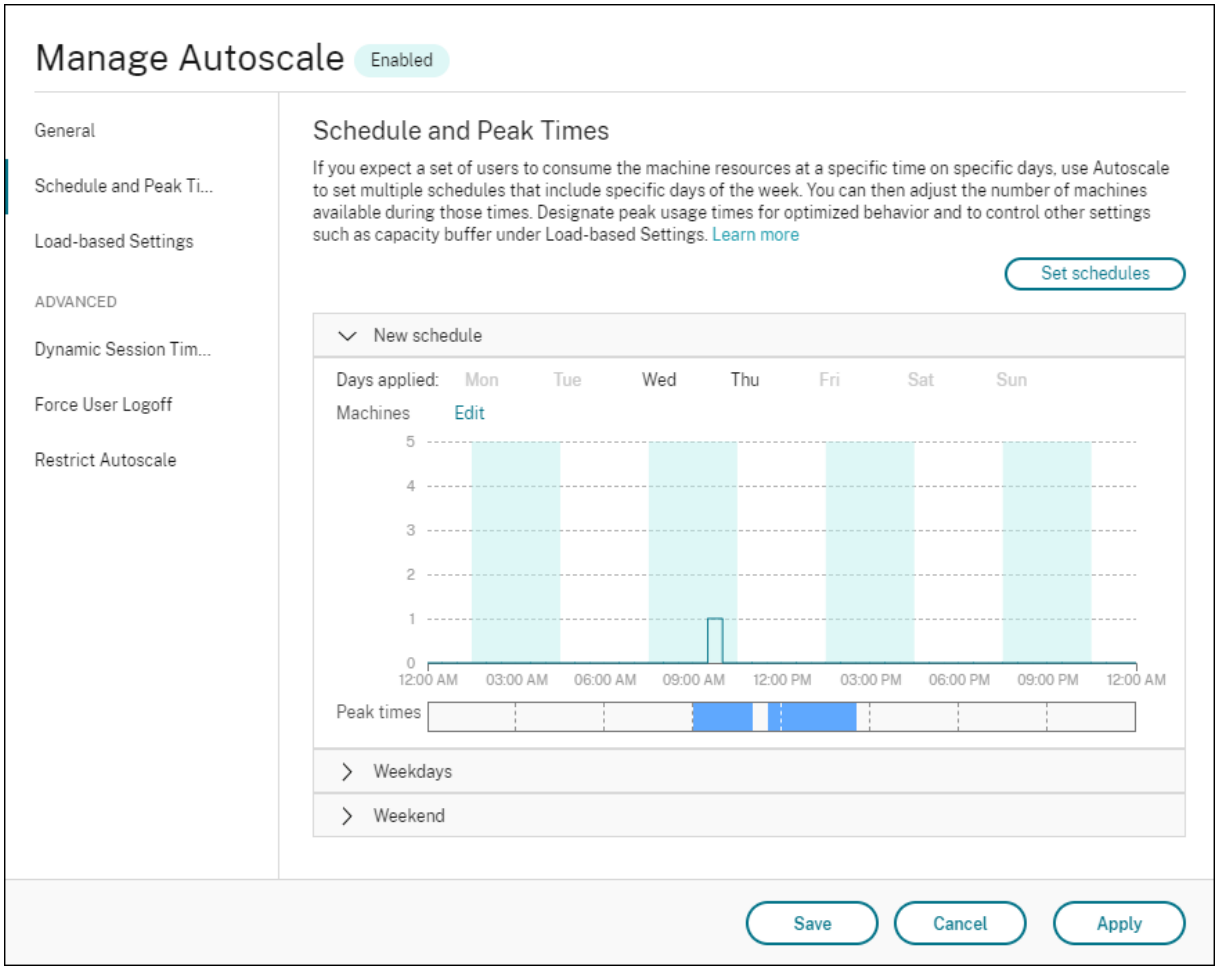


© 1997–2026 Citrix Systems, Inc. All rights reserved.

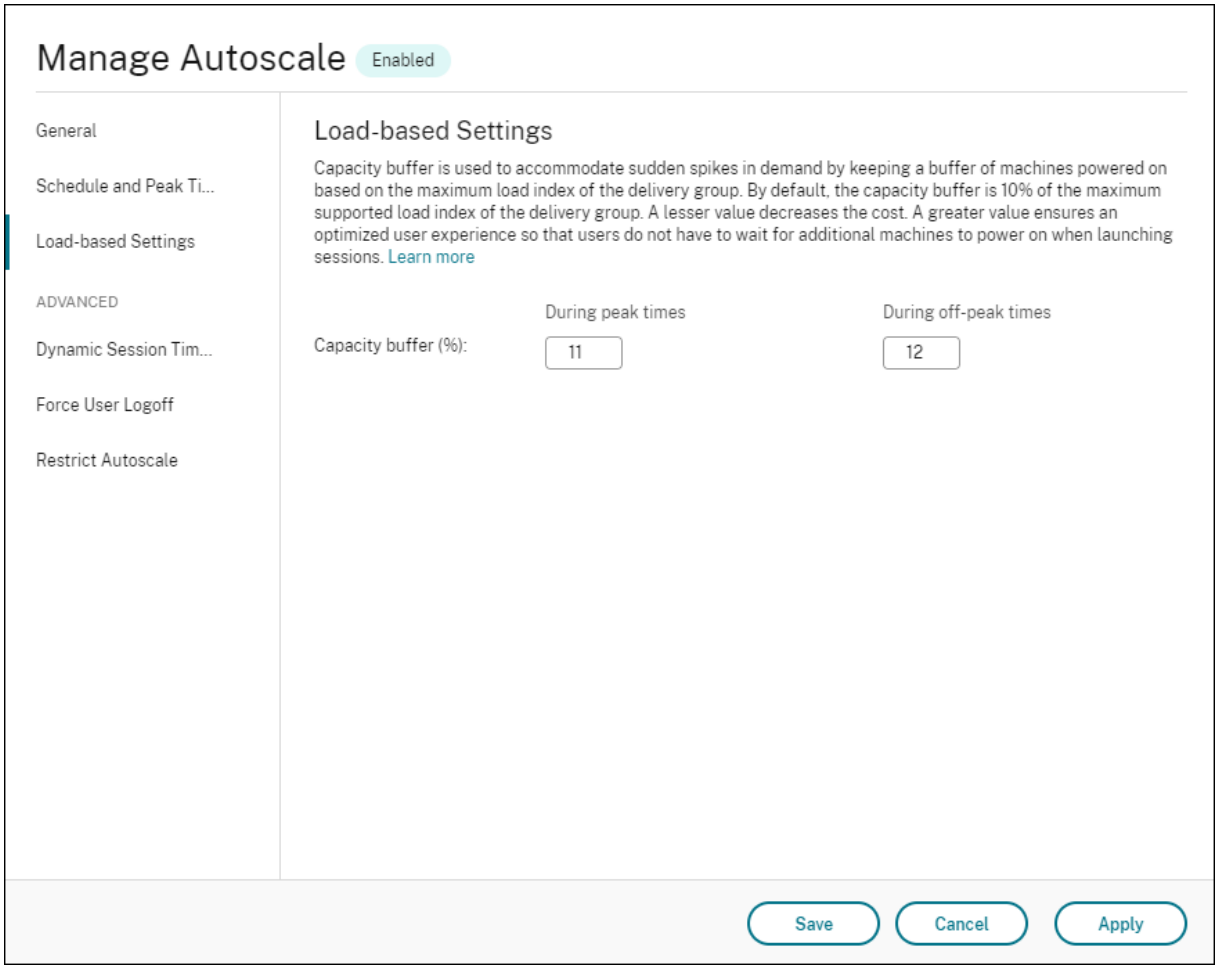


Autoscale user interface for *multi-session OS delivery groups*:

© 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.

> **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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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.

> **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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.

> **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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
  - 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

> **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.

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,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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%. 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.

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.

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.

© 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 (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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 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

    - 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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

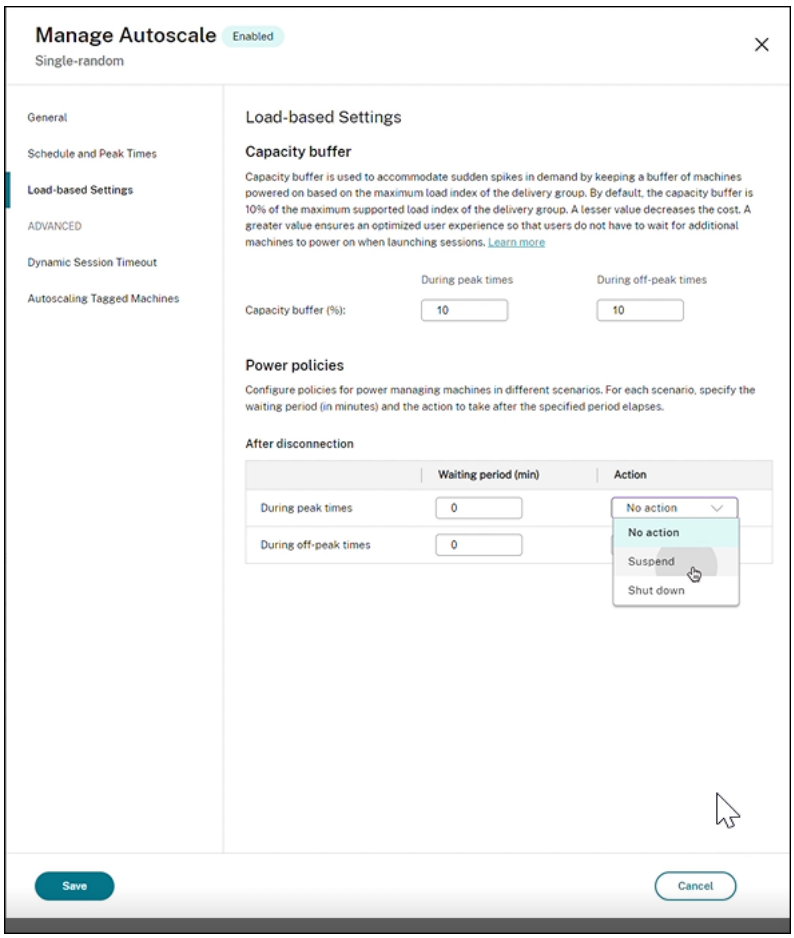
Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the total number of machines in the delivery group. By default, the capacity buffer is 10% of the total number of machines in the delivery group.

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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

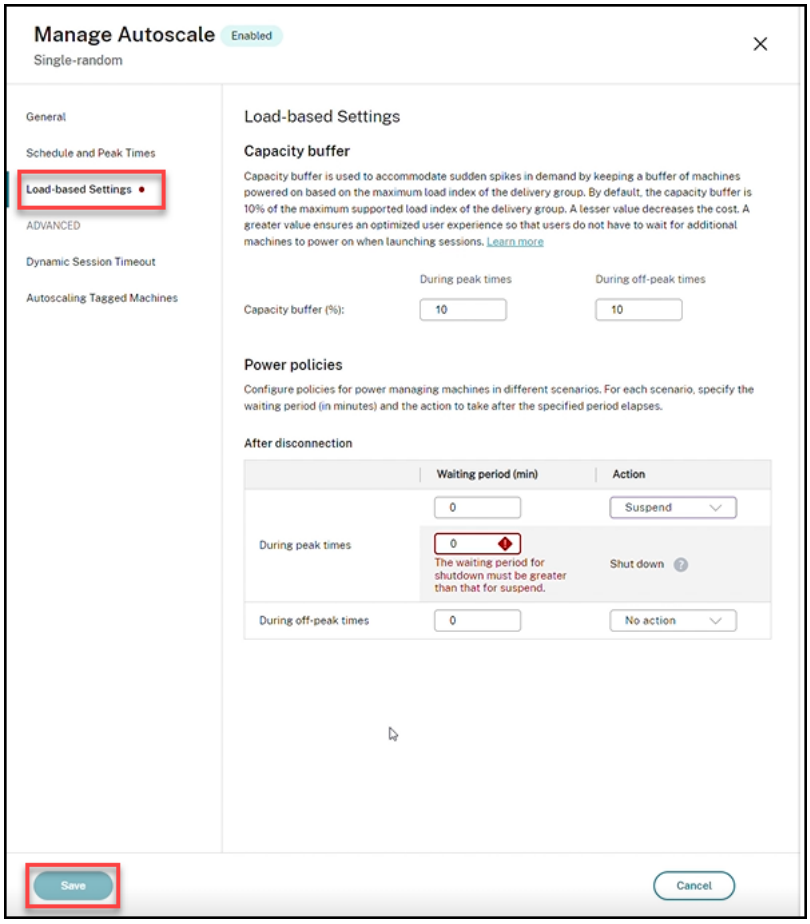


After disconnection, the following settings are applicable for both during peak times and during off-peak times:

- You can set the wait time in minutes and actions like, no action, suspend, or shut down from the drop down.
- If 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 is suspended. After the end of the second wait time, the machine will 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 shut down.

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%.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.
- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 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:

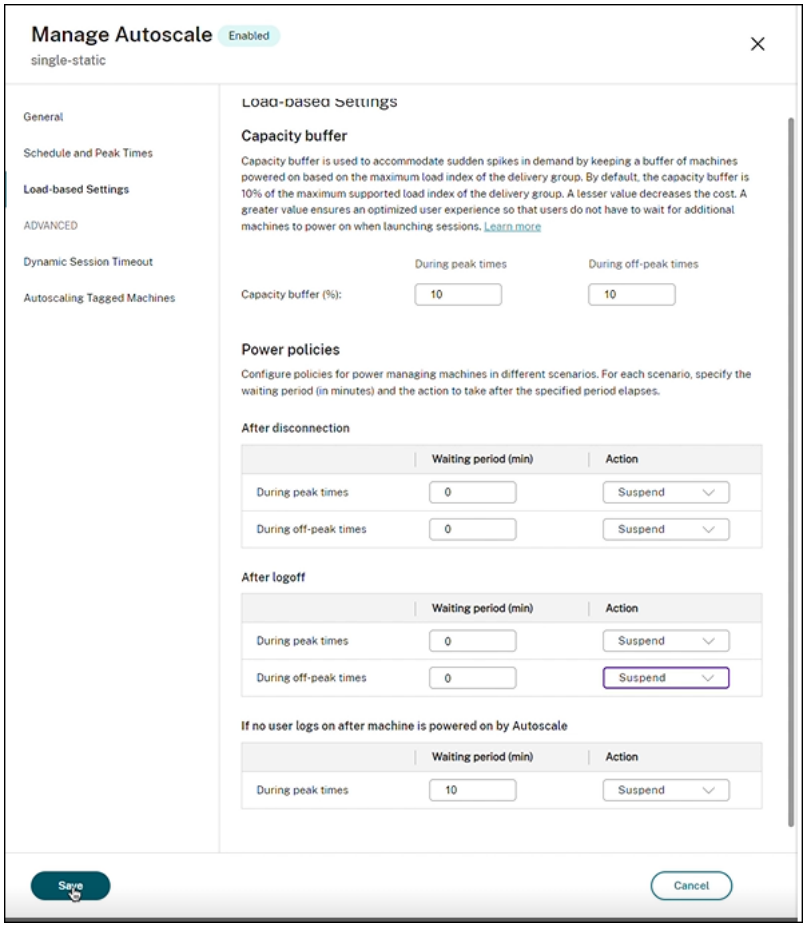
- The capacity buffer works only when the delivery group has one or more unassigned machines.
- If the delivery group has no unassigned machines (all machines in the delivery group are assigned), the capacity buffer does not play a role in powering machines on or off.
- The `AutomaticPowerOnForAssignedDuringPeak` property determines whether assigned machines are powered on during peak times. If it is set to true, Autoscale keeps the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 are applicable for Single-session OS random delivery groups and Single-session OS static delivery groups.



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.

© 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**
  - 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.
  - The unassigned machine M6 is waiting to serve a desktop to an incoming, unassigned user.
- End of schedule –06:00 PM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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

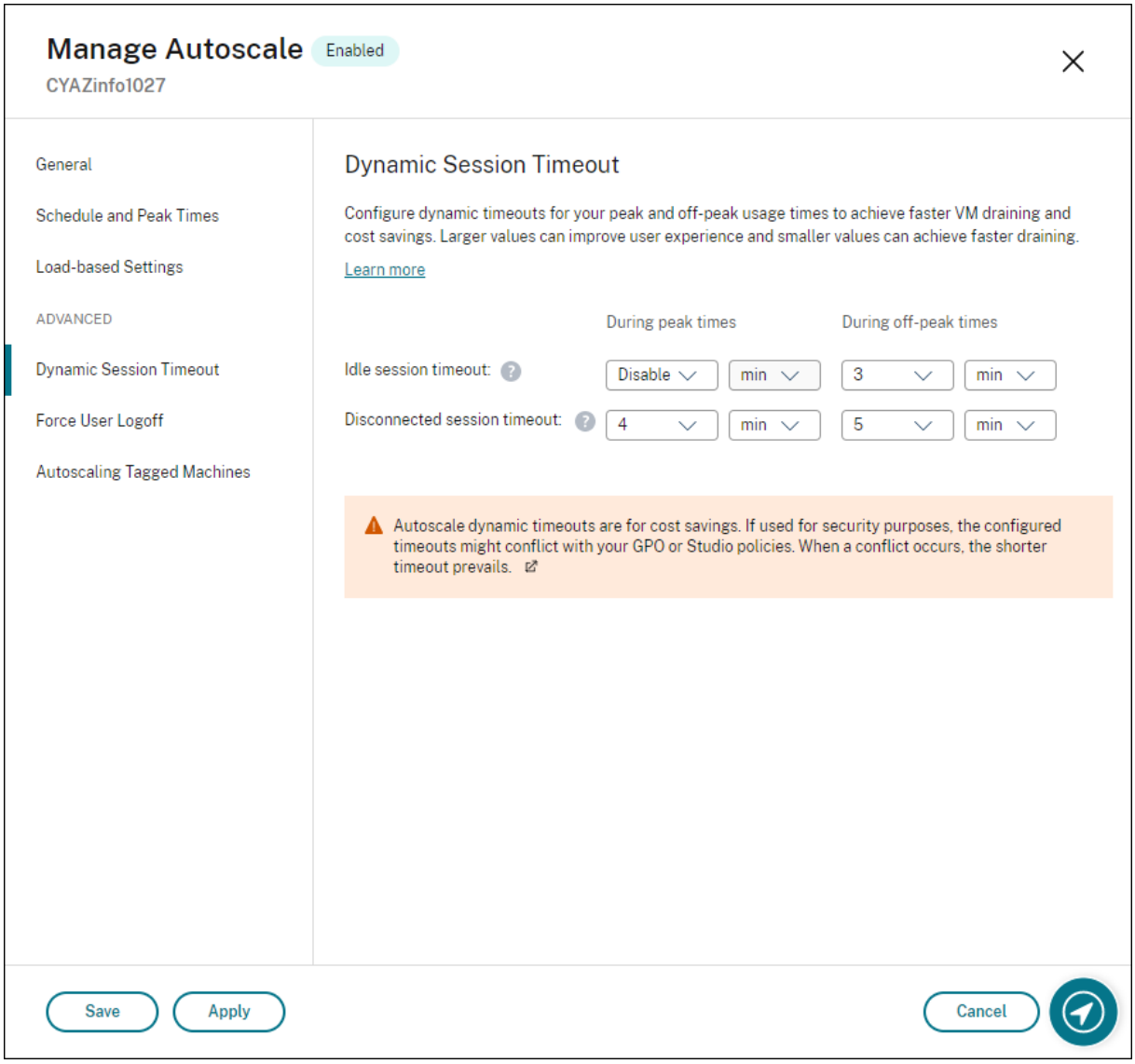
September 6, 2025

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 are not able to disconnect idle sessions within 10 minutes of being idle. A lesser value removes lingering sessions sooner, thus reducing costs.

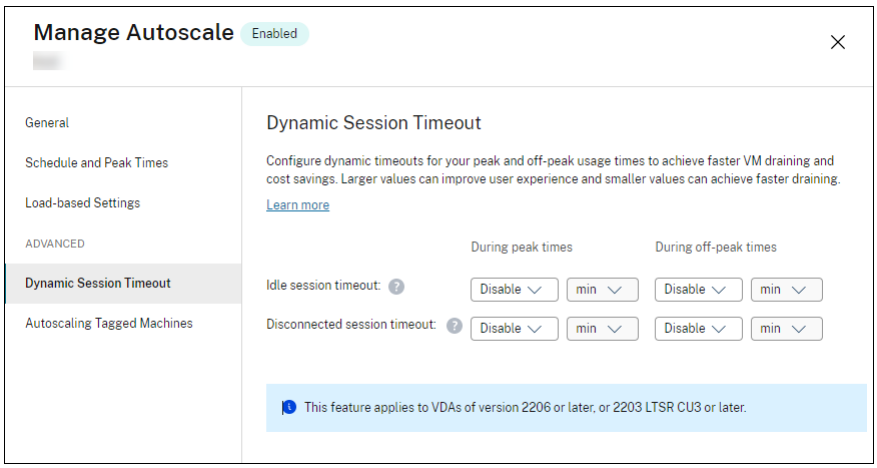
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Autoscale™ dynamic timeouts are for cost savings. If used for security purposes, the configured timeouts might conflict with your GPO or Manage console 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.

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 can 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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)

September 6, 2025

> **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.

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 the Manage console or PowerShell.

Use the Manage console to autoscale certain tagged machines

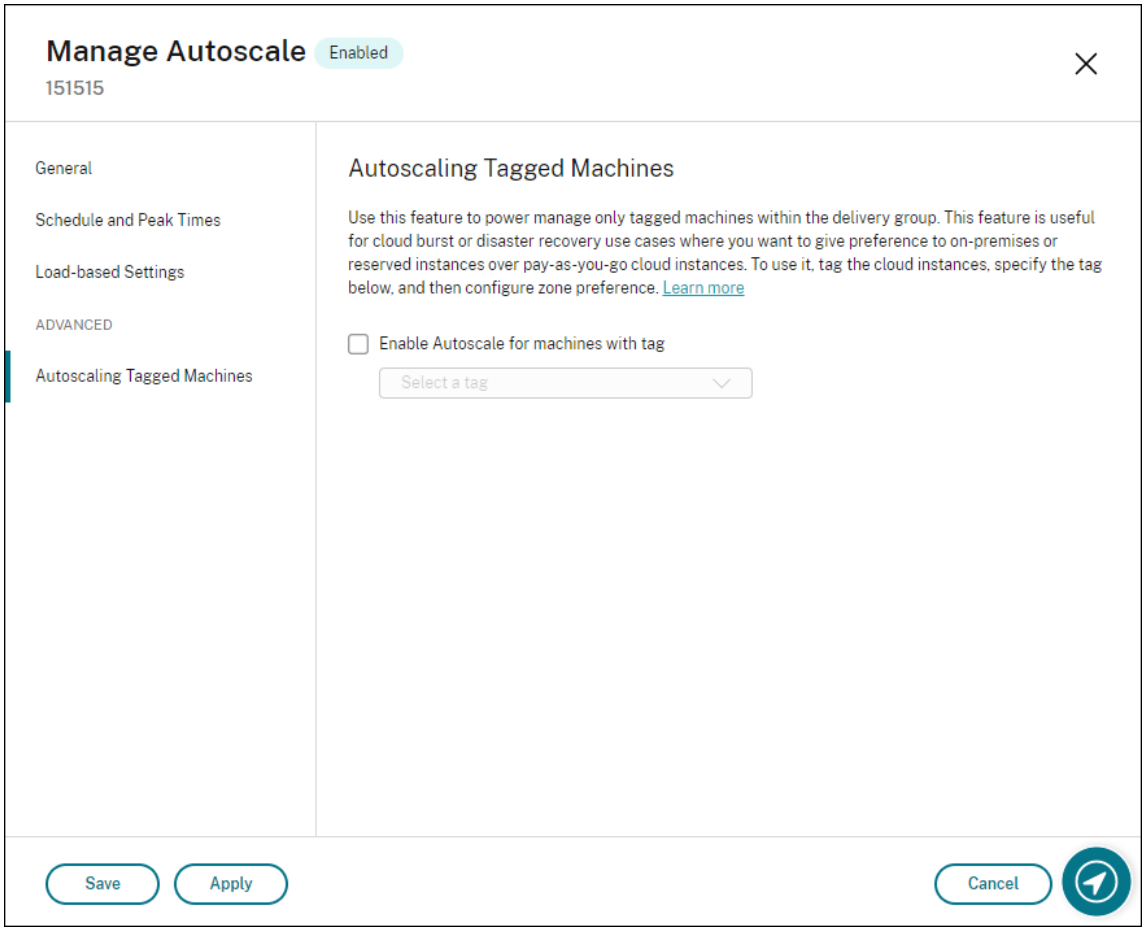
To autoscale certain tagged machines, complete the following steps:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

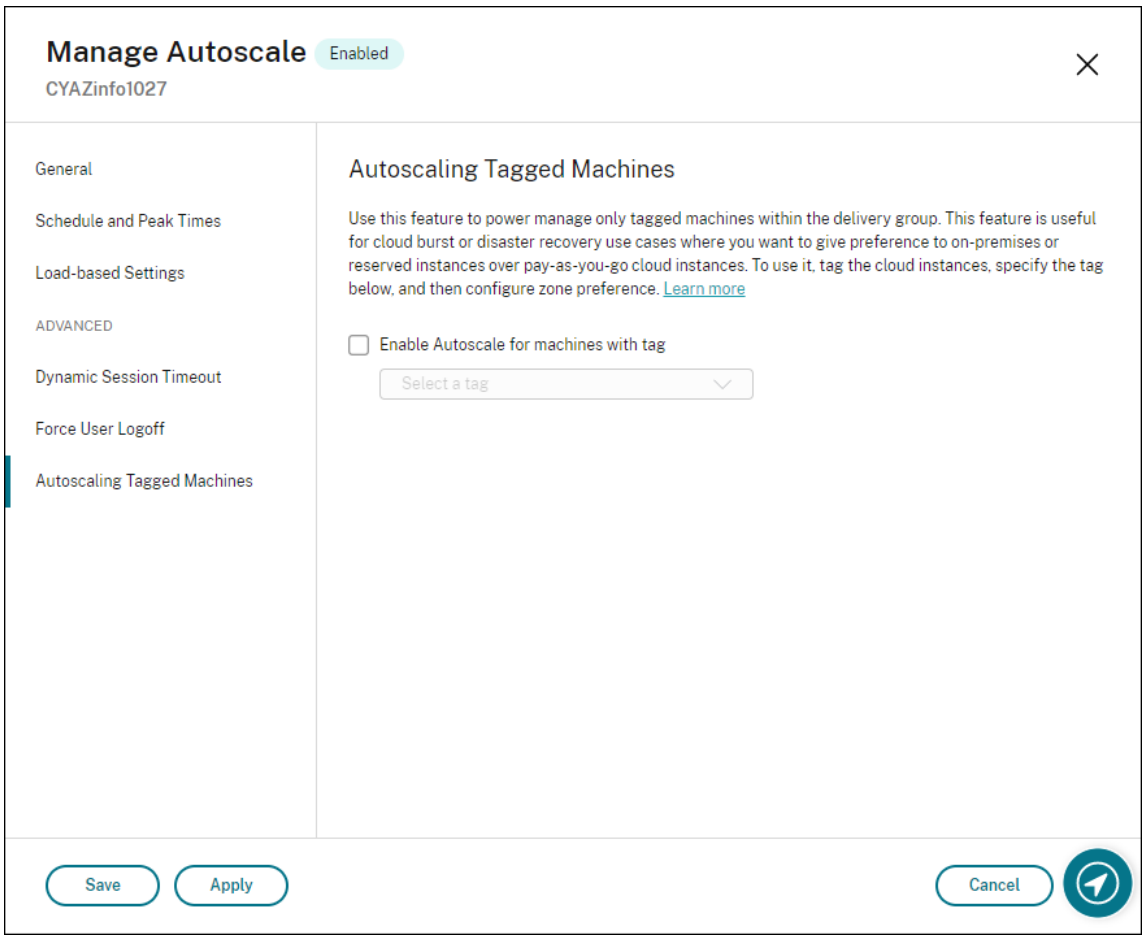
3. On the **Autoscaling Tagged Machines** page, select **Enable Autoscale for machines with tag**, select a tag from the list, and then click **Apply** to save your changes.

   User interface for single-session OS *static* and *random* delivery groups:



   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**.

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,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> go to the **Autoscaling Tagged Machines** page, remove the invalid tag, and then click **Apply** to save your changes.

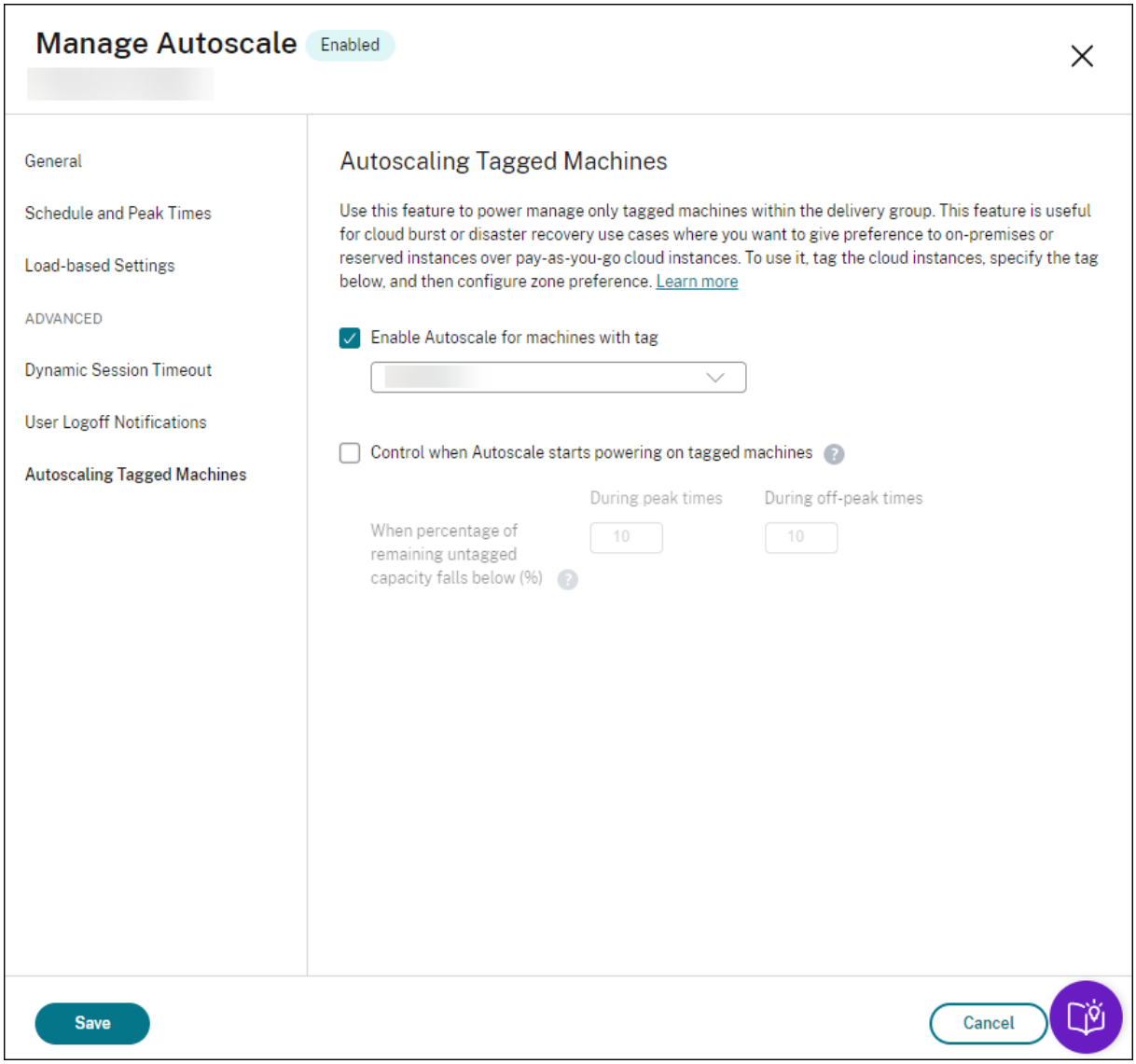
Control when Autoscale powers on resources

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 un-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> tagged 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").
   - 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/.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 -RestrictAutoscal $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**
  - 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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
  - 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
  - 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sessions are not directed to be hosted on machine M6 as long as the on-premises machines have available capacity.

User logoff notifications (formerly force user logoff)

September 6, 2025

> **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.

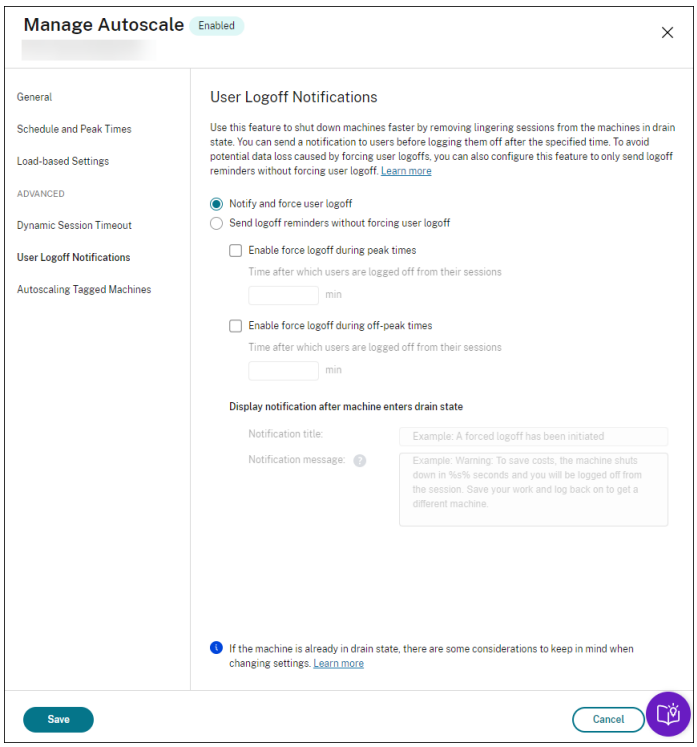
You have the following two options:

- **Notify and force user logoff**
- **Send logoff reminders without forcing user logoff**

Notify and force user logoff

If selected, Autoscale logs off users from their sessions after the times specified below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

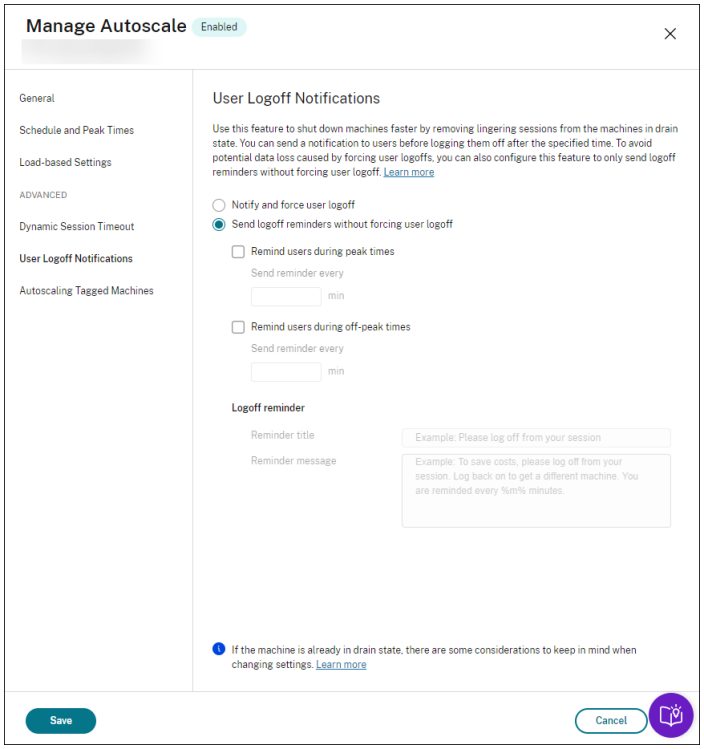
Display notification after machine enters drain state. Lets you send notifications to users after their machine enters drain state.

- **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`.
- **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`.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analyze the effectiveness of Autoscale™ settings

September 6, 2025

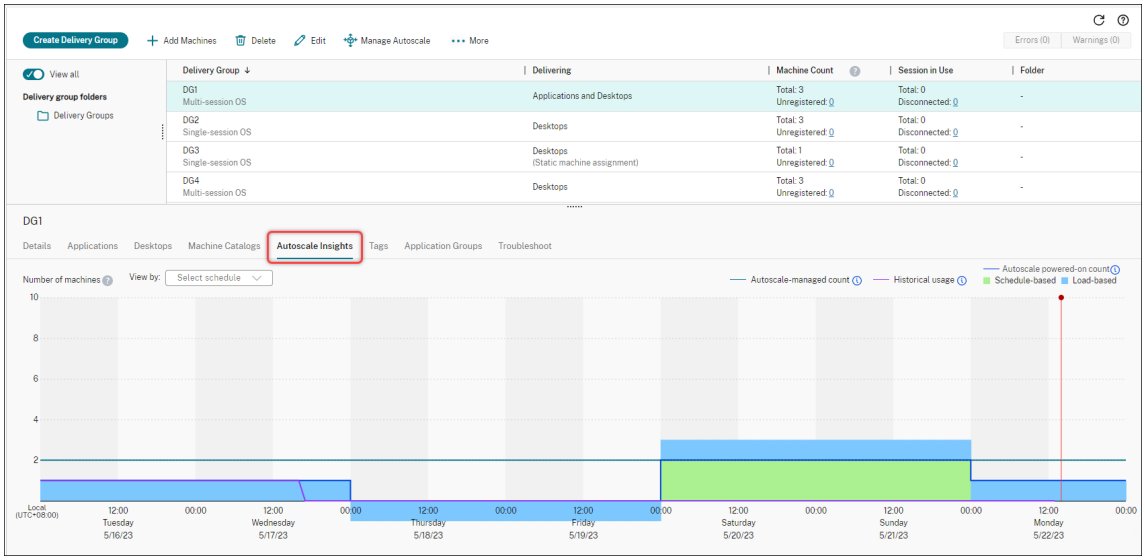
This article describes how to analyze the effectiveness of the Autoscale settings based on machine usage from the previous week. Through the analysis, you can gain these insights into the effectiveness of Autoscale settings:

- 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.



   * The red vertical line identifies the current time.

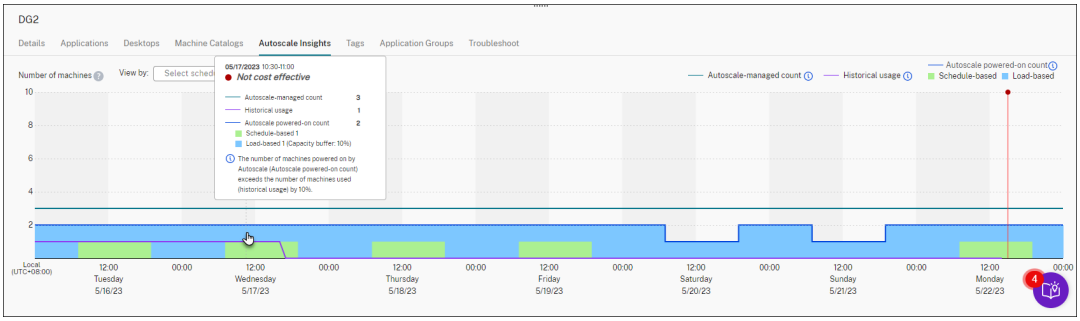
   The following table provides descriptions of the metrics shown in this graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

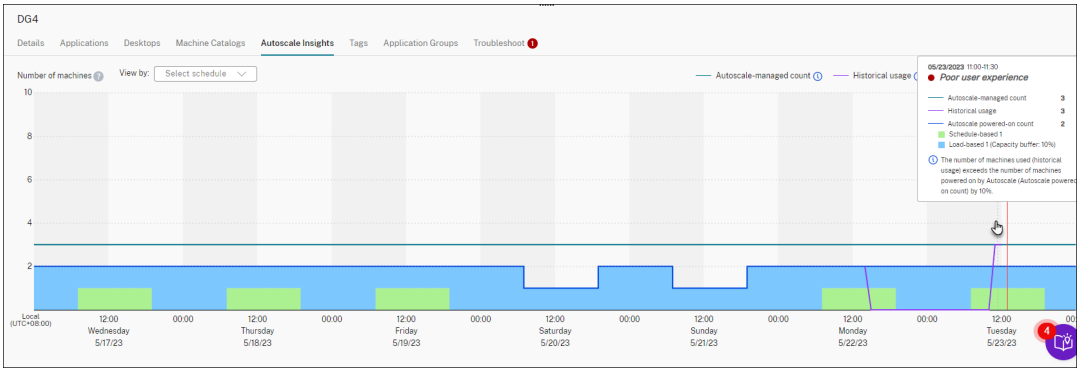
3. To check the effectiveness of Autoscale settings at a specific time slot, hover your mouse over that slot on the graph. An information box appears, showing the comparison results and detailed machine counts:

   - **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.

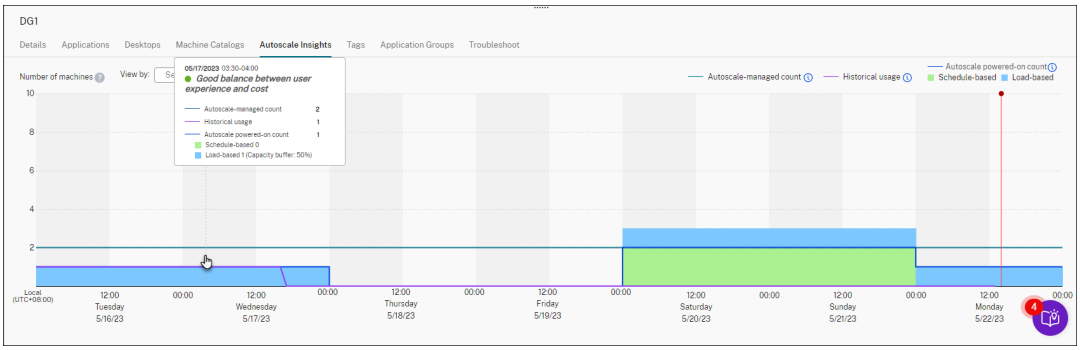


   - **Poor user experience**. The historical usage is more than 110% of the Autoscale settings (Autoscale powered-on count). As a result, users might experience longer wait times for machines to power on.

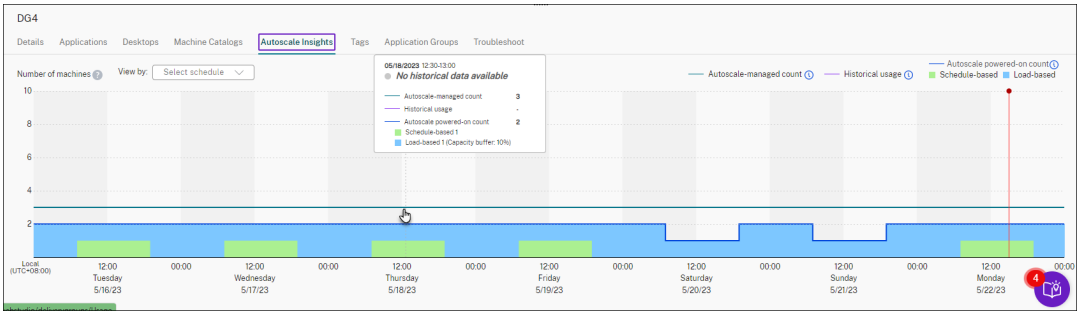
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **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.



- **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Broker PowerShell SDK commands

September 6, 2025

You can configure Autoscale for delivery groups using the Broker PowerShell SDK. To configure Autoscale using PowerShell commands, you must use PowerShell SDK version 7.21.0.12 or later. For more information about the PowerShell SDKs, 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

- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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"-SettlementPeriodBeforeAutoSh 30.`

Configure the **machine instance cost** setting

- 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`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 } } )
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte`
  `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."

Citrix Insight Services

September 13, 2025

Citrix Insight Services (CIS) is a Citrix platform for instrumentation, telemetry, and business insight generation. Its instrumentation and telemetry capabilities enable technical users (customers, partners, and engineers) to self-diagnose and fix problems and optimize their environments. For details and the latest information about CIS and how it works, see https://cis.citrix.com (Citrix account credentials required).

All information uploaded to Citrix is used for troubleshooting and diagnostic purposes, and improving the quality, reliability, and performance of products, subject to:

- Citrix Insight Services Policy at https://cis.citrix.com/legal
- Citrix Privacy Policy at https://www.cloud.com/privacy-policy

This Citrix Virtual Apps and Desktops™ release supports the following technologies.

- Citrix Virtual Apps and Desktops install and upgrade analytics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Customer Experience Improvement Program (CEIP)
- Citrix Call Home
- Citrix Scout

In addition to (and separate from) CIS and Citrix Analytics: Google Analytics are collected (and later uploaded) automatically when you install (or upgrade) Studio. After installing Studio, you can change this setting with the registry key HKLM\Software\Citrix\DesktopStudio\GAEnabled. A value of 1 enables collection and upload, 0 disables collection and upload.

Install and upgrade analytics

When you use the full-product installer to deploy or upgrade Citrix Virtual Apps and Desktops components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences.

The information is stored locally under %ProgramData%\Citrix\CTQs.

Automatic upload of this data is enabled by default in both the graphical and command line interfaces of the full-product installer.

- You can change the default value in a registry setting. If you change the registry setting before installing/upgrading, that value is used when you use the full-product installer.
- You can override the default setting if you install/upgrade with the command line interface by specifying an option with the command.

Control automatic uploads:

- Registry setting that controls automatic upload of install/upgrade analytics (default = 1):
  - Location: HKLM:\Software\Citrix\MetaInstall
  - Name: SendExperienceMetrics
  - Value: 0 = disabled, 1 = enabled
- Using PowerShell, the following cmdlet disables automatic upload of install/upgrade analytics:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
   SendExperienceMetrics -PropertyType DWORD -Value 0
```

- To disable automatic uploads with the XenDesktopServerSetup.exe or XenDesktopVDASetup.exe command, include the `/disableexperiencemetrics` option.

  To enable automatic uploads with the XenDesktopServerSetup.exe or XenDesktopVDASetup.exe command, include the `/sendexperiencemetrics` option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Customer Experience Improvement Program

When you participate in the Citrix Customer Experience Improvement Program (CEIP), anonymous statistics and usage information are sent to Citrix to help Citrix improve the quality and performance of Citrix products. For more information, see https://more.citrix.com/XD-CEIP.

Enrollment during Site creation or upgrade

You are automatically enrolled in CEIP when you create a Site (after you install the first Delivery Controller™). The first upload of data occurs approximately seven days after you create the Site.

You can stop your participation at any time after creating the Site. Select the **Settings** node in the Web Studio left pane and turn off the **Citrix Customer Experience Improvement Program** setting.

When you upgrade a Citrix Virtual Apps and Desktops deployment:

- If you upgrade from a version that did not support CEIP, you are asked if you want to participate.
- If you upgrade from a version that supported CEIP, and participation was enabled, CEIP is enabled in the upgraded Site.
- If you upgrade from a version that supported CEIP, and participation was disabled, CEIP is disabled in the upgraded Site.
- If you upgrade from a version that supported CEIP, and participation is unknown, you are asked if you want to participate.

The collected information is anonymous, so it cannot be viewed after it is uploaded to Citrix Insight Services.

Enrollment when installing a VDA

By default, you are automatically enrolled in CEIP when you install a Windows VDA. You can change this default in a registry setting. If you change the registry setting before installing the VDA, that value is used.

Registry setting that controls automatic enrolment in CEIP (default = 1):

Location: HKLM: \Software\Citrix\Telemetry\CEIP
Name: Enabled
Value: 0 = disabled, 1 = enabled

By default, the `Enabled` property is hidden in the registry. When it remains unspecified, the automatic upload feature is enabled.

Using PowerShell, the following cmdlet disables enrollment in CEIP:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
    Enabled -PropertyType DWORD -Value 0
```

The collected runtime datapoints are periodically written as files to an output folder (default %programdata%/Citrix/VdaCeip).

The first upload of data occurs approximately seven days after you install the VDA.

Enrollment when installing other products and components

You can also participate in CEIP when you install related Citrix products, components, and technologies, such as Citrix Provisioning™, AppDNA, Citrix License Server, Citrix Workspace™ app for Windows, Universal Print Server, and Session Recording. See their documentation for details about installation and participation default values.

Citrix Call Home

When you install certain components and features in Citrix Virtual Apps and Desktops, you are offered the opportunity to participate in Citrix Call Home. Call Home collects diagnostic data and then periodically uploads telemetry packages containing that data directly to Citrix Insight Services (via HTTPS on default port 443) for analysis and troubleshooting.

In Citrix Virtual Apps and Desktops, Call Home runs as a background service under the name Citrix Telemetry Service.

The Call Home scheduling functionality is also available in Citrix Scout. For details, see Citrix Scout.

What is collected

Citrix Diagnostic Facility (CDF) tracing logs information that can be useful for troubleshooting. Call Home collects a subset of CDF traces that can be helpful when troubleshooting common failures, for example, VDA registrations and application/desktop launches. This technology is known as always-on tracing (AOT). AOT logs are saved to disk at C:\ProgramData\Citrix\TelemetryService\CitrixAOT.

> **Note:**
>
> The `ProgramData` folder is hidden. To reveal it, click **View** > **Show** > **Hidden items**.

Call Home does not collect any other Event Tracing for Windows (ETW) information, nor can it be configured to do so.

Call Home also collects other information, such as:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Registries created by Citrix Virtual Apps and Desktops under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Windows Management Instrumentation (WMI) information under the Citrix namespace.
- List of processes running.
- Crash dumps of Citrix processes that are stored in %PROGRAM DATA%\Citrix\CDF.
- Installation and upgrade information. This can include the full product metainstaller log, failing MSI logs, output from the MSI log analyzer, StoreFront™ logs, Licensing compatibility check logs, and results from preliminary site upgrade tests.

The trace information is compressed as it is collected. The Citrix Telemetry Service retains a maximum of 10 MB of compressed recent trace information, with a maximum time limit of eight days.

- Compressing data allows Call Home to maintain a small footprint on the VDA.
- Traces are held in memory to avoid IOPs on provisioned machines.
- The trace buffer uses a circular mechanism to retain traces in memory.

Call Home collects the key datapoints listed in Call Home key datapoints.

Configure and manage summary

You can enroll in Call Home when using the full-product installation wizard or later, using PowerShell cmdlets. When you enroll, by default, diagnostics are collected and uploaded to Citrix every Sunday at approximately 3:00 AM, local time. The upload is randomized with a two hour interval from the specified time. This means an upload using the default schedule occurs between 3:00 AM and 5:00 AM.

If you do not want to upload diagnostic information on a scheduled basis (or if you want to change a schedule), you can use PowerShell cmdlets to manually collect and upload diagnostics or store them locally.

When you enroll in scheduled Call Home uploads and when you manually upload diagnostic information to Citrix, you provide Citrix account or Citrix Cloud™ credentials. Citrix exchanges the credentials for an upload token that is used to identify the customer and upload the data. The credentials are not saved.

When an upload occurs, a notification is emailed to the address associated with the Citrix account.

If you enable Call Home when you install a component, you can disable it later.

Prerequisites

- The machine must be running PowerShell 3.0 or later.
- The Citrix Telemetry Service must be running on the machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The system variable `PSModulePath` must be set to Telemetry's install path, for example, C:\Program Files\Citrix\Telemetry Service\.

Enable Call Home during component installation

During VDA installation or upgrade: When you install or upgrade a Virtual Delivery Agent using the graphical interface in the full-product installer, you are asked if you want to participate in Call Home. There are two options:

- Participate in Call Home.
- Do not participate in Call Home.

If you're upgrading a VDA and previously enrolled in Call Home, that wizard page does not appear.

During Controller installation or upgrade: When you install or upgrade a Delivery Controller using the graphical interface, you are asked if you want to participate in Call Home. There are three options:

When you're installing a Controller, you cannot configure information on the Call Home page in the installation wizard if that server has an Active Directory GPO with the policy setting "Log on as a service" applied. For details, see CTX218094.

If you're upgrading a Controller and previously enrolled in Call Home, you're not asked about participating.

PowerShell cmdlets

The PowerShell help provides comprehensive syntax, including descriptions of cmdlets and parameters that are not used in these common use cases.

To use a proxy server for uploads, see Configure a proxy server.

- **Enable scheduled uploads:** Diagnostic collections are automatically uploaded to Citrix. If you do not enter additional cmdlets for a custom schedule, the default schedule is used.

  ```
  $cred = Get-Credential
  Enable-CitrixCallHome -Credential $cred
  ```

  To confirm that scheduled uploads are enabled, enter `Get-CitrixCallHome`. If enabled, the return is `IsEnabled=True` and `IsMasterImage=False`.

- **Enable scheduled uploads for machines created from a master image:** Enabling scheduled uploads in a master image eliminates having to configure each machine that is created in the machine catalog.

  ```
  Enable-CitrixCallHome -Credential $cred -MasterImage
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To confirm that scheduled uploads are enabled, enter **Get-CitrixCallHome**. If enabled, the return is `IsEnabled=True` and `IsMasterImage=True`.

- **Create a custom schedule:** Create a daily or weekly schedule for diagnostic collections and uploads.

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
    -UploadFrequency {
Daily|Weekly }
```

Examples:

The following cmdlet creates a schedule to bundle and upload data at 10:20 every evening. The Hours parameter uses a 24-hour clock. When the `UploadFrequency` parameter value is Daily, the `DayOfWeek` parameter is ignored, if specified.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

To confirm the schedule, enter `Get-CitrixCallHomeSchedule`. In the preceding example, it returns `StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency =Daily`.

The following cmdlet creates a schedule to bundle and upload data at 10:20 every Wednesday evening.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -
    UploadFrequency Weekly
```

To confirm the schedule, enter `Get-CitrixCallHomeSchedule`. In the preceding example, it returns `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly` .

Disable Call Home

You can disable Call Home using a PowerShell cmdlet or through Citrix Scout.

AOT logs are collected and saved to disk, even when Call Home scheduled uploads are disabled. (When scheduled uploads are disabled, AOT logs are not automatically uploaded to Citrix.) You can disable the collection and local storage of AOT logs.

Disable Call Home with PowerShell After running the following cmdlet, diagnostic data will not be uploaded to Citrix automatically. (You can still upload diagnostic data using Citrix Scout or telemetry PowerShell cmdlets.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Disable-CitrixCallHome
```

To confirm that Call Home is disabled, enter `Get-CitrixCallHome`. If disabled, the return is `IsEnabled=False` and `IsMasterImage=False`.

Disable a collection schedule using Citrix Scout To disable a diagnostic collection schedule using Citrix Scout, follow the guidance in Schedule collections. In step 3, click **Off** to cancel the schedule for the selected machines.

Disable collection of AOT logs After running the following cmdlet (with the `Enabled` field set to **`false`**), AOT logs will not be collected.

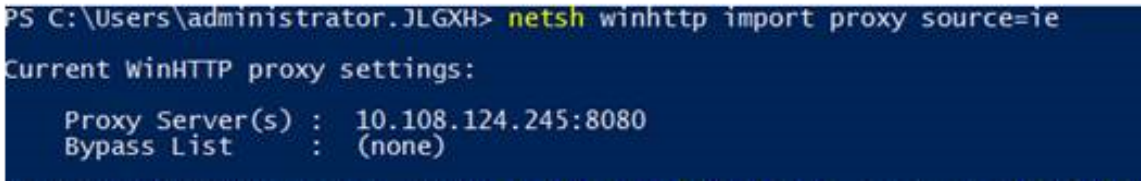
```
Enable-CitrixTrace -Listen'{ "trace":{ "enabled":false,"persistDirectory
":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds
":300 } } '
```

The `Listen` parameter contains arguments in JSON format.

Configure a proxy server for Call Home uploads

Complete the following tasks on the machine where Call Home is enabled. Example diagrams in the following procedure contain server address and port 10.158.139.37:3128. Your information will differ.

1. Add proxy server information in your browser. In Internet Explorer, select **Internet Options > Connections > LAN settings**. Select **Use a proxy server for your LAN**”and enter the proxy server address and port number.
2. In PowerShell, run `netsh winhttp import proxy source=ie`.

3. Using a text editor, edit the TelemetryService.exe config file, which is located in C:\Program Files\Citrix\Telemetry Service. Add the information shown in the red box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Restart the Telemetry Service.

Run the Call Home cmdlets in PowerShell.

Manually collect and upload diagnostic information

You can use the CIS website to upload a diagnostic information bundle to CIS. You can also use PowerShell cmdlets to collect and upload diagnostic information to CIS.

To upload a bundle using the CIS website:

1. Log on to Citrix Insight Services using your Citrix account credentials.
2. Select **My Workspace**.
3. Select **Healthcheck** and then navigate to the location of your data.

CIS supports several PowerShell cmdlets that manage data uploads. This documentation covers the cmdlets for two common cases:

- Use the `Start-CitrixCallHomeUpload` cmdlet to manually collect and upload a diagnostic information bundle to CIS. (The bundle is not saved locally.)
- Use the `Start-CitrixCallHomeUpload` cmdlet to manually collect data and store a diagnostic information bundle locally. This allows you to preview the data. Later, use the `Send-CitrixCallHomeBundle` cmdlet to manually upload a copy of that bundle to CIS. (The data you originally saved remains locally.)

The PowerShell help provides comprehensive syntax, including descriptions of cmdlets and parameters that are not used in these common use cases.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you enter a cmdlet to upload data to CIS, you are prompted to confirm the upload. If the cmdlet times out before the upload completes, check the status of the upload in the system event log. The upload request might be rejected if the service is already performing an upload.

Collect data and upload bundle to CIS:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
    string] [-Description string] [-IncidentTime string] [-SRNumber
    string] [-Name string] [-UploadHeader string] [-AppendHeaders string
    ] [-Collect string] [<CommonParameters>]
```

Collect data and save it locally:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
    Description string] [-IncidentTime string] [-SRNumber string] [-Name
     string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
    strings] [<CommonParameters>]
```

The following parameters are valid:

- **Credential:** Directs the upload to CIS.
- **InputPath:** Location of zip file to include in the bundle. This might be an additional file that Citrix Support requests. Be sure to include the .zip extension.
- **OutputPath:** Location where the diagnostic information is saved. This parameter is required when saving Call Home data locally.
- **Description and Incident Time:** Free form information about the upload.
- **SRNumber:** Citrix Technical Support incident number.
- **Name:** Name that identifies the bundle.
- **UploadHeader:** JSON-formatted string specifying the upload headers uploaded to CIS.
- **AppendHeaders:** JSON-formatted string specifying the appended headers uploaded to CIS.
- **Collect:** JSON-formatted string specifying which data to collect or omit, in the form {‘collector’ :{‘enabled’:Boolean}}, where Boolean is true or false.
  Valid collector values are:
  - ‘wmi’
  - ‘process’
  - ‘registry
  - ‘crashreport’
  - ‘trace’
  - ‘file’
  - ‘msi’
  - ‘localdata’

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ‘sitedata’
- ‘sfb’

By default, all collectors except ‘sfb’are enabled.

The ‘sfb’collector is designed to be used on demand to diagnose Skype for Business issues. In addition to the ‘enabled’parameter, the ‘sfb’collector supports the ‘account’and ‘accounts’ parameters to specify target users. Use one of the forms:

- “-Collect “{‘sfb’:{‘account’:’domain\\user1’}}”
- “-Collect “{‘sfb’:{‘accounts’:[‘domain\\user1’, ‘domain\\user2’]}}”

- **Common Parameters:** See the PowerShell help.

Upload data that was previously saved locally:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<
CommonParameters>]
```

The `Path` parameter specifies the location of the previously saved bundle.

Examples:

The following cmdlet requests an upload of Call Home data (excluding data from the WMI collector) to CIS. This data relates to registration failures of Citrix Provisioning VDAs, which were noted at 2:30 PM for Citrix Support case 123456. In addition to the Call Home data, the file “c:\Diagnostics\ExtraData.zip”is incorporated into the uploaded bundle.

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
    zip" -Description "Registration failures with Citrix Provisioning
    VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
    RegistrationFailure-021812016" -Collect "{
 'wmi':{
 'enabled':false }
  }
 " -UploadHeader "{
 'key1':'value1' }
 " -AppendHeaders "{
 'key2':'value2' }
 "
```

The following cmdlet saves Call Home data related to Citrix Support case 223344, noted at 8:15 AM. The data saved in the file mydata.zip on a network share. In addition to the Call Home data, the file “c:\Diagnostics\ExtraData.zip”will be incorporated into the saved bundle.

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\
    mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "
    Diagnostics for incident number 223344" -IncidentTime "8:15" -
    SRNumber 223344
```

The following cmdlet uploads the data bundle you saved earlier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle  –Credential $cred -Path \\mynetwork\
    myshare\mydata.zip
```

Citrix Scout

September 13, 2025

Introduction

Citrix Scout collects diagnostics and runs health checks. You can use the results to maintain your Citrix Virtual Apps and Desktops™ deployment. Citrix offers comprehensive, automated analysis of diagnostics collections through Citrix Insight Services. You can also use Scout to troubleshoot issues, on your own or with Citrix Support guidance.

You can upload collection files to Citrix for analysis and guidance from Citrix Support. Or, you can save a collection locally for your own review, and then later upload the collection file to Citrix for analysis.

Scout offers the following procedures:

- **Collect:** Runs a one-time diagnostics collection on machines that you select in a site. You can then either upload the file to Citrix or save it locally.
- **Trace & Reproduce:** Starts a manual trace on the machines that you select. Then you re-create issues on those machines. After re-creating the issue, the trace is stopped. Scout then collects other diagnostics and uploads the file to Citrix, or saves the file locally.
- **Schedule:** Schedules diagnostics collections to occur daily or weekly at a specified time on the machines you select. The file is automatically uploaded to Citrix.
- **Health Check:** Runs checks that gauge the health and availability of the site and its components. You can run health checks for Delivery Controllers, Virtual Delivery Agents (VDAs), StoreFront™ servers, and Citrix License Servers. If issues are found during the checks, Scout provides a detailed report. Each time Scout starts, it checks for updated health check scripts. If new versions are available, Scout downloads them automatically, for use the next time health checks are run.

> **Note:**
>
> The **Trace & Reproduce**, **Schedule**, and **Health Check** procedures are currently not available for Linux VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The graphical interface described in this article is the primary way to use Scout. Alternatively, you can use PowerShell to configure one-time or scheduled diagnostic collections and uploads. See Call Home.

Where to run Scout:

- In an on-premises deployment, run Scout from a Delivery Controller™ to capture diagnostics or run checks on one or more Virtual Delivery Agents (VDAs), Delivery Controllers, StoreFront servers, Federated Authentication Service (FAS) servers, and License Servers. You can also run Scout from a VDA to collect local diagnostics.

  > **Note:**
  >
  > Currently, the *Health Check* for diagnosing FAS configuration issues isn't supported by Scout on the FAS server.

- In a Citrix Cloud environment that uses Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), run Scout from a VDA to collect local diagnostics.

The log for the Scout application is stored in `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. This file can be used for troubleshooting.

What is collected

The diagnostics collected by Scout include Citrix Diagnostic Facility (CDF) trace log files. A subset of CDF traces called Always-on Tracing (AOT) is also included. AOT information can be helpful when troubleshooting common issues such as VDA registrations and application/desktop launches. No other Event Tracing for Windows (ETW) information is collected.

The collection includes:

- Registry entries created by Citrix Virtual Apps and Desktops under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Windows Management Instrumentation (WMI) information under the **Citrix namespace**.
- Processes that are running.
- Crash dumps of Citrix processes that are stored in %PROGRAMDATA%\Citrix\CDF.
- Citrix policy information, in CSV format.
- Installation and upgrade information. The collection can include the full product metainstaller log, failing MSI logs, output from the MSI log analyzer, StoreFront logs, Licensing compatibility check logs, and results from preliminary site upgrade tests.

About trace information:

- The trace information is compressed as it is collected, keeping a small footprint on the machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On each machine, the Citrix Telemetry Service keeps compressed recent trace information for a maximum of eight days.
- Beginning with Citrix Virtual Apps and Desktops 7 1808, AOT traces are saved to the local disk by default. (In earlier versions, traces were held in memory.) Default path = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- Beginning with Citrix Virtual Apps and Desktops 7 1811, AOT traces saved to network shares are collected with other diagnostics.
- You can modify the maximum size (default = 10 MB) and slice duration, using the `Enable-CitrixTrace` cmdlet or the `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` registry string.
- Traces append to the file until the file reaches 10% of `MaxSize`.

For a list of the datapoints that Scout collects, see Call Home key datapoints.

Scout configuration

Scout can be configured to work on Linux VDAs. For more information on Linux VDA and telemetry, see Integrate with the Citrix Telemetry Service

The Linux VDA might automatically change the `ctxtelemetry` socket port or the port for telemetry service. If so, you must configure the port manually.

1. Navigate to C:\Program Files\Citrix\Telemetry Service
2. Open the ScoutUI.exe.config file.
3. Change the value for LinuxVDATelemetryServicePort or LinuxVDATelemetryWakeupPort to what was configured on the Linux VDA:

- `<add key="LinuxVDATelemetryServicePort"value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort"value="7503"/>`

1. Save the changes and close the file.
2. Open Scout again to ensure it loads the latest configuration.

About health checks

Health check data is stored in folders under `C:\ProgramData\Citrix\TelemetryService\`.

Site health checks

Site health checks are included in the Environment Test Service, which provides a comprehensive evaluation of the FlexCast Management Architecture (FMA) services. In addition to checking for ser-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

vice availability, these checks look for other health indicators such as database connections.

Site health checks run on Delivery Controllers. Depending on your site's size, these checks can take up to an hour to complete.

Delivery Controller configuration checks As part of the site health checks. Delivery Controller configuration checks verify whether the following issues exist, based on Citrix recommendations for Virtual Apps and Desktops sites:

- One or more Delivery Controllers are in a failed state.
- There is only one Delivery Controller in the site.
- Delivery Controllers are of different versions.

In addition to meeting the permissions and requirements for health checks, Delivery Controller configuration checks require:

- At least one Controller powered on.
- The Broker Service running on a Controller.
- A working connection from the Controller to the site database.

VDA health checks

VDA health checks identify possible causes for common VDA registration, session launch, and time zone redirection issues.

For registration on the VDA, Scout 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, Scout checks:

- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Session launch registry settings

For time zone redirection on VDAs, Scout checks:

- Windows hotfix installation
- Citrix hotfix installation
- Microsoft group policy settings
- Citrix group policy settings

For Profile Management on VDAs, Scout 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:

- Citrix Default Domain service is running
- Citrix Credential Wallet service is running
- Connection from the StoreFront server to Active Directory port 88
- Connection from the StoreFront server to Active Directory port 389
- Base URL has a valid FQDN
- Correct IP address from the base URL can be retrieved
- IIS application pool is using .NET 4.0
- Whether the certificate is bound to the SSL port for the host URL
- Whether the certificate chain is complete
- Whether the certificates have expired
- Whether a certificate is expiring soon (within 30 days)

License Server checks

License Server checks verify:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- License Server connection from the Delivery Controller
- License Server firewall remote access status
- Citrix Licensing service status
- License Server License caching mode state
- License Server ports connection
- Whether the Citrix vendor daemon (CITRIX) is running
- Whether system clocks are synchronized
- Whether the Citrix Licensing service is running under the Local Service account
- Presence of the `CITRIX.opt` file
- Customer Success Services eligibility date
- Citrix License Server Update
- Whether the License Server certificate is in the Delivery Controller's trusted root store

In addition to meeting the permissions and requirements for health checks, the License Server must be joined to a domain. Otherwise, the License Server is not discovered.

Run health checks

The Health Check procedure comprises selecting machines, starting the checking, and then reviewing the results report.

1. Launch Scout. From the machine's **Start** menu, select **Citrix > Citrix Scout**. On the opening page, click **Health Check**.
2. Select machines. Click **Find machine** to discover machines. The **Select machines** page lists all the VDAs, Delivery Controllers, and License Servers discovered in the site. You can filter the display by machine name. Select the checkbox next to each machine that you want to collect diagnostics from, and then click **Continue**.

   To add other component types (such as StoreFront servers and VDA machines), see Add machines manually and Import VDA machines. You cannot manually add Citrix Provisioning™ Servers or License Servers.

   Scout automatically launches verification tests on each selected machine, making sure it meets the criteria listed in Verification tests. If verification fails, a message is posted in the **Status** column, and that machine's checkbox is cleared. You can either:

   - Resolve the issue and then select the machine's checkbox again. This triggers a retry of the verification tests.
   - Skip that machine (leave its checkbox unselected). Health checks are not run for that machine.

   When the verification tests complete, click **Continue**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 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). Click **Start Checking**.

   During and after checking:

   - The **Status** column indicates the current checking state for a machine.
   - 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, only all selected machines. Information from machines that have completed the checks is kept.
   - When the checks complete for all selected machines, the **Stop Checking** button in the lower right corner changes to **Done**.
   - 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 show the results.
   - After the check completes for all selected machines, don't click **Back**. (If you do, the check results are lost.)

4. When the checks complete, click **Done** to return to the Scout opening page.

Health check results

For report-generating Citrix checks, the reports contain:

- Time and date when the results report was generated
- Machines that were checked
- Conditions that the check looked for on the targeted machines

Permissions and requirements

Permissions:

- To collect diagnostics:
  - You must be a local administrator and domain user for each machine from which you're collecting diagnostics.
  - You must have permission to write to the LocalAppData directory on each machine.
- To run health checks:
  - You must be a member of the domain users group.
  - You must be either a full administrator or have a custom role with read-only and **Run Environment Tests** permissions for the site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Set the script execution policy to at least `RemoteSigned` to allow the scripts to run. For example: `Set-ExecutionPolicy RemoteSigned`. **Note:** other script execution privileges can work as well.

- Use **Run as administrator** when launching Scout.

For each machine from which you collect diagnostics or run health checks:

- Scout 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.
- The Citrix Telemetry Service must be running on the machine.
- Windows Management Infrastructure (WMI) access must be enabled on the machine.
- To set a schedule for diagnostic collection, the machine must be running a compatible Scout version.

Do not use the dollar sign ($) in user names specified in pathnames. It prevents the collection of diagnostic information.

Scout runs verification tests on the machines that you select, to make sure these requirements are met.

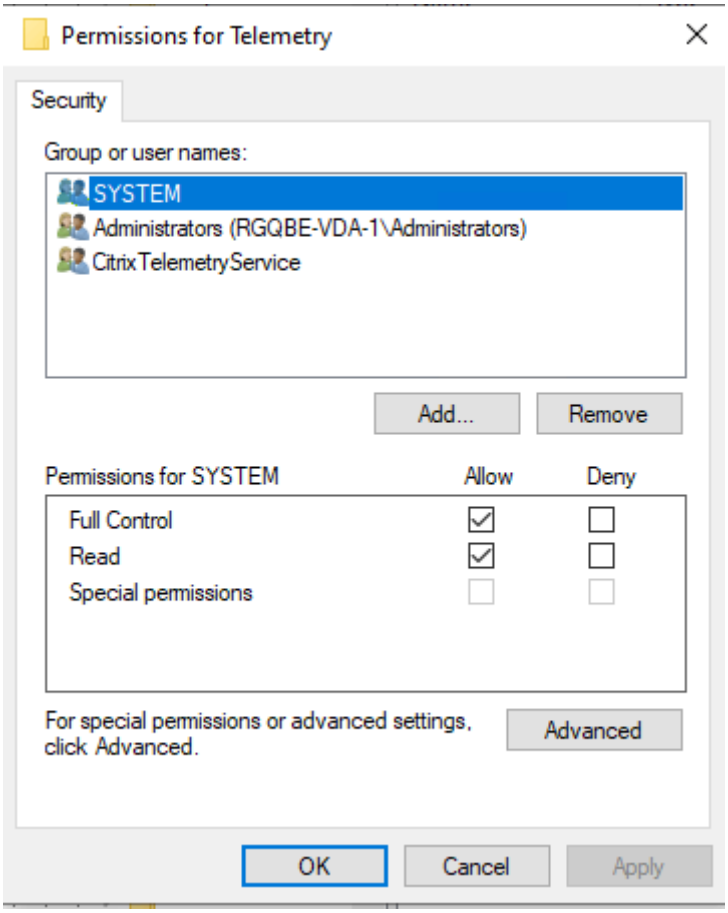
The Telemetry Service for Windows runs on Network Service.

Citrix Remote Broker Provider	Enables co...	Running	Automatic	Network Service
Citrix Storefront Privileged ...	Manages pr...	Running	Automatic	NT AUTHORITY\SYSTEM
Citrix Storefront Service	Manages de...	Running	Automatic	Network Service
Citrix Telemetry Service	Citrix Telem...	Running	Automatic (D...	Network Service
Citrix Trust Service	Citrix Trust ...	Running	Automatic	Network Service
Citrix Web Services for Lice...	A service th...	Running	Automatic	Local Service
Citrix XenServer Installation ...	Installs and ...		Manual	Local System
Citrix XenServer Windows ...	Monitors an...	Running	Automatic	Local System

The AOT Trace Folder is saved in `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`.

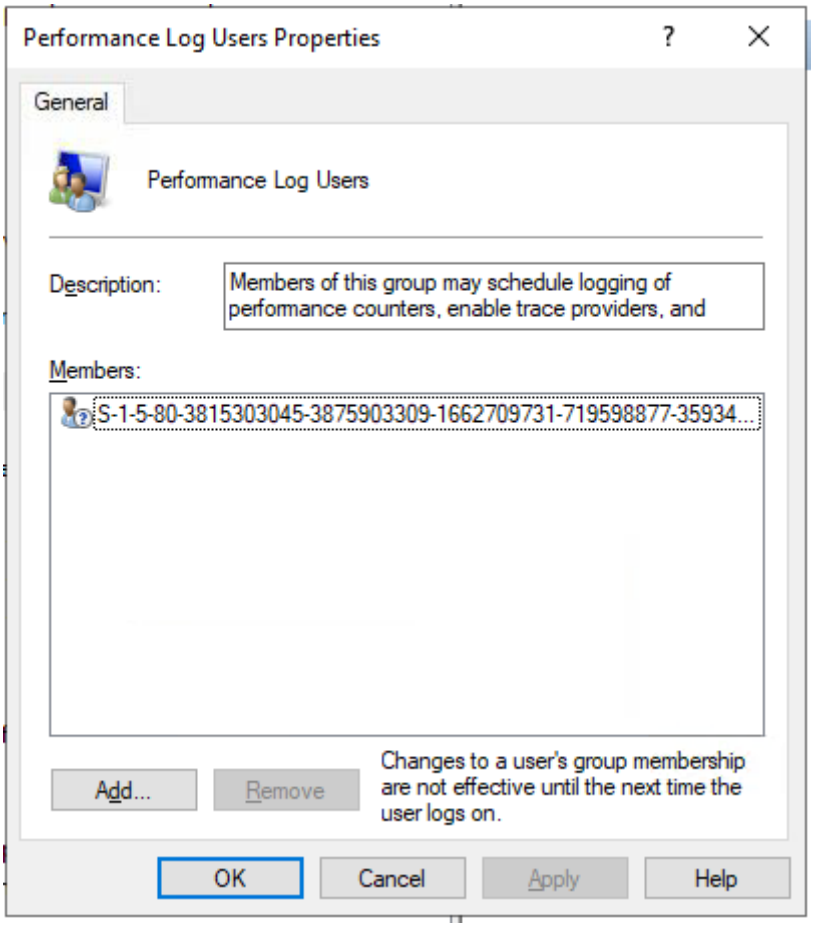
Only users in the Administrator group, System, and Telemetry Service SID have permission to access the `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry` registry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The Telemetry Service SID remains in the Performance Log Users group after uninstalling the Telemetry Service, but you can remove it manually.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Verification tests

Before a diagnostic collection or health check starts, verification tests run automatically for each selected machine. These tests make sure that the requirements are met. If a test fails for a machine, Scout displays a message with suggested corrective actions.

- **Scout 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.
- **Enable PSRemoting and WinRM** - You can enable PowerShell remoting and WinRM at the same time. Using **Run as administrator**, run the `Enable-PSRemoting` cmdlet. For details, see the Microsoft help for the cmdlet.
- **Scout requires PowerShell 3.0 (minimum)** - Install PowerShell 3.0 (or later) on the machine, and then enable PowerShell remoting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Unable to access LocalAppData directory on this machine** - Ensure that the account has permission to write to the LocalAppData directory on the machine.
- **Cannot locate Citrix Telemetry Service** - Ensure that the Citrix Telemetry Service is installed and started on the machine.
- **Cannot get schedule** - Upgrade the machine to (minimum) XenApp and XenDesktop 7.14.
- **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.
- **Newer version of Citrix Telemetry Service required** - (Version is checked only for Collect and Trace & Reproduce.) Upgrade the Telemetry Service version on the machine (see Install and upgrade). If you do not upgrade the service, that machine is not included in the **Collect** or **Trace & Reproduce** actions.
- **Scout cannot connect to the systemd socket on this machine** - Ensure that:
  - Port 7503 is open. Verify that the `systemd ctxtelemetry.socket` is listening on port 7503 on the machine. The port might be different if the `ctxtelemetry.socket` port has been changed. See Scout configuration to adjust ports.
  - The network connection is working properly. (This might include verifying that your firewall is properly configured.)
- **The Linux VDA Telemetry Service is not started on this machine** - Ensure that:
  - Port 7502 is open. Verify that the Linux VDA Telemetry Service is installed and started on the machine. The port might be different if the telemetry service port has been changed. See Scout configuration to adjust ports.
  - The network connection is working properly. (This might include verifying that your firewall is properly configured.)

Version compatibility

This version of Scout (3.x) is intended to be run on Citrix Virtual Apps and Desktops (or minimum XenApp and XenDesktop 7.14) Controllers and VDAs.

Feature	Scout 2.23	Scout 3.0
Support Citrix Virtual Apps and Desktops (plus XenApp and XenDesktop 7.14 through 7.18)	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Scout 2.23	Scout 3.0
Support XenDesktop 5.x, 7.1–7.13	Yes	No
Support XenApp 6.x, 7.5 to 7.13	Yes	No
Delivered with product	7.1–7.13	Beginning with 7.14
Can be downloaded from CTX article	Yes	No
Capture CDF traces	Yes	Yes
Capture Always-on-Traces (AOT)	No	Yes
Allow collection of diagnostic data	Up to 10 machines at once (by default)	Unlimited (subject to resource availability)
Allow diagnostic data to be sent to Citrix	Yes	Yes
Allow diagnostic data to be saved locally	Yes	Yes
Support Citrix Cloud™ credentials	No	Yes
Support Citrix credentials	Yes	Yes
Support proxy server for uploads	Yes	Yes
Adjust schedules	N/A	Yes
Script support	Command line (local Controller only)	PowerShell using Call Home cmdlets (any machine with the Telemetry Service installed)
Health checks	No	Yes
Data Masking	No	Beginning with 3.17

Install and upgrade

By default, Scout is installed or upgraded automatically as part of the Citrix Telemetry Service when you install or upgrade a VDA or a Controller.

If you omit the Citrix Telemetry Service when you install a VDA, or remove the service later, run `TelemetryServiceInstaller_xx.msi` from the `x64\Virtual Desktop Components` or `x86\Virtual Desktop Components` folder on the Citrix Virtual Apps and Desktops installation media.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you select the **Collect** or **Trace & Reproduce** action, you're notified if a machine is running an older version of the Citrix Telemetry Service. Citrix recommends using the latest supported version. If you don't upgrade the Telemetry Service on that machine, it is not included in the **Collect** or **Trace & Reproduce** actions. To upgrade the Telemetry Service, use the same procedure as installing it.

Upload authorization

If you plan to upload diagnostic collections to Citrix, you must have a Citrix or Citrix Cloud account. (These are the credentials that you use to access Citrix downloads or access the Citrix Cloud Control Center.) After your account credentials are validated, a token is issued.

If you authenticate with a Citrix account or a Citrix Cloud account, click a link to access Citrix Cloud using HTTPS with your default browser. After you enter your Citrix Cloud credentials, the token is displayed. Copy the token and then paste it into Scout. You can then continue in the Scout wizard.

The token is stored locally on the machine where you're running Scout. To enable use of that token the next time you run **Collect** or **Trace & Reproduce**, select the **Store token and skip this step in the future** checkbox.

You must reauthorize each time you select **Schedule** on the Scout opening page. You cannot use a stored token when creating or changing a schedule.

Use a proxy for uploads

If you want to use a proxy server to upload collections to Citrix, you can instruct Scout to use the proxy settings configured for your browser's Internet Properties. Alternatively, you can specify the proxy server's IP address and port number.

Find machine

For the **Collect**, **Trace & Reproduce**, and **Schedule** procedures, Scout lists the Controllers and VDAs it discovers automatically.

When you run Scout Health Check from the Delivery Controller, click **Find machine** to discover machines, including delivery controllers, VDAs, license servers, and StoreFront servers.

When you run Scout Health Check from a domain-joined machine which is not an Delivery Controller, Scout cannot discover machines automatically. You need to add machines manually or import VDA machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add machines manually

After Scout lists the Controllers and VDAs it discovers, you can manually add other machines in the deployment, such as StoreFront servers, License Servers, and Citrix Provisioning servers.

When running health checks:

- Citrix License Servers in the domain are discovered automatically. You cannot add License Servers manually.
- Health checks do not currently support Citrix Provisioning servers.

On any Scout page that lists the discovered machines, click **+ Add machine**. Type the FQDN of the machine that you want to add, and then click **Continue**. Repeat to add other machines, as needed. (Although entering a DNS alias instead of an FQDN can appear valid, the health checks might fail.)

Manually added machines always appear at the top of the machines list, above the discovered machines.

An easy way to identify a manually added machine is the red delete button on the right end of the row. Only manually added machines have that button. Discovered machines don't.

To remove a manually added machine, click the red button on the right end of the row. Confirm the deletion. Repeat to delete other manually added machines.

Scout remembers manually added machines until you remove them. When you close and then reopen Scout, the manually added machines are still listed at the top of the list.

CDF traces are not collected when using **Trace & Reproduce** on StoreFront servers. However, all other trace information is collected.

> **Tips:**
>
> Scout supports showing the **+ Add machine** button on the **Collect** page when it is running on the StoreFront type machine starting from Citrix Virtual Apps and Desktops LTSR 2507 version. This option enable users to manually add multiple StoreFront Server machines in the same cluster and trigger collection at the same time. The older versions of *TelemetryService* do not support this feature.

Import VDA machines

You can import VDA machines in the deployment when running health checks.

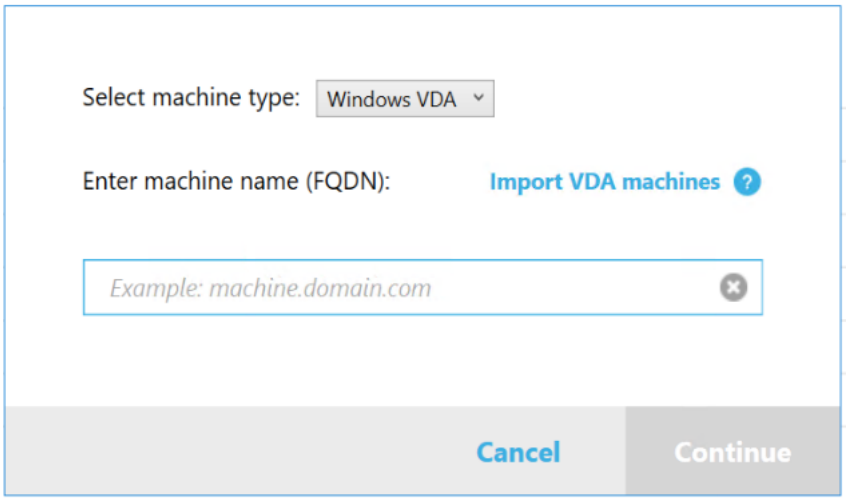
1. On Delivery Controller or Connector, generate the machine list file with the PowerShell command. On Connector, you must input Citrix credentials and select the customer in the pop-up dialog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList
.txt
```

2. Copy the machineList.txt file to the domain-joined machine that you want to launch Scout Health Check.
3. On the Scout Health Check page, click **Add Machine**.
4. Select the **Windows VDA** machine type.
5. Click **Import VDA machines**.
6. Select the machineList.txt file.
7. Click **Open**.

The imported VDA machines are listed on the Scout Health Check page.



Collect diagnostics

The **Collect** procedure comprises selecting machines, starting the diagnostics collection, and then uploading the file containing the collection to Citrix or saving it locally.

1. Launch Scout. From the machine's **Start** menu, select **Citrix > Citrix Scout**. On the opening page, click **Collect**.
2. Select machines.
    - On a Controller, the **Select machines** page lists all the VDAs and Controllers in the site. You can filter the display by machine name. To add other machines manually (such as StoreFront or Citrix Provisioning servers), see Add machines manually.
    - On a StoreFront, the **Select machines** page lists only the local machine. To add other StoreFront machines in the same cluster, see Add machines manually.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On other components (such as VDA servers), the **Select machines** page lists only the local machine. Manually adding machines is not supported.

Select the checkbox next to each machine you want to collect diagnostics from, and then click **Continue**.

Scout automatically launches verification tests on each selected machine, ensuring it meets the criteria listed in Verification tests. If verification fails, a message is posted in the **Status** column, and that machine's checkbox is unselected. You can either:

- Resolve the issue and then select the machine's checkbox again. This triggers a retry of the verification tests.
- Skip that machine (leave its checkbox unselected). Diagnostics won't be collected from that machine.

When the verification tests complete, click **Continue**.

3. Collect diagnostics. The summary lists all the machines from which diagnostics are collected (the machines you selected that passed the verification tests). Click **Start Collecting**.

   During collection:

   - The **Status** column indicates the current collection state for a machine.
   - To stop an in-progress collection on a single machine, click **Cancel** in the **Action** column for that machine.
   - To stop all in-progress collections, click **Stop Collection** in the lower right corner of the page. Diagnostics from machines that have completed collection are kept. To resume the collection, click **Retry** in the **Action** column for each machine.
   - When the collection completes for all selected machines, the **Stop Collection** button in the lower right corner changes to **Continue**.
   - To collect diagnostics again, click **Collect Again** in that machine's **Action** column. The newer collection overwrites the earlier.
   - If a collection fails, you can click **Retry** in the **Action** column. Only successful collections are uploaded or saved.
   - After the collection completes for all selected machines, don't click **Back**. (If you click it, the collection is lost.)

   When the collection completes, click **Continue**.

4. Save or upload the collection. Choose whether to upload the file to Citrix, or save it on the local machine.

   If you choose to upload the file now, continue with Step 5.

   If you choose to save the file locally:

   - A Windows **Save** dialog box appears. Navigate to the desired location.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When the local save completes, the pathname of the file is displayed and linked. You can view the file. You can upload the file later to Citrix. See CTX136396.

Click **Done** to return to the Scout opening page. You don't need to complete any further steps in this procedure.

5. Authenticate for uploads and optionally specify a proxy. For details, see Upload authorization.

   - If you haven't authenticated through Scout, continue with this step.
   - If you have authenticated through Scout, the stored authorization token is used by default. If this is what you want to do, select this option and click **Continue**. You aren't prompted for credentials for this collection. Continue with Step 6.
   - If you authenticated previously, but want to reauthorize and get a new token, click **Change/Reauthorize** and continue with this step.

   Choose whether you want to use Citrix credentials or Citrix Cloud credentials to authenticate the upload. Click **Continue**. The credentials page appears only if you're not using a stored token.

   On the credentials page:

   - If you want to use a proxy server for the file upload, click **Configure proxy**. You can instruct Scout to use the proxy settings configured for your browser's internet properties. Or, you can enter the proxy server's IP address and port number. Close the proxy dialog box.
   - For a Citrix Cloud account, click **Generate token**. Your default browser launches to a Citrix Cloud page where a token is displayed. Copy the token, and then paste it on the Scout page.
   - For a Citrix account, enter your credentials.

   When you're done, click **Continue**.

6. Enter information about the upload.

   - The name field contains the default name for the file for the collected diagnostics. This suffices for most collections, although you can change the name. (If you delete the default name and leave the name field empty, the default name is used.)
   - Optionally, specify an 8-digit Citrix Support case number.
   - In the optional **Description** field, describe the issue and indicate when the issue occurred, if applicable.

   When you're done, click **Start Upload**.

   During the upload, the lower left portion of the page approximates the percentage of the upload that has completed. To cancel an in-progress upload, click **Stop Upload**.

   When the upload completes, the URL of its location is displayed and linked. You can follow the link to the Citrix location to view the analysis of the upload, or you can copy the link.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click **Done** to return to the Scout opening page.

Trace and reproduce

The **Trace and Reproduce** procedure comprises selecting machines, starting a trace, reproducing issues, completing the diagnostics collection, and then uploading the file to Citrix, or saving it locally.

This procedure is similar to the standard **Collect** procedure. However, it allows you to start a trace on machines and then re-create issues on those machines. All diagnostics collections include AOT trace information. This procedure adds CDF traces to help troubleshooting.

1. Launch Scout. From the machine's **Start** menu, select **Citrix > Citrix Scout**. On the opening page, click **Trace & Reproduce**.
2. Select machines. The **Select machines** page lists all the VDAs and Controllers in the site. You can filter the display by machine name. Select the checkbox next to each machine you want to collect traces and diagnostics from. Then click **Continue**.

   To add other machines manually (such as StoreFront or Citrix Provisioning servers), see Add machines manually.

   Scout automatically launches verification tests on each selected machine, making sure it meets the criteria listed in Verification tests. If verification fails for a machine, a message is posted in the **Status** column, and that machine's checkbox is unselected. You can either:

   - Resolve the issue and then select the machine's checkbox again. This triggers a retry of the verification tests.
   - Skip that machine (leave its checkbox unselected). Diagnostics and traces are not collected from that machine.

   When the verification tests complete, click **Continue**.
3. Start the trace. The summary lists all the machines from which traces are collected. Click **Start Tracing**.

   On one or more of the selected machines, reproduce the issues you experienced. Trace collection continues while you're doing that. When you're done reproducing the issue, click **Continue** in Scout. That stops the trace.

   After you stop the trace, indicate whether you reproduced the issue during the trace.
4. Collect diagnostics from machines. Click **Start Collecting**. During collection:

   - The **Status** column indicates the current collection state for a machine.
   - To stop an in-progress collection on a single machine, click **Cancel** in the **Action** column for that machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To stop all in-progress collections, click **Stop Collection** in the lower right corner of the page. Diagnostics from machines that have completed collection are kept. To resume the collection, click **Retry** in the **Action** column for each machine.
- When the collection completes for all selected machines, the **Stop Collection** button in the lower right corner changes to **Continue**.
- To collect diagnostics again from a machine, click **Collect Again** in that machine's **Action** column. The newer collection overwrites the earlier.
- If a collection fails, you can click **Retry** in the **Action** column. Only successful collections are uploaded or saved.
- After the collection completes for all selected machines, don't click **Back**. (If you do, the collection is lost.)

When the collection completes, click **Continue**.

5. Save or upload the collection. Choose whether to upload the file to Citrix or save it locally.

   If you choose to upload the file now, continue with Step 6.

   If you choose to save the file locally:

   - A Windows Save dialog box appears. Select the desired location.
   - When the local save completes, the pathname of the file is displayed and linked. You can view the file. Remember: You can upload the file later from Citrix; see CTX136396 for Citrix Insight Services.

   Click **Done** to return to the Scout opening page. You don't need to complete any further steps in this procedure.

6. Authenticate for uploads and optionally specify a proxy. Review Upload authorization for details of this process.

   - If you haven't authenticated through Scout, continue with this step.
   - If you authenticated through Scout, the stored authorization token is used by default. If this what you want to do, choose this option and click **Continue**. You aren't prompted for credentials for this collection. Continue with Step 7.
   - If you previously authenticated, but want to reauthorize and get a new token, click **Change/Reauthorize** and continue with this step.

   Choose whether you want to use Citrix credentials or Citrix Cloud credentials to authenticate the upload. Click **Continue**. The credentials page appears only if you're not using a stored token.

   On the credentials page:

   - If you want to use a proxy server for the file upload, click **Configure proxy**. You can instruct Scout to use the proxy settings configured for your browser's Internet Properties. Or, you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

can enter the proxy server's IP address and port number. Close the proxy dialog box.
- For a Citrix Cloud account, click **Generate token**. Your default browser launch to a Citrix Cloud page where a token is displayed. Copy the token, and then paste it on the Scout page.
- For a Citrix account, enter your credentials.

When you're done, click **Continue**.

7. Provide information about the upload.

   Enter upload details:

   - The name field contains the default name for the file for the collected diagnostics. This suffices for most collections, although you can change the name. (If you delete the default name and leave the name field empty, the default name is used.)
   - Optionally, specify an 8-digit Citrix Support case number.
   - In the optional Description field, describe the issue and indicate when the issue occurred, if applicable.

   When you're done, click **Start Upload**.

   During the upload, the lower left portion of the page approximates what percentage of the upload has completed. To cancel an in-progress upload, click **Stop Upload**.

   When the upload completes, the URL of its location is displayed and linked. You can follow the link to the Citrix location to view the analysis of the upload, or you can copy the link.

   Click **Done** to return to the Scout opening page.

Scout supports TraceLogging provider

Previously, Scout supported only the Windows performance provider, which required extra decoding files and traced only sessions and events from a single session for the same provider.

Starting with the Citrix Virtual Apps and Desktops version 2411, Scout supports the TraceLogging provider. This provider does not require extra decoding files and can enable and receive events from up to eight trace sessions for the same provider. This feature is enabled by default.

Enable additional log collection

The **Enable additional log collection** function lets you use the trace and reproduce function with more tools, like perfmon, Netsh, DebugView, and Wireshark.

Starting with the 2407 release, when you enable additional log collection, Scout automatically detects the CDC-related tools installed on your machine and auto collects the CDC tool-related trace logs in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the zip package. You can customize these zip files and attach them to Scout. With this automation, you can use Citrix Scout more effectively and this helps you to diagnose the issues quickly.

> **Note:**
>
> This only applies to local machines.

To enable additional log collection, ensure the following required tools are installed and their directories are created manually at the specified location.

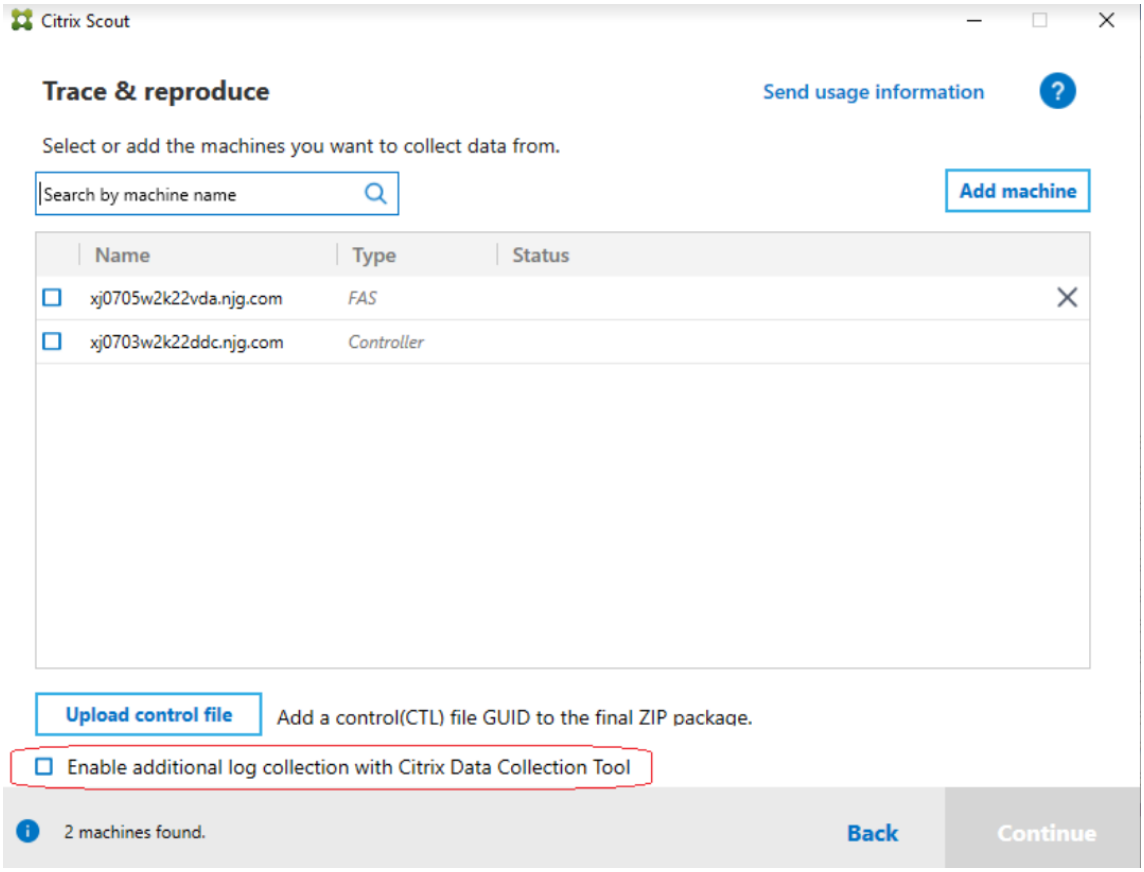
Tool installation locations:

- **Procdump** logs: Download **Procdump** and place it at %ProgramData%\Citrix\TelemetryService\CDC\Lib\Re
- **StoreFront** logs: Download **DbgView** and place it at %ProgramData%\Citrix\TelemetryService\CDC\Lib\Res
- **Procmon** logs: Download **Process Monitor** and place it at %ProgramData%\Citrix\TelemetryService\CDC\Li
- **Wireshark** logs: Install **Wireshark** manually on your system.

To collect additional logs:

1. On the Scout home page, click **Trace & Reproduce**.
2. On the **Select or add machines** page to collect data from the page, check the box for local machine. The status must show as *Verified*.
3. Select the **Enable additional log collection with Citrix Data Collection Tool** checkbox to enable additional log collection.
4. Click the **Upload control file** button to load one CTL file. This button allows you to add additional GUIDs in the AOT collection list for AOT collection with Scout.
5. Click **Continue** and follow the Trace and Reproduce instructions.
6. After completion, check the logs in the zip file. The logs are zipped in the folder *CDCLogs*.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> If the Procmon Tool is selected for tracing, Process Monitor logs can grow large quickly. Ensure you select only what tools are needed. You can also monitor the size of the logs under *%temp%\Scout-CDC-Log*.

Schedule collections

> **Note:**
>
> You can currently schedule collections, but not health checks.

The Schedule procedure comprises selecting machines and then setting or canceling the schedule. Scheduled collections are automatically uploaded to Citrix. (You can save scheduled collections locally using the PowerShell interface. See Citrix Call Home.)

1. Launch Scout. From the machine's Start menu, select **Citrix > Citrix Scout**. On the opening page, click **Schedule**.
2. Select machines. All the VDAs and Controllers in the site are listed. You can filter the display by machine name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you installed VDAs and Controllers using the graphical interface, if you set a Call Home schedule (see Citrix Call Home), Scout displays those settings, by default. You can use this version of Scout to start scheduled collections for the first time, or change a previously configured schedule.

Although you enabled/disabled Call Home on a per-machine basis during component installation, a schedule configured in Scout affects all the machines you select.

Select the checkbox next to each machine that you want to collect diagnostics from, and then click **Continue**.

To add other machines manually (such as StoreFront or Citrix Provisioning servers), see Add machines manually.

Scout automatically launches verification tests on each of the selected machines, making sure it meets the criteria in Verification tests. If verification fails for a machine, a message is posted in the **Status** column, and that machine's checkbox is unselected. You can either:

- Resolve the issue and then select the machine's checkbox again. This triggers a retry of the verification tests.
- Skip that machine (leave its checkbox unselected). Diagnostics (or traces) are not collected from that machine.

When the verification tests complete, click **Continue**.

The summary page lists the machines to which schedules are applied. Click **Continue**.

3. Set the schedule. Indicate when you want diagnostics to be collected. Remember: The schedule affects all selected machines.

   - To configure a weekly schedule for the selected machines, click **Weekly**. Choose the day of the week. Enter the time of day (24-hour clock) for the collection to begin.
   - To configure a daily schedule for the selected machines, click **Daily**. Enter the time of day (24-hour clock) for the collection to begin.
   - To cancel an existing schedule for the selected machines (and not replace it with another), click **Off**. This cancels any schedule that was previously configured for those machines.

   Click **Continue**.

4. Authenticate for uploads and optionally specify a proxy. Review Upload authorization for details of this process. Remember: You cannot use a stored token to authenticate when working with a Scout schedule.

   Choose whether you want to use Citrix credentials or Citrix Cloud credentials to authenticate the upload. Click **Continue**.

   On the credentials page:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you want to use a proxy server for the file upload, click **Configure proxy**. You can instruct Scout to use the proxy settings configured for your browser's Internet Properties. Or, you can enter the proxy server's IP address and port number. Close the proxy dialog box.
- For a Citrix Cloud account, click **Generate token**. Your default browser launches to a Citrix Cloud page where a token is displayed. Copy the token, and then paste it on the Scout page.
- For a Citrix account, enter your credentials.

When you're done, click **Continue**.

Review the configured schedule. Click **Done** to return to the Scout opening page.

During a collection, each selected machine's Windows application log contains entries about the collection and upload.

Data masking

The diagnostic information collected using Citrix Scout might contain security-sensitive information. The Citrix Scout data masking feature allows you to mask sensitive data in diagnostics files before uploading them to Citrix.

Scout data masking is configured to mask the IP address, machine names, domain names, user names, hypervisor names, Delivery Group names, catalog names, application names, and SIDs.

> **Note:**
>
> CDF traces are encrypted and cannot be masked.
>
> Linux VDA logs are compressed to `.tar.gz2` format and cannot be masked.

Collect new diagnostics and perform data masking

To use the Citrix Scout data masking feature, launch Scout from the command line.

1. In Windows, open the command prompt as an administrator.
2. Go to the directory where Scout is installed: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Launch Scout: `ScoutUI.exe datamasking`.
4. Click **Collect** or **Trace & Reproduce** to collect diagnostics.
5. After the collection completes, select **Enable data masking**. This option is enabled by default.
6. Configure the data mask. You can use the default rules or customize the rules.
7. Select whether to upload or save the diagnostics collection.
    - If you select **Upload the diagnostics collection to Citrix**, masked diagnostics files are uploaded to Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you select **Save the diagnostics collection on your local machine**, both the original and masked diagnostics are saved to the specified location.

Perform data masking on existing diagnostics

1. In Windows, open the command prompt as an administrator.
2. Go to the directory where Scout is installed: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Launch Scout directly in data masking mode: `ScoutUI.exe datamasking filePath`.
4. Select "Enable data masking"to continue. This option is enabled by default.
5. Configure the data mask. You can run data masking with the default rules or customize the rules.
6. Select whether to upload or save the diagnostics collection.
    - If you select **Upload the diagnostics collection to Citrix**, masked diagnostics files are uploaded to Citrix.
    - If you select **Save the diagnostics collection on your local machine**, both the original and masked diagnostics are saved to the specified location.

Masked data file and mapping file locations

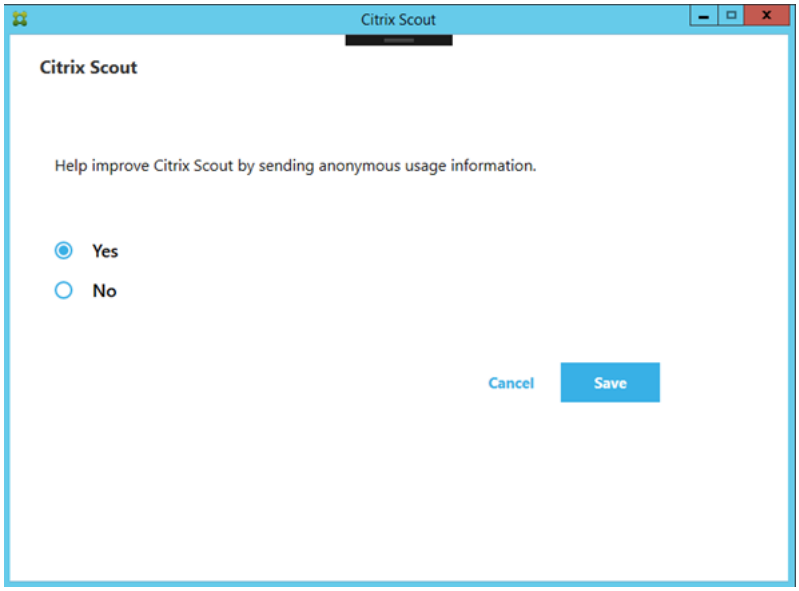
After you have uploaded or saved the diagnostics collection, click the link to open the original and masked diagnostics, and open the mapping information file.

Usage data collection

When you use Scout, 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 Scout 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.



Command-line interfaces for Scout functionalities

You can now use command-line interfaces for Scout functionalities, enabling you to collect needed logs and data without opening the Scout UI. This feature provides convenience for advanced users to automate the log or trace process locally or remotely for target machines or sites. This feature is enabled by default.

Commands are added for the following functionalities:

- Help
- Collect diagnostics
- Start trace
- Stop trace
- List ongoing trace sessions
- Start and stop CDC

> **Note:**
>
> When running the remote trace session, the new telemetry version must be installed on both VDA and DDC. This installation is required because the Scout Command-line is supported starting from Citrix Virtual Apps and Desktops version 2411, and older versions of `TelemetryService` do not support this feature.

The following table describes the newly added commands:

Help

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Command-line interface	Description	Example
`ScoutCLI.exe -h`	Displays context-sensitive help.	`ScoutCLI.exe -h` `ScoutCLI.exe -help`

Command for collect diagnostics

Command-line interface	Description	Example
`ScoutCLI.exe Collect -exclude <collector>`	Excludes the diagnostics from the specified collectors (Windows Management Instrumentation (WMI) process, registry, crash report, header, trace, `msi`, `vcu`, tool telemetry, and local data).	`ScoutCLI.exe collect -exclude wmi, localdata -output "C:/Logs/mydata.zip"`
`ScoutCLI.exe Collect -output <filename>`	Specifies where to save the output log file with `.zip` as the suffix.	
`ScoutCLI.exe Collect -fqdn <hostname>`	Collects diagnostics on specified machines in a site.	`ScoutCLI.exe collect -fqdn hostname -exclude wmi, localdata -output "C:/Logs/mydata.zip"`

Start trace

Command-line interface	Description	Example
`ScoutCLI.exe StartTrace -guids <filename (xxx.ctl)>`	Collects target modules'logs for the specified GUIDs.	Example for local machine trace start - `ScoutCLI.exe StartTrace -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50;` Example for remote machine trace start - `ScoutCLI.exe StartTrace -fqdn hostname -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`
`ScoutCLI.exe StartTrace -output <filename>`	Specifies where to save the output log file with .etl as the suffix.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Command-line interface	Description	Example
`ScoutCLI.exe StartTrace -name <session name>`	Defines the name of the tracing session.	
`ScoutCLI.exe StartTrace -level <value>`	Selects the log level to log target diagnostic details. The default value is 16.	
`ScoutCLI.exe StartTrace -max <value>`	Specifies the maximum log file size in MB. The default value is 50.	
`ScoutCLI.exe StartTrace -fqdn <hostname>`	Starts tracing on specified machines in a site.	

Stop trace

Command-line interface	Description	Example
`ScoutCLI.exe StopTrace -name <session name>`	Stop the specified tracing session.	`ScoutCLI.exe StopTrace -name session1`
`ScoutCLI.exe StopTrace -fqdn <hostname>`	Stops tracing on specified machines in a site. -o option is needed to assign the local path where the remote `.etl` is copied to.	`ScoutCLI.exe StopTrace -fqdn hostname -name session1 -output C:\Logs\xxx.etl`
`ScoutCLI.exe StopTrace -output <filename>`	Specifies where to save the output log file with .etl as the suffix.	

List ongoing trace sessions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Command-line interface	Description	Example
`ScoutCLI.exe ListSession -name <session name>`	Shows details for the specified tracing session. If no name is specified, shows details for all running tracing sessions.	`ScoutCLI.exe ListSession -name session1`
`ScoutCLI.exe ListSession -fqdn <hostname>`	Shows tracing details on specified machines in a site.	`ScoutCLI.exe ListSession -fqdn hostname -name session1`

Start and stop CDC

Command-line interface	Description	Example
`ScoutCLI.exe StartCDC -config <filename>`	Specifies the JSON configuration file for the Citrix Diagnostic Collectors (CDC) tool parameters.	`ScoutCLI.exe StartCDC -config xxx.json -path C:\Logs`
`ScoutCLI.exe StartCDC -path <folder>`	Specifies where the output log files are saved.	
`ScoutCLI.exe StopCDC`	Stop the collection of CDC tools.	`ScoutCLI.exe StopCDC`

Collect a Citrix Diagnostic Facility (CDF) trace at system startup

September 2, 2025

The CDFControl utility is an event tracing controller or consumer for capturing Citrix Diagnostic Facility (CDF) trace messages displayed from various Citrix tracing providers. It is intended to troubleshoot complex Citrix-related issues, parse filter support, and collect performance data. To download the CDFControl utility, see CTX111961.

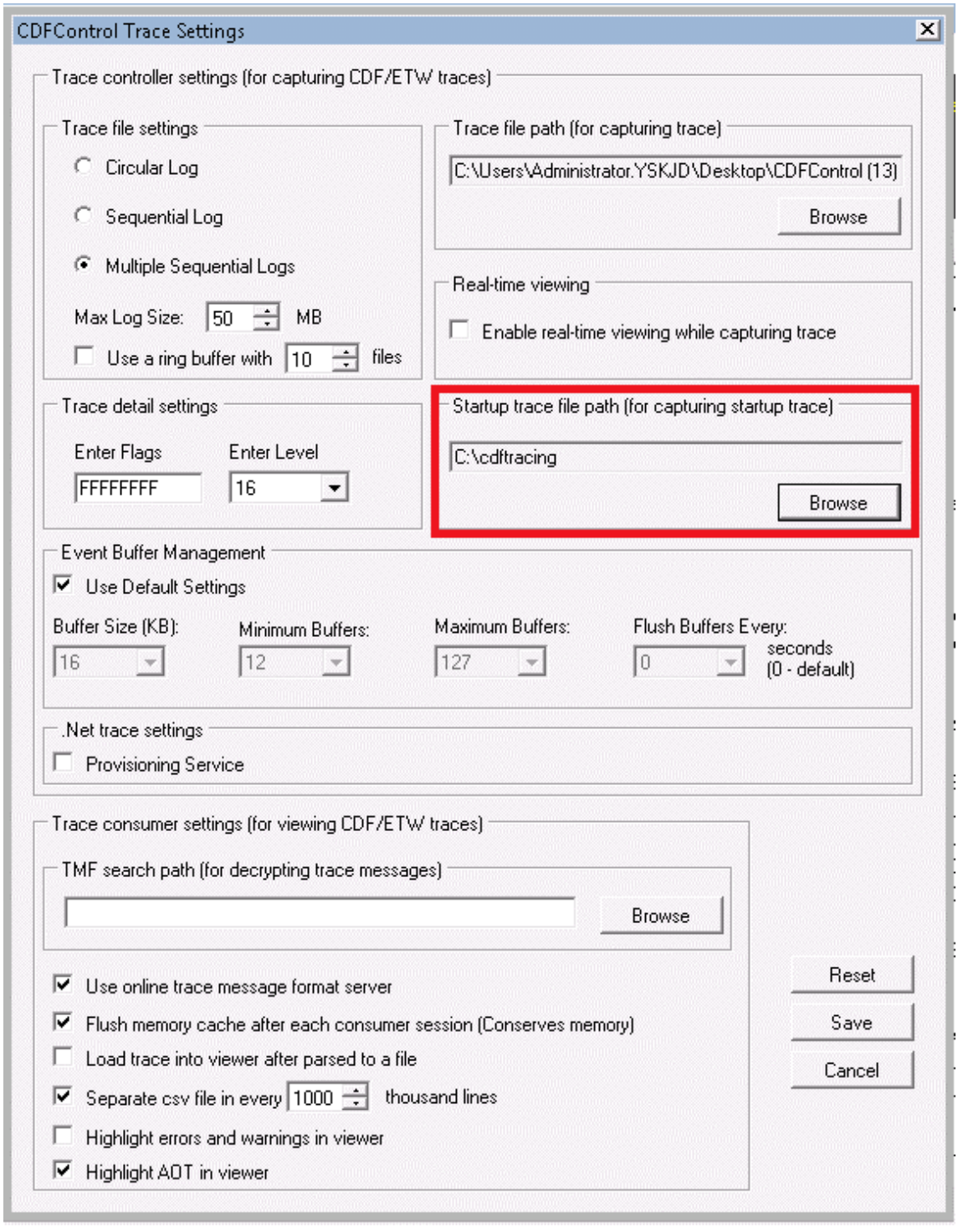
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Collect a trace at system startup

Use the following procedure to collect a CDF trace at system startup. You need administrator privileges.

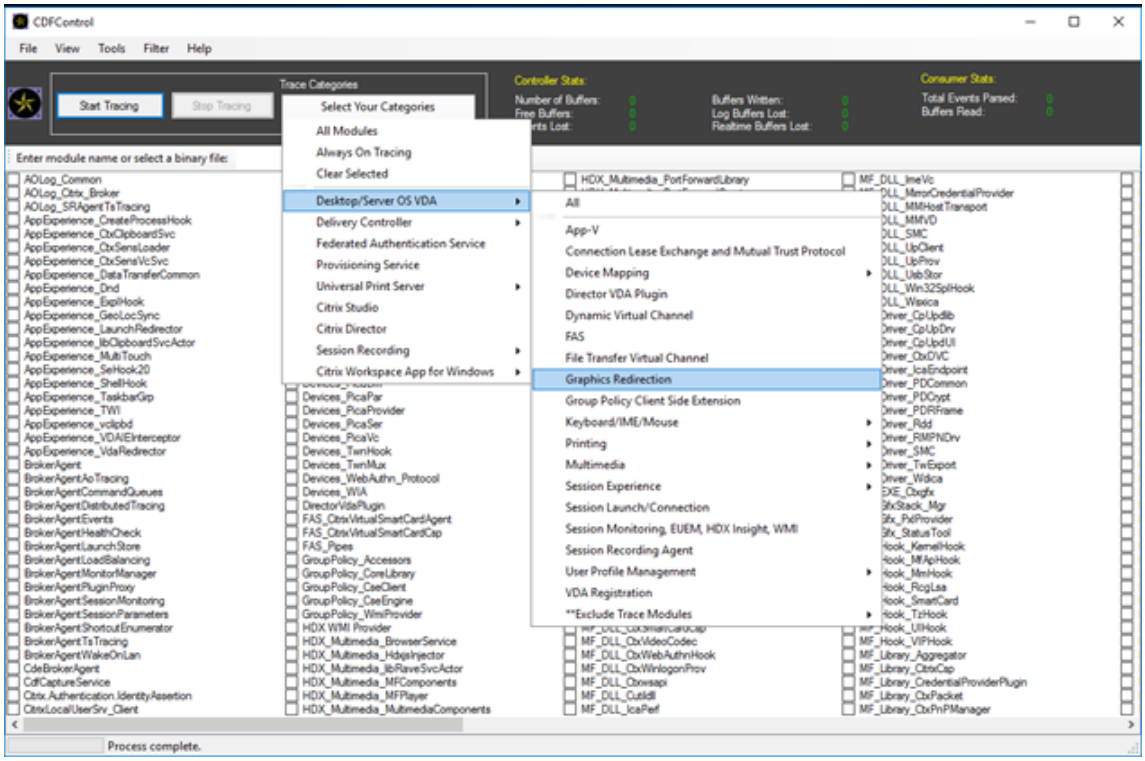
1. Start **CDFControl** and select **Options** from the **Tools** menu.
2. Specify the trace file path in the **Startup trace file path for capturing startup trace** section. Then click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Select the **Trace Categories** recommended by Citrix Support. (In the following example, **Graphics Redirection** is selected. That selection is only an example. We recommend that you enable the providers for the specific issue you are troubleshooting.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Select **Startup Tracing** and select **Enable** from the **Tools** menu.

   After selecting **Enable**, the animated bar starts scrolling. This activity does not affect the procedure. Continue to the next step.

5. After the **Startup Tracing** is enabled, close the **CDFControl utility** and restart the system.
6. Start the **CDFControl** utility. After the system restarts and the error appears, disable startup tracing by selecting **Startup Tracing** from the **Tools** menu, and clicking **Disable**.
7. Go to the trace file path specified in step 2 and collect the trace log file (.etl) for analysis.

Delegated administration

September 13, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The delegated administration model offers the flexibility to match how your organization wants to delegate administration activities, using role and object-based control. Delegated administration accommodates deployments of all sizes, and allows you to configure more permission granularity as your deployment grows in complexity. Delegated administration uses three concepts: administrators, roles, and scopes.

- **Administrators:** An administrator represents a person or a group of people identified by their Active Directory account. Each administrator is associated with one or more role and scope pairs.
- **Roles:** A role represents a job function, and has defined permissions associated with it. For example, the Delivery Group Administrator role has permissions such as 'Create Delivery Group' and 'Remove Desktop from Delivery Group.'An administrator can have multiple roles for a site, so a person can be a Delivery Group Administrator and a Machine Catalog Administrator. Roles can be built-in or custom.

  The built-in roles are:

Role	Permissions
Full Administrator	Can perform all tasks and operations. A Full Administrator is always combined with the All scope.
Read Only Administrator	Can see all objects in specified scopes in addition to global information, but cannot change anything. For example, a Read Only Administrator with Scope=London can see all global objects (such as Configuration Logging) and any London-scoped objects (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).
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Role	Permissions
Machine Catalog Administrator	Can create and manage Machine Catalogs and provision the machines into them. Can build Machine Catalogs from the virtualization infrastructure, Provisioning Services, and physical machines. This role can manage base images and install software, but cannot assign applications or desktops to users.
Delivery Group Administrator	Can deliver applications, desktops, and machines; can also manage the associated sessions. Can also manage application and desktop configurations such as policies and power management settings.
Host Administrator	Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.

In certain product editions, you can create custom roles to match the requirements of your organization and delegate permissions with more detail. You can use custom roles to allocate permissions at the granularity of an action or task in a console.

- **Scopes:** A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your organization (for example, the set of Delivery Groups used by the Sales team). Objects can be in more than one scope; you can think of objects being labeled with one or more scopes. There is one built-in scope: 'All,' which contains all objects. The Full Administrator role is always paired with the **All** scope.

Example

Company XYZ decided to manage applications and desktops based on their department (Accounts, Sales, and Warehouse) and their desktop operating system (Windows 7 or Windows 8). The administrator created five scopes and then labeled each Delivery Group with two scopes: one for the department where they are used and one for the operating system they use.

The following administrators were created:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Administrator	Roles	Scopes
domain/fred	Full Administrator	All (the Full Administrator role always has the All scope)
domain/rob	Read Only Administrator	All
domain/heidi	Read Only Administrator, Help Desk Administrator	All Sales
domain/warehouseadmin	Help Desk Administrator	Warehouse
domain/peter	Delivery Group Administrator, Machine Catalog Administrator	Win7

- Fred is a Full Administrator and can view, edit, and delete all objects in the system.
- Rob can view all objects in the site but cannot edit or delete them.
- Heidi can view all objects and can perform help desk tasks on Delivery Groups in the Sales scope. This allows her to manage the sessions and machines associated with those groups; she cannot make changes to the Delivery Group, such as adding or removing machines.
- Anyone who is a member of the warehouseadmin Active Directory security group can view and perform help desk tasks on machines in the Warehouse scope.
- Peter is a Windows 7 specialist and can manage all Windows 7 Machine Catalogs and can deliver Windows 7 applications, desktops, and machines, regardless of which department scope they are in. The administrator considered making Peter a Full Administrator for the Win7 scope. However, she decided against this, because a Full Administrator also has full rights over all objects that are not scoped, such as 'Site' and 'Administrator.'

How to use delegated administration

Generally, the number of administrators and the granularity of their permissions depends 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 delegation. In this case, create each administrator with the built-in Full Administrator role, which 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 are Full Administrators, and others are Help Desk Administrators. Also, an administrator might manage only certain groups of objects (scopes), such as machine catalogs. In this case, create new scopes, plus administrators with one of the built-in roles and the appropriate scopes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Even larger deployments might require more (or more specific) scopes, plus different administrators with unconventional roles. In this case, edit or create more scopes, create custom roles, and create each administrator with a built-in or custom role, plus existing and new scopes.

For flexibility and ease of configuration, you can create scopes when you create an administrator. You can also specify scopes when creating or editing Machine Catalogs or connections.

Create and manage administrators

When you create a site as a local administrator, your user account automatically becomes a Full Administrator with full permissions over all objects. After a site is created, local administrators have no special privileges.

The Full Administrator role always has the All scope; you cannot change this.

By default, an administrator is enabled. Disabling an administrator might be necessary if you are creating the administrator now, but that person won't start administration duties until later. For existing enabled administrators, you might want to disable several of them while you are reorganizing your object/scopes, then re-enable them when you are ready to go live with the updated configuration. You cannot disable a Full Administrator if it would result in there being no enabled Full Administrator. The enable/disable check box is available when you create, copy, or edit an administrator.

When you delete a role/scope pair while copying, editing, or deleting an administrator, it deletes only the relationship between the role and the scope for that administrator. It does not delete either the role or the scope. It also does not affect any other administrator who is configured with that role/scope pair.

To create and manage administrators, follow these steps:

1. Sign in to Web Studio, click **Administrators** in the left pane, and then click the **Administrators** tab.
2. Follow the instructions for the task you want to complete:

    - **Create an administrator:** Click **Create Administrator** in the action bar. Type or browse to the user account name, select or create a scope, and then select a role. The new administrator is enabled by default; you can change this.
    - **Copy an administrator:** Select the administrator and then click **Copy Administrator** in the action bar. Type or browse to the user account name. You can select and then edit or delete any of the role/scope pairs, and add new ones. The new administrator is enabled by default; you can change this.
    - **Edit an administrator:** Select the administrator and then click **Edit Administrator** in the action bar. You can edit or delete any of the role/scope pairs, and add new ones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Delete an administrator:** Select the administrator and then click **Delete Administrator** in the action bar. You cannot delete a Full Administrator if it would result in there being no enabled Full Administrator.

The upper pane displays the administrators that you created. Select an administrator to view its details in the lower pane. The **Warnings** column indicates whether the role and scope pairs associated with the administrator contain unusable roles or scopes. The following warning message appears if an associated role and scope pair contains unusable roles or scopes:

- Associated role or scope not usable

> **Important:**
>
> A warning message appears only when an associated role and scope pair contains unusable roles or scopes or both.

To remove the role and scope pair from the administrator, complete one of the following steps:

- Delete the role and scope pair.
  1. In the action bar, click **Edit Administrator**.
  2. In the **Administrator Name and Details** window, select the role and scope pair and then click **Delete**.
  3. Click **Save** to exit.
- Delete the administrator.
  1. In the action bar, click **Delete Administrator**.
  2. In the confirmation window, Click **Delete**.

Create and manage roles

When administrators create or edit a role, they can enable only the permissions that they themselves have. This 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).

Role names can contain up to 64 Unicode characters; they cannot contain: 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, or apostrophe. Descriptions can contain up to 256 Unicode characters.

You cannot edit or delete a built-in role. You cannot delete a custom role if any administrator is using it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Only certain product editions support custom roles. Only editions that support custom roles have related entries in the action bar.

To create and manage roles, follow these steps:

1. Sign in to Web Studio, click **Administrators** in the left pane, and then click the **Roles** tab.
2. Follow the instructions for the task you want to complete:
    - **View role details:** Select the role. The lower pane lists the object types and associated permissions for the role. Click the **Administrators** tab in the lower pane to view a list of administrators who currently have this role.
    - **Create a custom role:** Click **Create Role** in the action pane. Enter a name and description. Select the object types and permissions.
    - **Copy a role:** Select the role, and then click **Copy Role** in the action bar. Change the name, description, object types, and permissions, as needed.
    - **Edit a custom role:** Select the role, and then click **Edit Role** in the action bar. Change the name, description, object types, and permissions, as needed.
    - **Delete a custom role:** Select the role, and then click **Delete Role** in the action bar. When prompted, confirm the deletion.

Create and manage scopes

When you create a site, the only available scope is the 'All' scope, which cannot be deleted.

You can create scopes using the following procedure. You can also create scopes when you create an administrator; each administrator must be associated with at least one role and scope pair. When you are creating or editing desktops, machine catalogs, applications, or hosts, you can add them to an existing scope. If you do not add them to a scope, they remain part of the 'All' scope.

Site creation cannot be scoped, nor be delegated administration objects (scopes and roles). However, objects you cannot scope are included in the 'All' scope. (Full Administrators always have the All scope.) Machines, power actions, desktops, and sessions are not directly scoped. Administrators can be allocated permissions over these objects through the associated machine catalogs or delivery groups.

Rules for creating and managing scopes:

- Scope names can contain up to 64 Unicode characters. Scope names cannot include: 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, or apostrophe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Scope descriptions can contain up to 256 Unicode characters.
- When you copy or edit a scope, keep in mind that removing objects from the scope can make those objects inaccessible to the administrator. If the edited scope is paired with one or more roles, ensure that the scope updates do not make any role/scope pair unusable.

To create and manage scopes, follow these steps:

1. Sign in to Web Studio, click **Administrators** in the left pane, and then click the **Scopes** tab.
2. Follow the instructions for the task you want to complete:
    - **Create a scope:** Click **Create new Scope** in the action bar. Enter a name and description. To include all objects of a particular type (for example, Delivery Groups), select the object type. To include specific objects, expand the type and then select individual objects (for example, Delivery Groups used by the Sales team).
    - **Copy a scope:** Select the scope and then click **Copy Scope** in the actions bar. Enter a name and description. Change the object types and objects, as needed.
    - **Edit a scope:** Select the scope and then click **Edit Scope** in the action bar. Change the name, description, object types, and objects, as needed.
    - **Delete a scope:** Select the scope and then click **Delete Scope** in the action bar. When prompted, confirm the deletion.

Set up tenant management

Set up tenant management to create management partitions within a single Citrix Virtual Apps and Desktops site. Each tenant has segregated resources and configurations such as machine catalogs and delivery groups. Administrators with access to a specific tenant can manage only resources and configurations associated with that tenant. Example use cases include corporates with different business silos (independent divisions or separate IT management teams) in a single site.

At a high level, the workflow for setting up tenant management includes:

1. Create tenants
2. Add administrators for tenants

Create tenants

Create a tenant by creating a tenant scope. Detailed steps are as follows:

1. Sign in to Web Studio, click **Administrators** in the left pane, and then click the **Scopes** tab.
2. Click *Create Scope** to start tenant creation.
3. Enter the following details for the tenant scope:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) Type a descriptive name for the scope. This name also serves as the tenant's identifier.
b) (Optional) Enter a brief description.
c) Select **Tenant scope**.
d) If necessary, select the objects associated with the tenant. You can also add objects to tenant scopes when creating or managing objects.
e) Click **OK** to complete the creation.

After completion, you can see:

- The new tenant scope record appears in the Scope list, identified as a **Tenant** in the **Type** column.
- The scope name is shown in the **All Tenants** dropdown list located in the top right corner of Web Studio.

When working with a tenant scope, keep these considerations in mind:

- The tenant property follows a hierarchical assignment order: Hosting > Machine Catalogs > Delivery Groups > Applications. Lower-level objects inherit the tenant property from higher-level objects. For example, when selecting a delivery group for a tenant scope, ensure that you also select the associated hosting and machine catalog. Otherwise, the delivery group cannot inherit the tenant's 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.

Add administrators for tenants

Add administrators for a tenant by assigning user accounts with administrator roles and tenants.

To add an administrator for a tenant, follow these steps:

1. Sign in to Web Studio, click **Administrators** in the left pane, and then click the **Administrators** tab.
2. Click **Add Administrator**, and follow these steps to complete:

    a) Type or browse to the user account name and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b) Select **Custom access** and then select one or more roles (for example, Machine Catalog Administrator) as necessary.
c) Click **Edit scopes** next to each role, change the scope from **All** to the desired tenant scope, and then click **Save**.

3. Click **Next**.
4. On the **Review and confirm** page, click **Send invitation**.

Create reports

You can create two types of delegated administration reports:

- An HTML report that lists the role/scope pairs associated with an administrator, plus the individual permissions for each type of object (for example, delivery groups and machine catalogs). You generate this report from Web Studio.

  To create this report, follow these steps:

  1. Sign in to Web Studio, click **Administrators** in the left pane
  2. Select an administrator and then click **Create Report** in the action bar.

  You can also request this report when creating, copying, or editing an administrator.

- An HTML or CSV report that maps all built-in and custom roles to permissions. You generate this report by running a PowerShell script named OutputPermissionMapping.ps1.

  To run this script, you must be a Full Administrator, a Read Only Administrator, or a custom administrator with permission to read roles. The script is located in: Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts.

  Syntax:

  ```
  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]
  ```

Parameter	Description
`-Help`	Displays script help.
`-Csv`	Specifies CSV output. Default = HTML
`-Path string`	Where to write the output. Default = stdout
`-AdminAddress string`	IP address or host name of the Delivery Controller™ to connect to. Default = localhost

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter	Description
-Show	(Valid only when the -Path parameter is also specified) When you write the output to a file, -Show causes the output to be opened in an appropriate program, such as a web browser.
CommonParameters	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, and OutVariable. For details, see the Microsoft documentation.

The following example writes an HTML table to a file named Roles.html and opens the table in a web browser.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html  – Show
```

The following example writes a CSV table to a file named Roles.csv. The table is not displayed.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
 – CSV -Path Roles.csv
```

From a Windows command prompt, the preceding example command is:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
```

Delivery Controllers

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Delivery Controller is the server-side component that is responsible for managing user access, plus brokering and optimizing connections. Controllers also provide the Machine Creation Services™ that create desktop and server images.

A site must have at least one Controller. After you install the initial Controller, you can add more Controllers when you create a site, or later. There are two primary benefits from having more than one Controller in a site.

- **Redundancy:** As best practice, in a production site, always have at least two Controllers on different physical servers. If one Controller fails, the others can manage connections and administer the site.
- **Scalability:** As site activity grows, so does CPU utilization on the Controller and database activity. Additional Controllers enable you to handle more users and more applications and desktop requests, and can improve overall responsiveness.

Each Controller communicates directly with the site database. In a site with more than one zone, the Controllers in every zone communicate with the site database in the primary zone.

> **Important:**
>
> Do not change the computer name or the domain membership of a Controller after the site is configured.

How VDAs register with Controllers

Before a VDA can be used, it must register (establish communication) with a Delivery Controller in the site. For information about VDA registration, see VDA registration with Controllers.

Add, remove, or move Controllers

To add, remove, or move a Controller, you must have the server role and database role permissions listed in the Databases article.

Installing a Controller on a node in an SQL clustering or SQL mirroring installation is not supported.

When you add a Delivery Controller™ to a site, be sure to add logon credentials for that machine to any replica SQL Servers that you use for high availability.

If your deployment uses database mirroring:

- Before adding, removing, or moving a Controller, ensure that the principal and mirrored databases are both running. In addition, if you are using scripts with SQL Server Management Studio, enable SQLCMD mode before running the scripts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To verify mirroring after adding, removing, or moving a Controller, run the PowerShell `Get-configdbconnection` cmdlet. That cmdlet ensures that the Failover Partner has been set in the connection string to the mirror.

After you add, remove, or move a Controller:

- If auto-update is enabled, the VDAs receive an updated list of Controllers within 90 minutes.
- If auto-update is not enabled, ensure that the Controller policy setting or ListOfDDCs registry key are updated for all VDAs. After moving a Controller to another site, update the policy setting or registry key on both sites.

Add a Controller

You can add Controllers when you create a site and later. You cannot add Controllers installed with an earlier version of this software to a site that was created with this version.

1. Run the installer on a server containing a supported operating system. Install the Delivery Controller component and any other core components you want. Complete the installation wizard.
2. If you have not yet created a site, run Citrix Site Manager on this Controller to create a site. The IP address of this Controller is automatically added to the new site.

   If you plan to generate scripts that initialize the databases, add the Controllers before you generate the scripts.
3. If you have already created a site, follow these steps:

   a) Run Citrix Site Manager on this Controller, click **Join an existing site**, and type the address of a Controller in the site that you want to join.
   b) Run Studio configuration tool to add the Controller to the Web Studio.

Remove a Controller

Removing a Controller from a site does not uninstall the Citrix software or any other component. That action removes the Controller from the database so that it can no longer be used to broker connections and perform other tasks. If you remove a Controller, you can later add it back to the same site or to another site. A site requires at least one Controller, so you cannot remove the last one listed in Web Studio.

When you remove a Controller from a site, the Controller logon to the database server is not removed. This avoids potentially removing a logon that is used by other products' services on the same machine. The logon must be removed manually if it is no longer required. The `securityadmin` server role permission is needed to remove the logon.

After you remove a Controller:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VDAs using auto-update reregister with other available Controllers. This reregistration occurs only if the auto-update mechanism is enabled and the VDAs can reach other controllers (in the same secondary zone as the removed Controller, or in the primary zone for on-premises deployments).
- Update Controller information in Citrix StoreFront. For more information, see Manage Controllers.
- In Citrix StoreFront, update Secure Ticket Authority (STA) URLs for remote access through Citrix Gateway. For more information, see Manage Secure Ticket Authorities.
- In Citrix Gateway, update any virtual server STA URLs. For more information, see Citrix Gateway.

> **Important:**
>
> Do not remove the Controller from Active Directory until after you remove it from the site.

1. Make sure that the Controller is powered on so that Web Studio loads can load and displays the Controller you want to remove.
2. After Web Studio has fully loaded the Controller, verify that all the services on the Controller are running and the Controller remains powered on.
3. Sign in to Web Studio, select **Settings** in the left pane.
4. Locate the **Delivery Controller** tile and click **Edit**.
5. On the **Manage Delivery Controller** page, select the Controller you want to remove.
6. Select **Remove Controller**. If you do not have the correct database roles and permissions, you are offered the option of generating a script that allows your database administrator to remove the Controller for you.

   Web Studio performs a pre-check before removing a Controller. A controller is safe to remove if it is powered off and not in the following service status:

   - Unknown
   - Pending failure
   - Older version
   - Newer version
   - Version change in progress
   - Missing mandatory features

   If the Controller is not powered off and is in any of the mentioned service status, Web Studio prompts you to power off the Controller.
7. You must remove the Controller's machine account from the database server. Before removing, check that another service is not using the account.

After using Web Studio to remove a Controller, traffic to that Controller might linger for a short amount of time to ensure proper completion of current tasks. If you want to force the removal of a Controller

© 1997–2026 Citrix Systems, Inc. All rights reserved.

in a short time, Citrix recommends you shut down the server where it was installed, or remove that server from Active Directory. Then, restart the other Controllers on the site to ensure no further communication with the removed Controller.

Move a Controller to another zone

If your site contains more than one zone, you can move a Controller to a different zone. See the Zones for information about how this moving can affect VDA registration and other operations.

1. Select **Zone** in the left pane.
2. Select a zone in the middle pane, and then select a Controller.
3. Select **Move Items** in the action bar.
4. On the **Move Items** page that appears, select the zone where you want to move the Controller.
5. Click **Save**.

Move a VDA to another site

If a VDA was provisioned using Citrix Provisioning™ or is an existing image, you can move a VDA to another site (from site 1 to site 2) when upgrading, or when moving a VDA image that was created in a test site to a production site. VDAs provisioned using Machine Creation Services (MCS) cannot be moved from one site to another. MCS does not support changing the ListOfDDCs a VDA checks to register with a Controller. VDAs provisioned using MCS always check the ListOfDDCs associated with the site in which they were created.

There are two ways to move a VDA to another site: using the installer or Citrix policies.

Installer Run the installer and add a Controller, specifying the FQDN (DNS entry) of a Controller in site 2.

Specify Controllers in the installer only when the Controllers policy setting is not used.

Group Policy Editor The following example moves multiple VDAs between sites.

1. Create a policy in site 1 that contains the following settings, then filter the policy to the Delivery Group level to initiate a staged VDA migration between the sites.
    - Controllers: Containing FQDNs (DNS entries) of one or more Controllers in site 2.
    - Enable auto update of Controllers: set to disabled.
2. Each VDA in the Delivery Group is alerted within 90 minutes of the new policy. The VDA ignores the list of Controllers it receives (because auto-update is disabled); it selects one of the Controllers specified in the policy, which lists the Controllers in site 2.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. When the VDA successfully registers with a Controller in site 2, it receives the site 2 ListOfDDCs and policy information, which has auto-update enabled by default. The Controller with which the VDA was registered in site 1 is not on the list sent by the Controller in site 2. So, the VDA re-registers, choosing among the Controllers in the site 2 list. From then on, the VDA is automatically updated with information from site 2.

For information about how to use the Group Policy Editor, see the Citrix policies documentation.

Home page for Web Studio

September 13, 2025

The Web Studio's Home page provides an overview of your Citrix Virtual Apps and Desktops™ deployment and workloads along with information that helps you get the most from your subscription. This article introduces the available widgets on this page:

- Site details
- Resources
- Sessions
- Recent
- Errors and warnings
- Get started

You can customize this Home page by adding, removing, or repositioning widgets to suit your needs.

Site details

This widget provides an at-a-glance summary of your Citrix Virtual Apps and Desktops site. It displays key information such as your license type, Studio version, and the version and status of your Delivery Controllers.

Resources

This widget provides an overview of your Citrix Virtual Apps and Desktops 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 Director.

Sessions

This widget provides an overview of your Citrix Virtual Apps and Desktops workloads in the last 7 days. Shows the number of desktop and app sessions launched daily over the previous seven days.

Recent

This widget displays a history of objects that you've recently accessed in Web Studio. It helps you quickly review your object access history. Clicking an object name in the list takes you directly to that object within its respective node.

Keep the following in mind:

- The list is stored locally in your browser's cache. Clearing your cache, switching browsers, or using incognito mode resets the list.
- The list is limited to the last 100 objects that you've accessed within the past 30 days.
- This list records only individual object views or operations. If you select *multiple* objects at once, they *aren't* recorded in the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The following objects *aren't* tracked:
  - Objects within the **Settings**, **Licensing**, and **Logging** nodes.
  - Objects within the **Comparison** and **Modeling** tabs of the **Policies** node.
  - Objects within the **History** and **Settings** tabs of the **Backup and restore** node.

Get started

This widget guides you through a series of questions to help you set up your Citrix Virtual Apps and Desktops deployment. By answering these questions, you can quickly configure your deployment.

Errors and warnings

Centrally displays errors and warnings from your 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.

Customize the Home page

To customize the Home page, follow these steps:

1. Sign in to Web Studio.

   The home page appears.
2. Click the **Edit** icon in the top right corner of the Home page.
3. To reposition a widget, drag it to a wanted position.
4. To remove a widget from the Home page, click the **Delete** icon in the top right of the widget.
5. To add a widget back to the Home page, click the **Add widget** icon in the top right corner of the Home page.
6. Click **Done** to save changes.

IPv4/IPv6 support

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This release supports pure IPv4, pure IPv6, and dual-stack deployments that use overlapping IPv4 and IPv6 networks.

The following components support only IPv4. All others support IPv4 and IPv6.

- XenServer®
- Virtual Delivery Agents (VDAs) not controlled by the **Only use IPv6 Controller registration** policy setting

IPv6 communications are controlled with two VDA connection-related Citrix® policy settings.

- **Primary setting that enforces the use of IPv6:** Only use IPv6 Controller registration.

  This policy setting controls which form of address the VDA uses to register with the Delivery Controller.

  When enabled, the VDA registers and communicates with the Controller using a single IPv6 address chosen in the following precedence: global IP address, Unique Local Address (ULA), link-local address (only if no other IPv6 addresses are available).

  When disabled, the VDA registers and communicates with the Controller using the machine's IPv4 address. This is the default value.

  If a team frequently uses an IPv6 network, publish the desktops and applications for those users based on an image or Organizational Unit (OU) that has the **Only use IPv6 Controller registration** policy setting enabled.

  If a team frequently uses an IPv4 network, publish the desktops and applications for those users based on an image or OU that has the **Only use IPv6 Controller registration** policy setting disabled.

- **Dependent setting that defines an IPv6 netmask:** Controller registration IPv6 netmask.

  A machine can have multiple IPv6 addresses. This policy setting allows administrators to restrict the VDA to only a preferred subnet, rather than a global IP, if one is registered. This setting specifies the network where the VDA registers. The VDA registers only on the first address that matches the specified netmask.

  This setting is valid only when the **Only use IPv6 Controller registration policy** setting is enabled. Default = Empty string

Deployment considerations

If your environment contains both IPv4 and IPv6 networks, create separate delivery group configurations for IPv4-only clients and for the clients who can access the IPv6 network. Consider using naming, manual Active Directory group assignment, or SmartAccess filters to differentiate users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session reconnection might fail if the connection starts on an IPv6 network, and then you try to connect again from a client that has only IPv4 access.

NOTE - These considerations do not apply if you have DNS resolution enabled

Licensing for Citrix Virtual Apps and Desktops™ using Web Studio

December 12, 2025

> **Note:**
>
> - You can manage your Citrix Virtual Apps and Desktops deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.
> - The License Activation Service (LAS) is a new cloud-based licensing solution that provides an alternative to the traditional Citrix® legacy licensing. LAS introduces new modules for activation, ensuring a seamless and modern approach to license management. See License Activation Service for more information.

From Web Studio, you can manage and track licensing, if the license server is in the same domain as Web Studio or in a trusted domain. For information about licensing tasks, see the licensing documentation and Multi-type licensing.

The following table lists the supported editions and license models:

Products	Editions	License models
Citrix Virtual Apps	Premium, Advanced, Standard	Concurrent
Citrix Virtual Desktops	Premium, Advanced, Standard	User/Device and Concurrent

For more information, see Concurrent license and User/device license.

Supported Current Release (CRs) and Long Term Service Release (LTSRs) version

Citrix strongly recommends that you always use the latest available version of Citrix License Server to benefit from any functional or security improvements it may contain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The License Server VPX is deprecated and won't receive any further maintenance or security fixes. Customers using 11.16.6 or previous versions of License Server VPX are advised to migrate to the latest version of License Server for Windows as soon as possible.

For more information about Citrix products' lifecycle dates, see Product Matrix.

For information on legacy products and product versions, refer to the Legacy Product Matrix.

You must be a full license administrator to complete the following tasks. To view license information in Web Studio, an administrator must have at least the Read Licensing delegated administration permission. The built-in Full Administrator and Read-Only Administrator roles have that permission.

Download and install a license from Citrix using Web Studio

1. Sign in to Web Studio and select **Licensing** in the left pane.
2. Select **Allocate Licenses** in the action bar.
3. Enter the License Access Code. You received in an email from Citrix after licenses are purchased or renewed.
4. Select a product and choose **Allocate Licenses**. Licenses available for that product are allocated and downloaded. After you allocate and download all the licenses for a specific License Access Code, you cannot reuse that License Access Code. To do other transactions with the same code, log on to My Account.

Add licenses that are stored on your local computer or on the network

1. Sign in to Web Studio and select **Licensing** in the left pane.
2. Select **Add Licenses** in the action bar.
3. Browse to a license file and add it to the license server.

Change the license server

1. Sign in to Web Studio and select **Licensing** in the left pane.
2. Select **Change License Server** in the action bar.
3. Type the address of the license server in the form *name:port*, where the name is a DNS, NetBIOS, or IP address. If you do not specify a port number, the default port (27000) is used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Select the type of license to use

- When configuring the Site, after you specify the license server, you're prompted to select the type of license to use. If there are no licenses on the server, the option to use the product for a 30-day trial period without a license is automatically selected.
- If there are licenses on the server, their details are displayed and you can select one of them. Or, you can add a license file to the server and then select that one.

Change the product edition and licensing model

1. Sign in to Web Studio and select **Licensing** in the left pane.
2. Select **Edit Product Edition** in the action bar.
3. Update the appropriate options.

To access the License Administration Console, in the action bar, select **License Administration Console**. The console either appears immediately, or if the dashboard is configured as password-protected, you're prompted for License Administration Console credentials. For details about how to use the console, see the licensing documentation.

> **Note:**
>
> When you switch licenses in the Web Studio, the change takes up to 5 minutes to appear in the Citrix Director. For example, if you switch between Advanced and Premium.

Add a licensing administrator

1. Sign in to Web Studio and select **Licensing** in the left pane.
2. Select the **Licensing Administrators** tab.
3. Select **Add licensing administrator** in the action bar.
4. Browse to the user you want to add as an administrator and choose permissions.

Change a licensing administrator's permissions or delete a licensing administrator

1. Sign in to Web Studio and select **Licensing** in the left pane.
2. Select the **Licensing Administrators** tab and then select the administrator.
3. Select either **Edit licensing administrator** or **Delete licensing administrator** in the action bar.

Add a licensing administrator group

1. Sign in to Web Studio and select **Licensing** in the left pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the **Licensing Administrators** tab.
3. Select **Add licensing administrator group** in the action bar.
4. Browse to the group you want to act as licensing administrators and choose permissions. Adding an Active Directory Group gives licensing administrator permissions to the users within that group.

Change a licensing administrator group's permissions or delete a licensing administrator group

1. Sign in to Web Studio and select **Licensing** in the left pane.
2. Select the **Licensing Administrators** tab and then select the administrator group.
3. Select either **Edit licensing administrator group** or **Delete licensing administrator group** in the action bar.

View license information

Sign in to Web Studio and select **Licensing** in the left pane. A summary of license usage and settings for the Site is displayed with a list of all the licenses currently installed on the specified license server.

Ensure that the licensing settings for the site, which include the product type, license edition, and licensing model, match the licenses your configured License Server uses. If not, you might have to download or allocate your exiting licenses to match the site's license settings.

Run the command `Get-Brokersite` to get the following licensing information:

- TotalUniqueLicenseUsers
- PeakConcurrentLicenseUsers
- PeakConcurrentLicensedDevice

> **Note:**
>
> Use the cloud licensing APIs to get the information in Citrix DaaS. For information on cloud licensing APIs, see APIs to manage Citrix Cloud licensing.

View license expiration alerts

Web Studio queries for license file expiration dates from the Citrix License Server. Web Studio alerts administrators on the Overview tab if license files are approaching expiration or already expired.

Related links

- See Citrix on-premises subscription for annual and term-based retail licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- See Transition and Trade-Up (TTU) with Hybrid Rights.

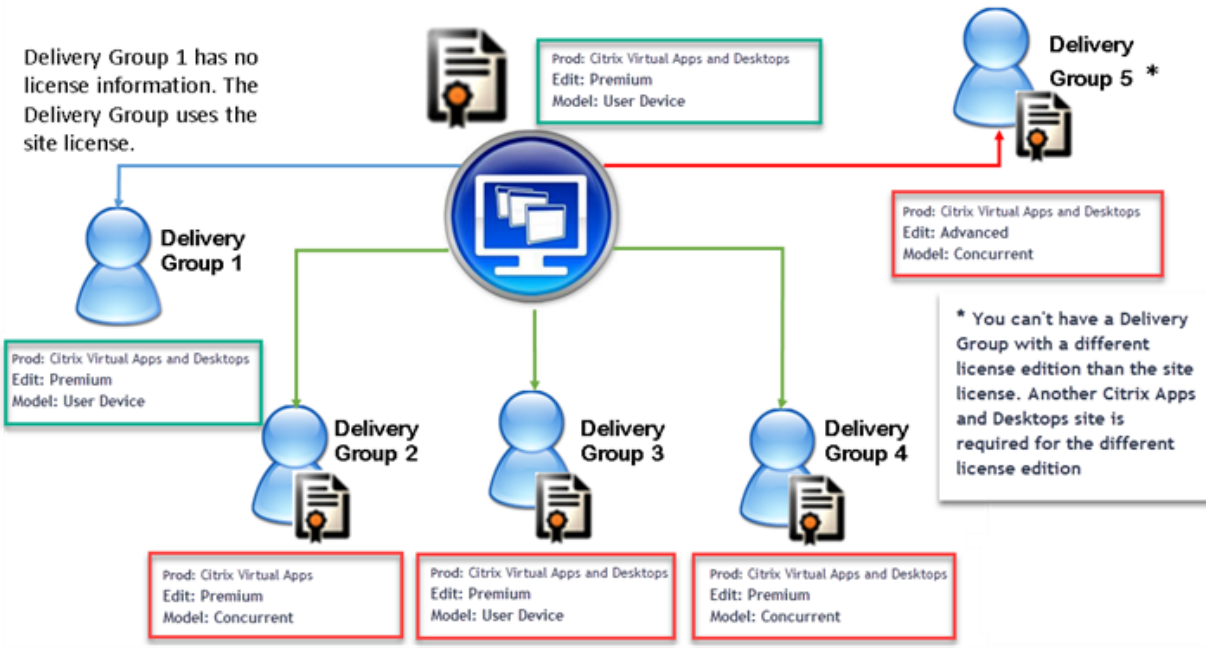
Multi-type licensing

September 6, 2025

> **Note:**
>
> License Activation Service does not support multi-type licensing.

Multi-type licensing supports consumption of different license types for delivery groups on a single Citrix Virtual Apps and Desktops site. **Type** is a single combination of Product ID (XDT or MPS) and Model (UserDevice or Concurrent). The delivery groups must use the same Product Edition (PLT/Premium or ENT/Advanced) as configured at the site level. Be aware of the special considerations at the end of this article when looking to configure multi-type licensing for your Citrix Virtual Apps and Desktops deployments.

If multi-type licensing is not configured, different license types can be used only when configured for separate sites. The delivery groups use the site license. For important notification limitations when multi-type licensing is configured, see Special considerations.



To determine the delivery groups that consume the different types of licenses, use these Broker PowerShell cmdlets:

- New-BrokerDesktopGroup

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

To install licenses, use:

- Citrix Studio
- Citrix Licensing Manager
- citrix.com

Customer Success Services dates are specific to each license file and to each product and model. Delivery groups set differently might have different Customer Success Services dates than each other.

Special considerations

Multi-type licensing has different functionality than regular Citrix Virtual Apps and Desktops™ licensing.

There are no alerts and notifications from Director or Studio for delivery groups configured to use a type that differs from the site configuration:

- No information when nearing license limits or the trigger or expiry of the License burst mode.
- No notification when a specific group has a problem.

Delivery groups configured for multi-type licenses consume ONLY that license type and don't fall back to the site configuration when fully consumed.

Though Citrix Virtual Apps Standard and Citrix Virtual Desktops™ Standard license edition names indicate that they are both Standard, they are not the same edition. Multi-type licensing is not available with Citrix Virtual Apps Standard and Citrix Virtual Desktop Standard licenses.

License compatibility matrix

This table details old product names, new product names, and the associated feature names. The four compatibility columns specify which product and license model combinations are compatible for multi-type licensing. CCU and CCS stand for concurrent licenses and UD is user/device licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

Broker PowerShell SDK

The **DesktopGroup** object has these two properties you can manipulate using the associated New-BrokerDesktopGroup and Set-BrokerDesktopGroup cmdlets.

Name	Value	Restriction
LicenseModel	A parameter (Concurrent or UserDevice) specifying the licensing model for the group. If none is specified, the site-wide license model is used.	If the feature toggle is disabled, attempting to set a property fails.
ProductCode	A text string of XDT (for Citrix Virtual Desktops) or MPS (for Citrix Virtual Apps™) specifying the licensing Product ID for the group. If none is specified, the site-wide product code is used.	If the feature toggle is disabled, attempting to set a property fails.

For more information about the LicenseModel and ProductCode, see about_Broker_Licensing.

New-BrokerDesktopGroup

Creates a desktop group for managing the brokering of groups of desktops. For more information on this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set-BrokerDesktopGroup

Disables or enables an existing broker desktop group or alters its settings. For more information on this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

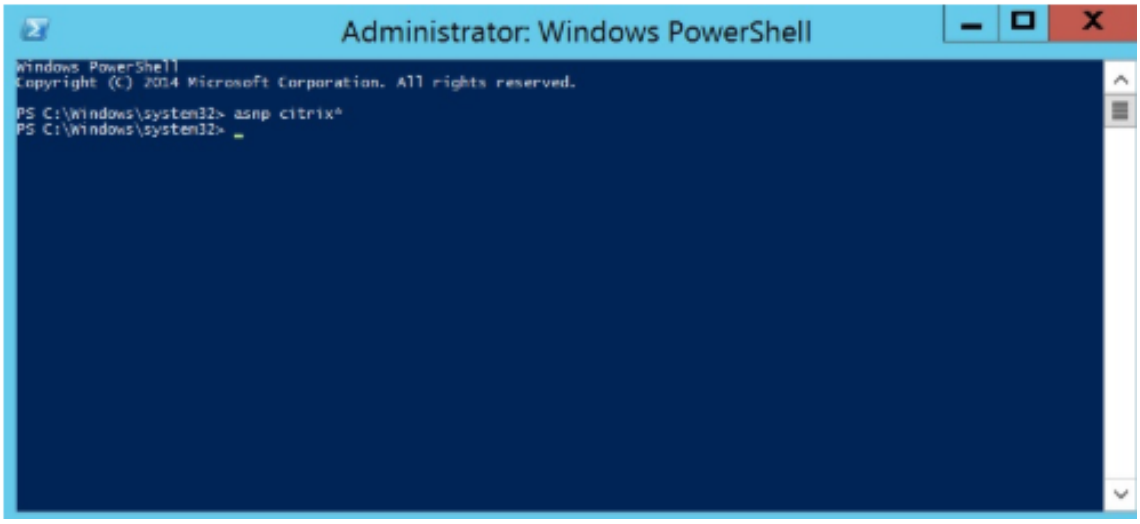
Get-BrokerDesktopGroup

Retrieves desktop groups matching the specified criteria. The output of the Get-BrokerDesktopGroup cmdlet includes the **ProductCode** and **LicenseModel** properties of the group. If the properties have not been set using New- BrokerDesktopGroup or Set-BrokerDesktopGroup, null values are returned. If null, the site-wide license model and product code are used. For more information on this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/.

Configure different license products and models per delivery group

> **Note:**
>
> You can't configure two or more different types of products, editions, or license models configured on a single delivery group. In case you have different types of products, editions, or license models, configure them in separate delivery groups.

1. Open PowerShell with Administrative rights and add the Citrix snap-in.

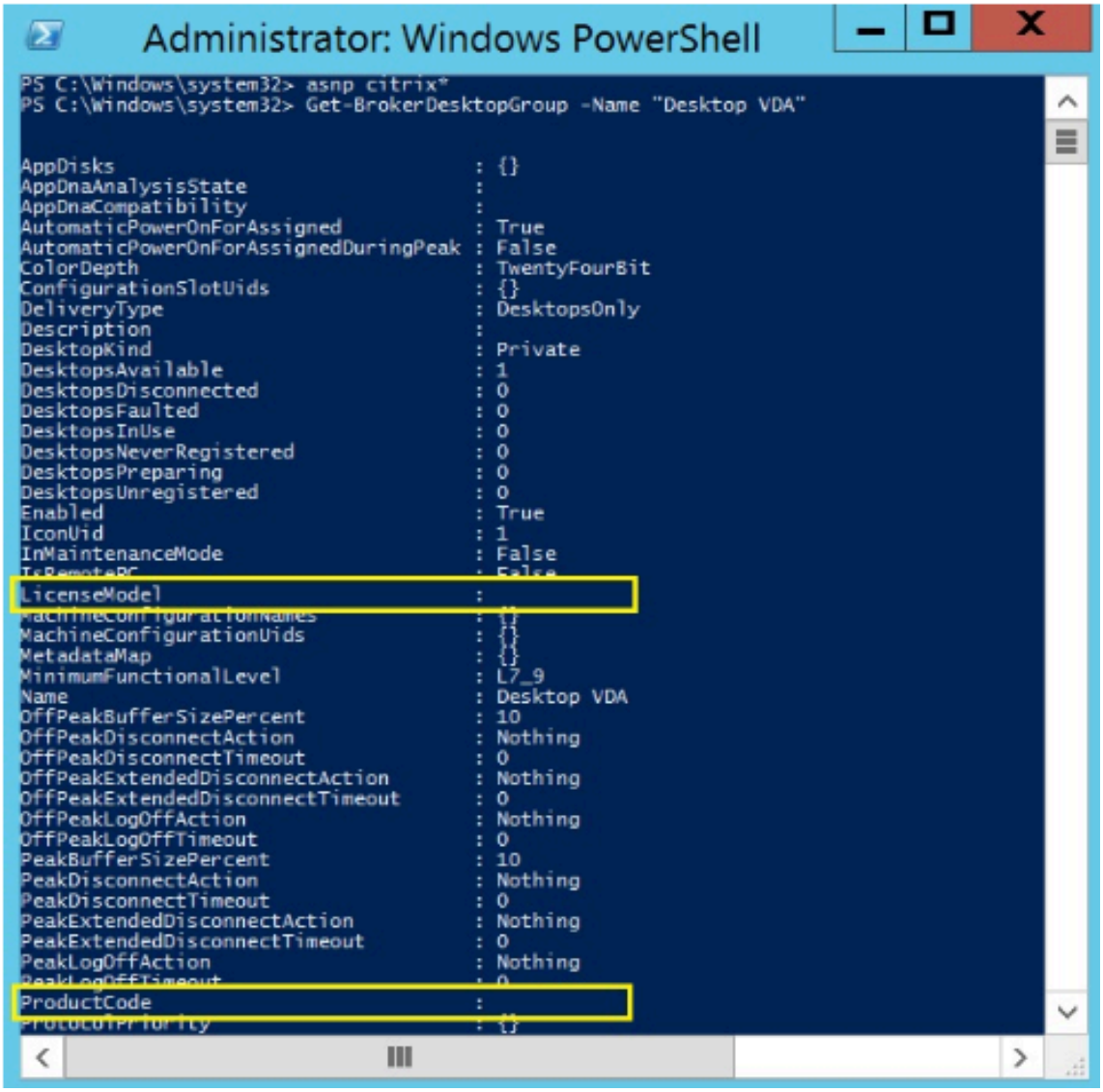


2. Run the command **Get-BrokerDesktopGroup –Name "DeliveryGroupName"** to view the current license configuration. Find the parameters **LicenseModel** and **ProductCode**. If you haven't configured these parameters before, they might be blank.

   > **Note:**
   >
   > If a delivery group does not have license information set, it defaults to **Site level Site li-**

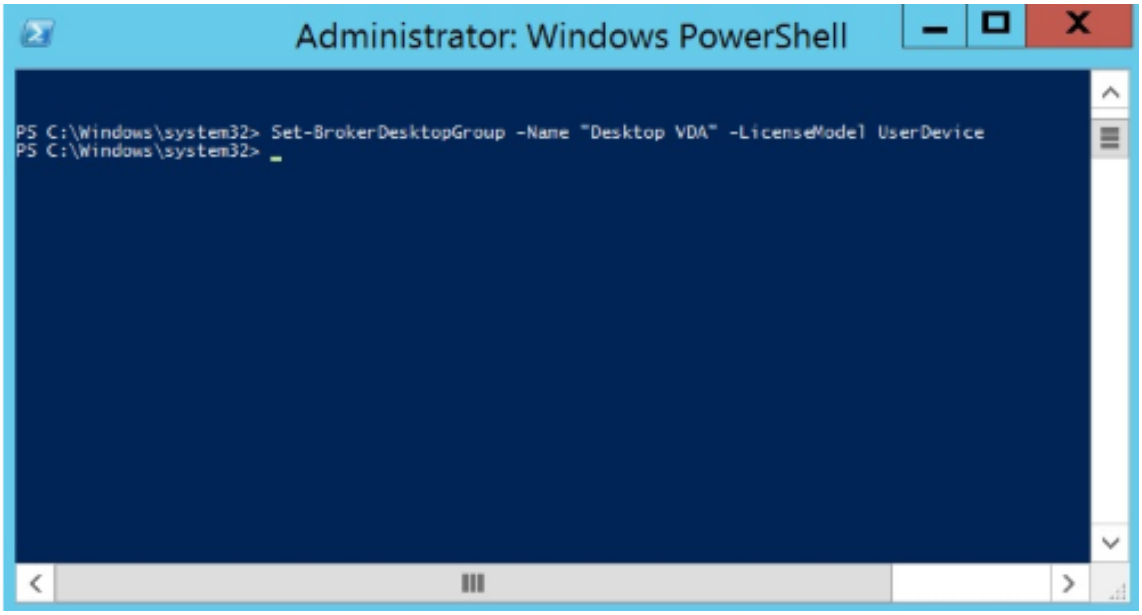
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **cense**.

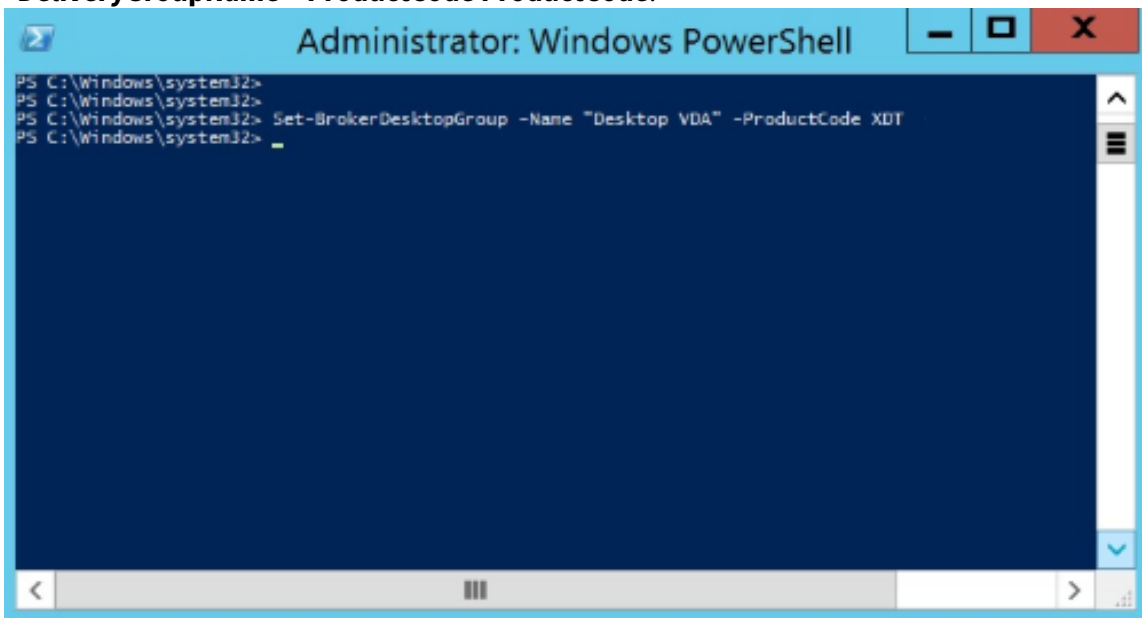


3. Change the license model by running the command: **Set-BrokerDesktopGroup –Name "DeliveryGroupName"–LicenseModel LicenseModel**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



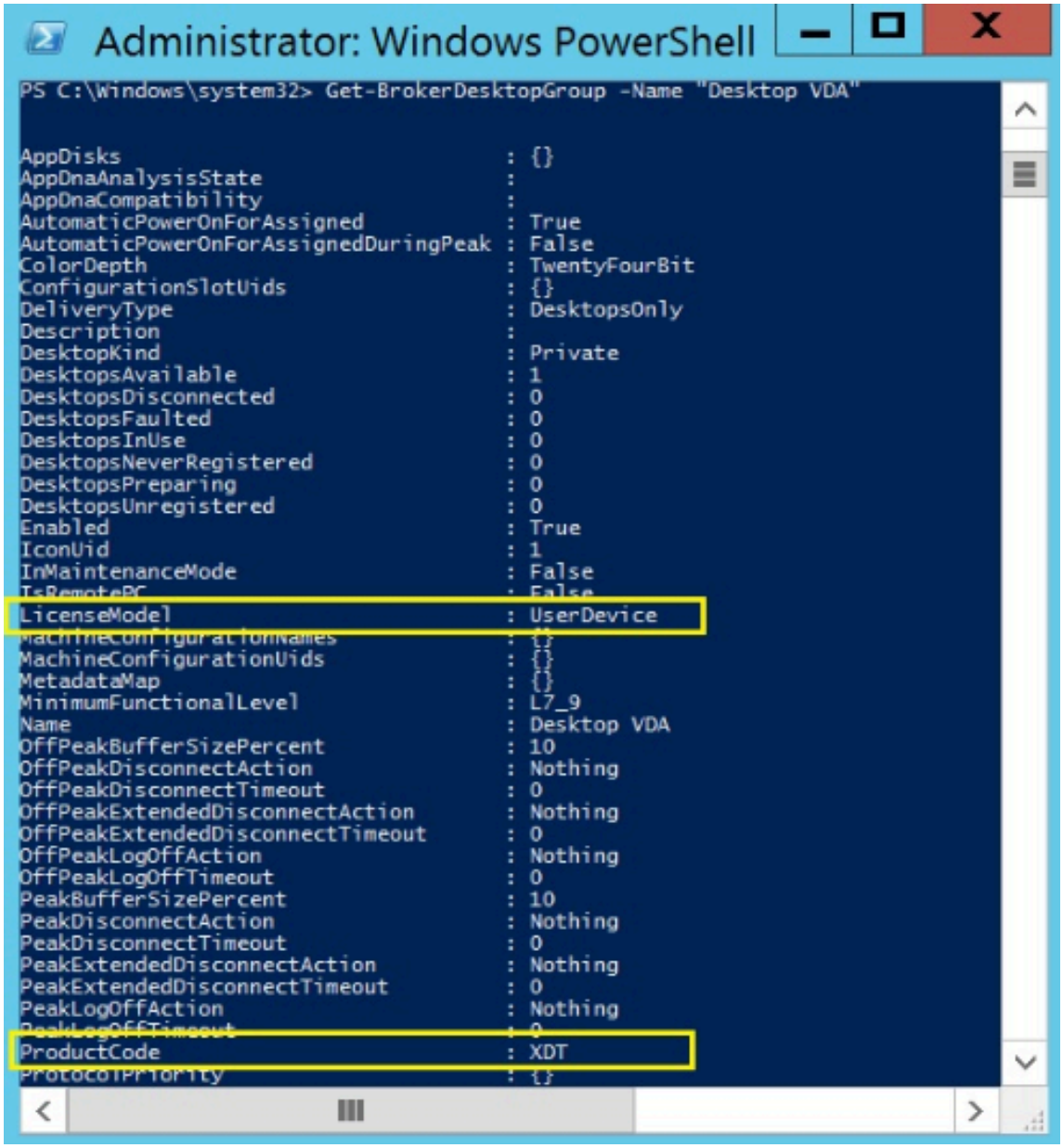
4. Change the license product by running the command: **Set-BrokerDesktopGroup –Name "DeliveryGroupName"–ProductCode ProductCode**.



5. Enter the command **Get-BrokerDesktopGroup –Name "DeliveryGroupName"** to validate the changes.

> **Note:**
>
> You cannot mix and match editions in the same site. For example, Premium and Advanced licenses. Multiple sites are required if you have licenses with different editions.

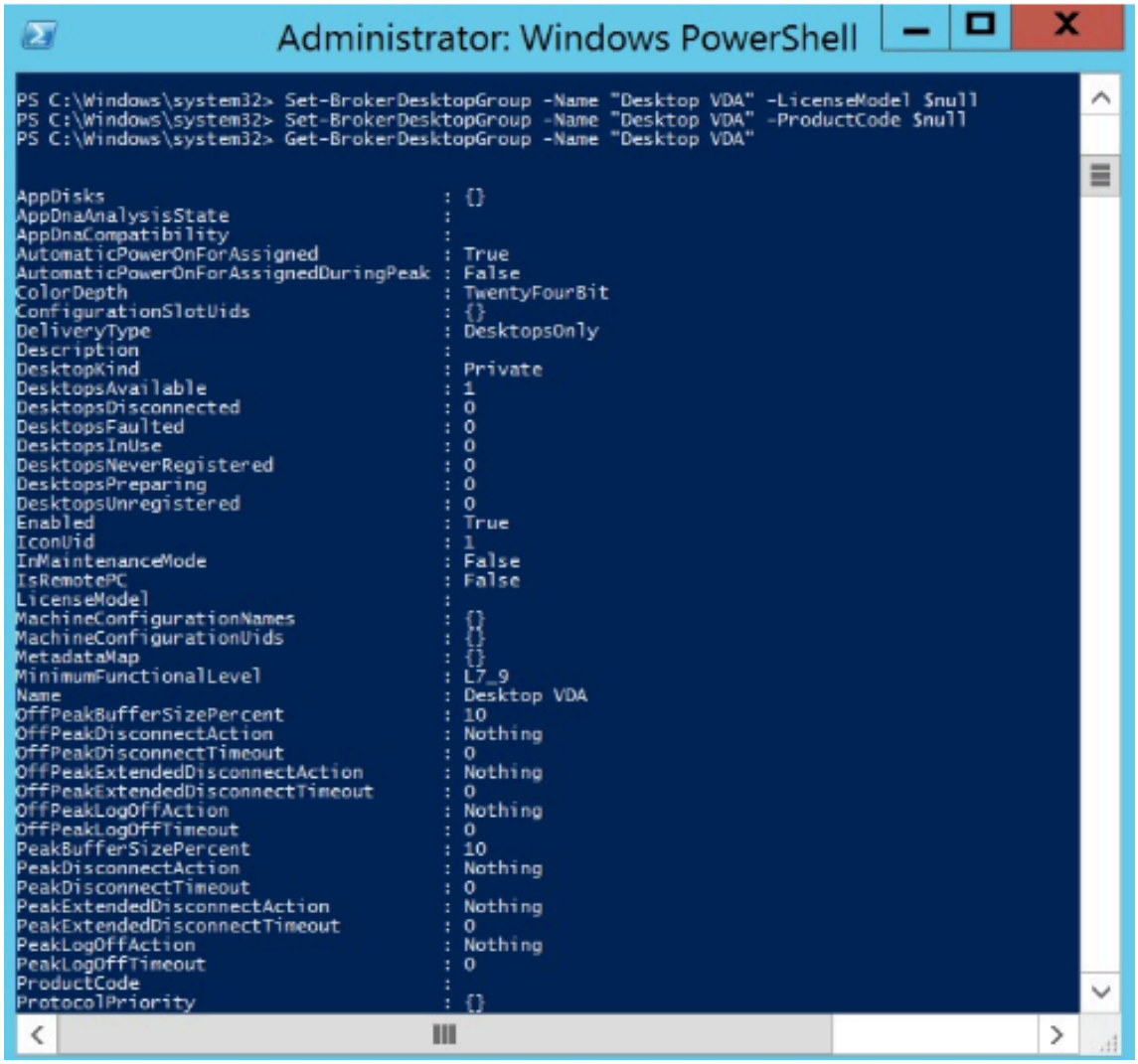
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Remove the license configuration by running the same **Set-BrokerDesktopGroup** commands as described in previous steps, and set the value to **$null**.

> **Note:**
>
> Studio doesn't display the license configuration for each delivery group. Use PowerShell to view the current configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Example

This PowerShell cmdlet example illustrates setting multi-type licensing for two existing delivery groups and creates and sets a third delivery group.

To see the license product and license model associated with a delivery group, use the **Get-BrokerDesktopGroup** PowerShell cmdlet.

1. We set the first delivery group for XenApp® and Concurrent.

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Apps Premium Concurrent”-ProductCode MPS -LicenseModel Concurrent

2. We set the second delivery group for XenDesktop® and Concurrent.

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium Concurrent”-ProductCode XDT -LicenseModel Concurrent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. We create and set the third delivery group for XenDesktop and UserDevice.

   New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice”-PublishedName “MyDesktop”-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

License Activation Service

April 22, 2026

The License Activation Service (LAS) is a new cloud-based licensing solution that provides an alternative to the traditional Citrix® legacy licensing. LAS introduces new modules for activation, ensuring a seamless and modern approach to license management.

The LAS simplifies the Citrix Licensing experience. There are no longer license access codes or files to generate, download, or install on the license server. You only need to upgrade your license server and register with Citrix Cloud. Once the compatible products are pointed to the license server, they can be activated automatically.

After activation, the License Server regularly communicates with the License Activation Service to keep its activation up to date. The LAS is built with cloud technology, which improves performance and ensures that there is no downtime. If, for any reason, the License Server or LAS is unreachable, the system enters license caching mode, which is designed to protect the system from being unlicensed and avoid an outage. For more information, see License caching mode.

For more details on LAS, see the Licensing documentation License Activation Service.

Prerequisites

- Install or update the License Server to version 11.17.2 build 53100 or later.
- Reliable and continuous internet connection for the License Server.
- Desktop Group level license settings must be disabled.

> **Note:**
>
> To ensure if DG level licensing is disabled, use Get-brokerdesktopgroup and LicenseModel should be “None”.

Considerations

- All Delivery Controllers must be compatible with LAS before the Web Studio prompts for activation. A single site can use either legacy licenses or LAS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can have multiple License Servers registered with the same Citrix Cloud ID (CCID) or OrgID. However, a site can be configured to point to only one license server.

Limitations

- Migrating to LAS sets the Product Edition to **Premium** and the License Model to **Concurrent** but this might change in the future. Do not modify the license configuration using PowerShell as this might impact registration and session launch.
- You can migrate your Citrix Virtual Apps and Desktops™ site from the existing legacy license to LAS using only Web Studio.

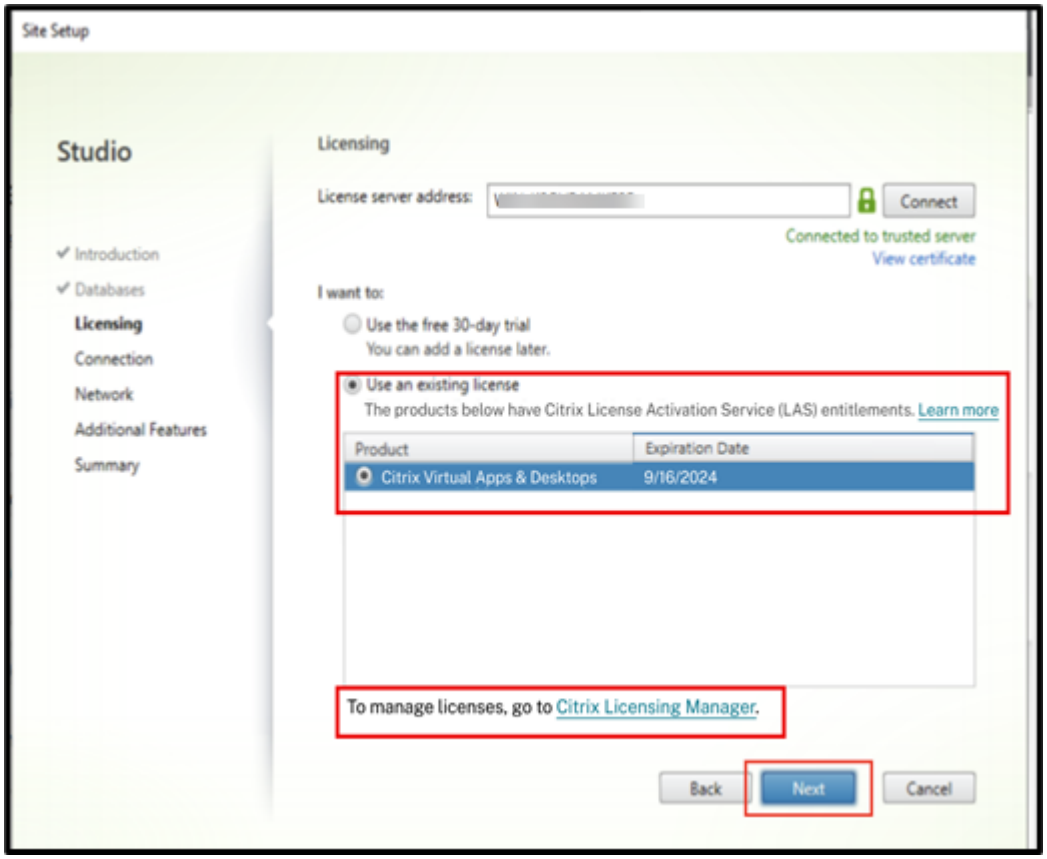
Key steps

1. Install or upgrade the License Server to version 11.17.2 build 53100 or later and configure LAS as per the instructions mentioned in How to Configure License Server for License Activation Service.
2. Install Citrix Virtual Apps and Desktops version 2411 or later. Install the core components, such as Citrix Delivery Controller, Citrix Studio, Web Studio, and Citrix Director.

   > **Note:**
   >
   > All Delivery Controllers in the Citrix Virtual Apps and Desktops site must be compatible with LAS.

3. After you install the required components, use Citrix Site Manager to create a site. For information on creating a site, see Create a site. If the License Server is configured to use LAS, the Metainstaller displays the entitlements. The entitlements are provided along with their corresponding license expiration dates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> If the License Server is not upgraded to the latest License Server version, you get an error message.

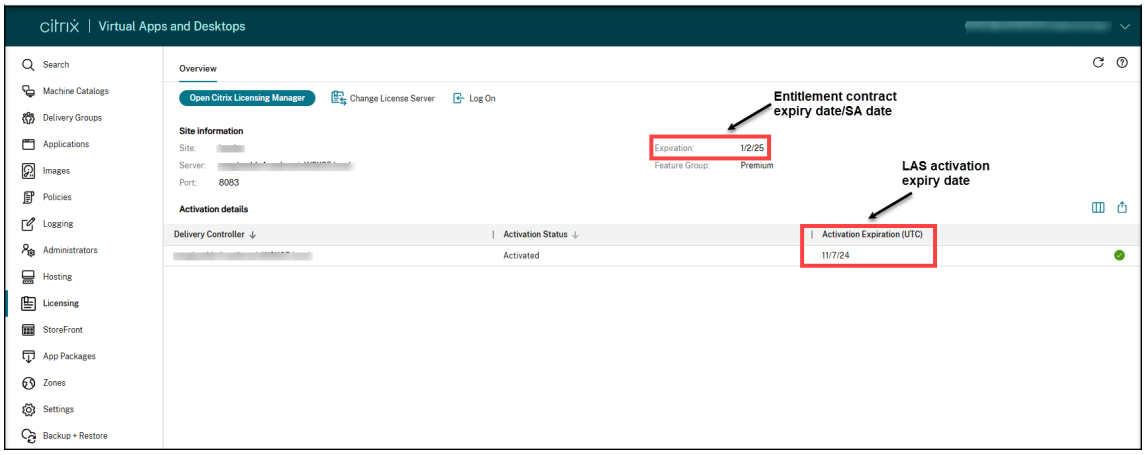
4. Check licensing details.
5. Migrate legacy licensing to LAS.

Check licensing details

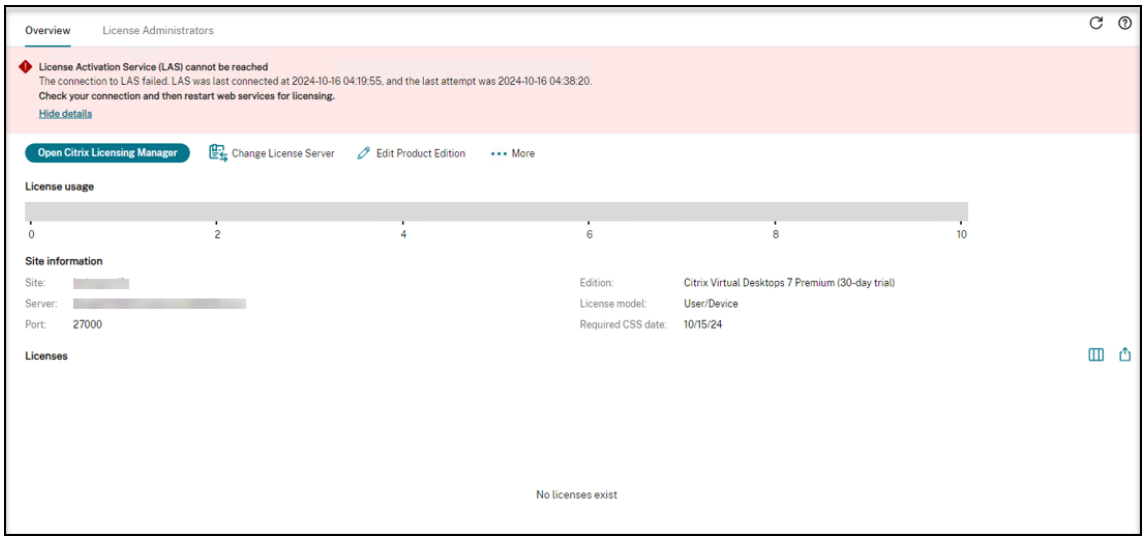
After creating the site, check the licensing details using Web Studio.

1. In Web Studio, select the **Licensing** node.
2. On the **Overview** tab, check if the Citrix Virtual Apps and Desktops site has the appropriate license or if the license has expired while using LAS features.

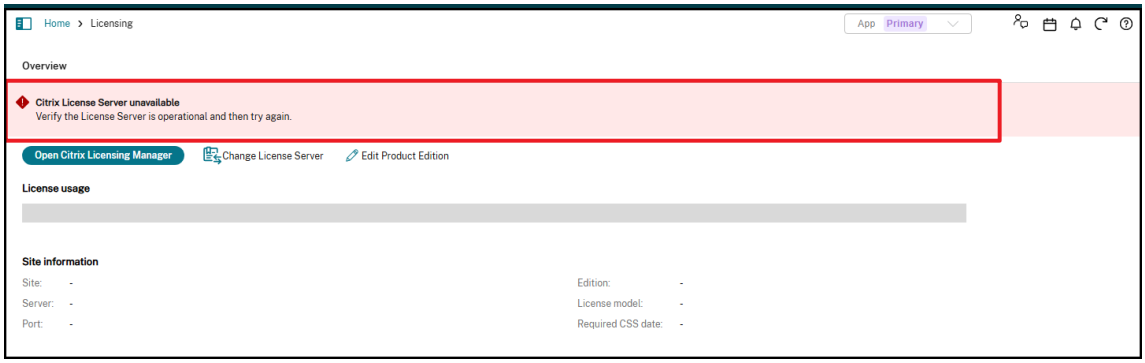
© 1997–2026 Citrix Systems, Inc. All rights reserved.



If the LAS is not reachable, you might see an error message:

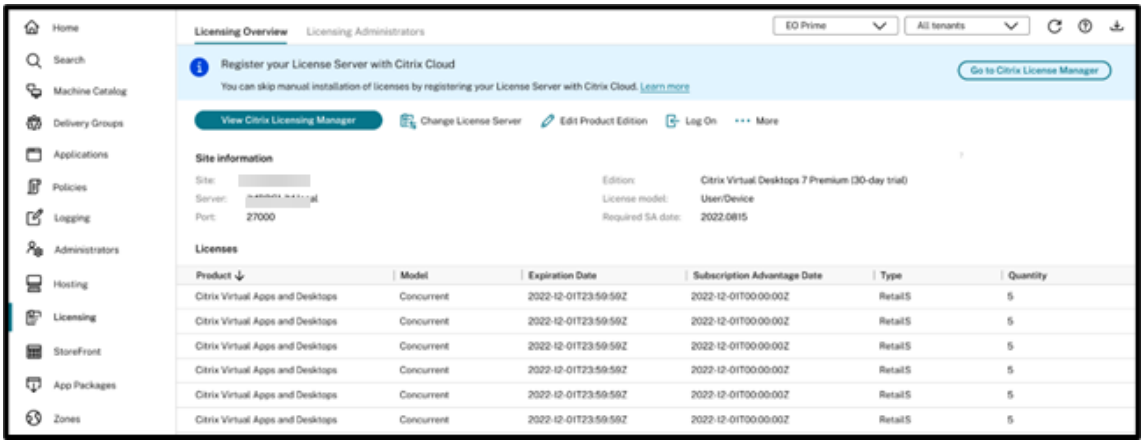


If the License Server is not available, you might see an error message:



If your License Server is still using an old legacy license and the Citrix Virtual Apps and Desktops site is LAS-aware, then the Web Studio prompts you to register your License Server with Citrix Cloud.

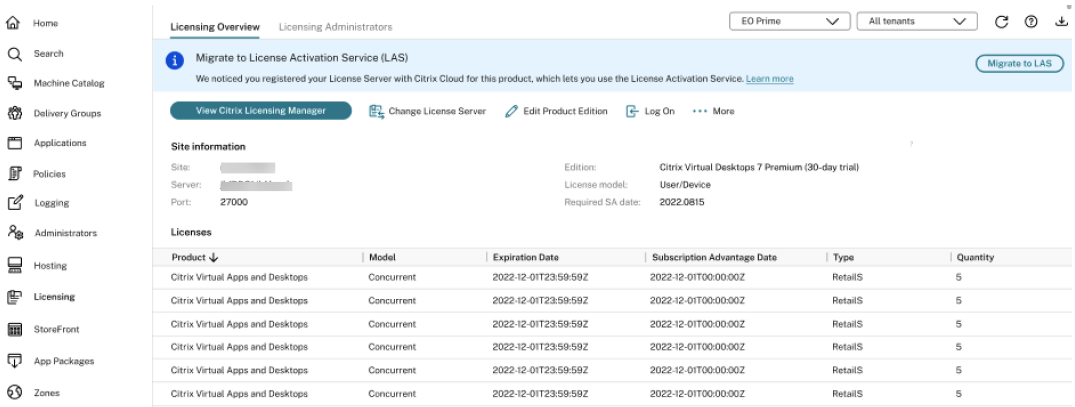
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Migrate legacy licensing to LAS

If you have already registered your License Server with Citrix Cloud and have the necessary entitlement, you must follow the specific sequence below to migrate your existing Citrix Virtual Apps and Desktops site from legacy licensing to LAS without impacting user sessions.

1. **Upgrade License Server:** Upgrade the License Server to the minimum supported version.
2. **Upgrade Delivery Controllers:** Upgrade all the Delivery Controllers in the site to a LAS-supported version.
3. **Remove Delivery Group License Assignments:**
   - Before clicking **Migrate to LAS**, manually remove any license assignments set below the Site level (that is, remove the license assignment in the delivery group level).
4. **Confirm Allocations:** Verify that the LAS allocations are accurate.
5. **Click Migrate to LAS:**
   - Once the previous steps are complete, click **Migrate to LAS**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **License Edition** of the Citrix Virtual Apps and Desktops site is set to **Citrix Virtual Apps and Desktops Premium** and the **License Model** is configured to **Concurrent** once you migrate to LAS.

Roll back from LAS to legacy licensing

Do the following to roll back from LAS to legacy licensing:

1. Run the following PowerShell command.

```
Set-ConfigSite -UseLicenseActivationService $false
```

2. Configure the legacy licenses in Web Studio.

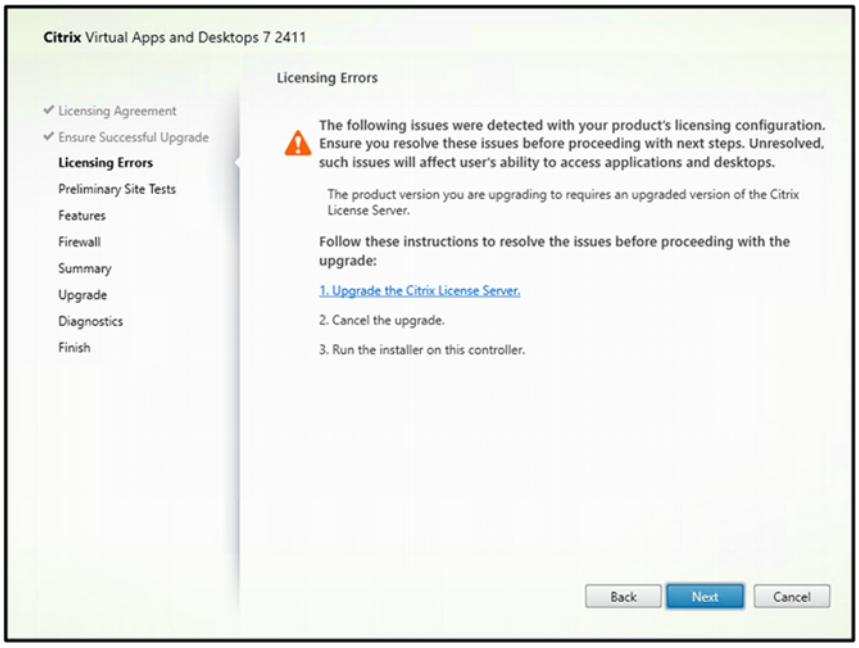
> **Note:**
>
> These steps are provided for temporary troubleshooting only. Legacy license files are approaching End of Life (EOL) and will not function beyond April 15, 2026. To ensure uninterrupted service, we recommend migrating to the License Activation Service (LAS). For details, see the announcement.

Important considerations for upgrade

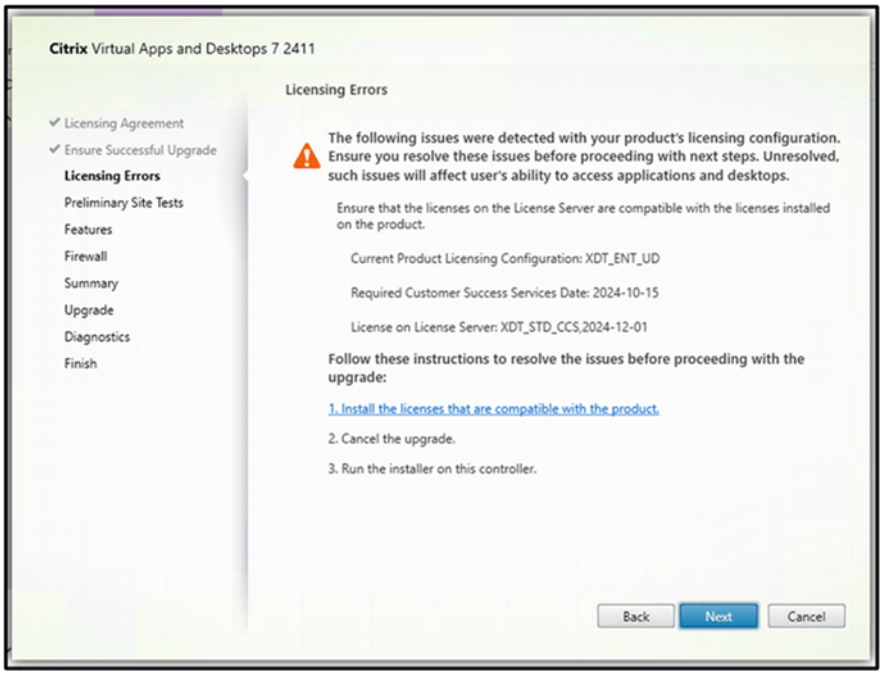
When you upgrade from any earlier Citrix Virtual Apps and Desktops version to 2411 and later, upgrade the License Server to the latest version (version 11.2.17 build 53100 or later).

- You get the following errors on the Licensing Errors page while upgrading using the metainstaller UI:
  - If you do not upgrade to the latest License Server version:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- If there are any incompatibilities, such as an outdated License Server or unavailability of licenses:



- If you are upgrading using the command-line, run the following commands to avoid upgrade failure (assuming you are inside the \x64 folder in the mounted ISO):

1. Run the following:

```
\x64\Licensing\CitrixLicensing.exe /quiet
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you have copied the Licensing binaries to any of the local drives, then run the following command:

```
\x64\Licensing\CitrixLicensing.exe /quiet /l install.log
```

2. Run the following:

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components "
    CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
```

Uninstall core components

During upgrade, if you have installed License Server first using the commands `\x64\Licensing\CitrixLicensing.exe /quiet` or `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` and then installed the core components, then follow the same order to uninstall:

1. Uninstall License Server using the command line:

```
CitrixLicensing.exe /quiet /uninstall /l uninstall.log
```

2. Uninstall components using the GUI or command line. For information, see Remove components.

If you uninstall the License Server and components using the command line `XenDesktopServerSetup.exe` or `removeall`, then clean up the registry entry and the remaining files.

To clean registry entries :

1. Search for the registry key `Citrix Licensing` and delete that entry. Mostly, you can find the entry in the following location:

```
"Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\
    Windows\CurrentVersion\Uninstall\
```

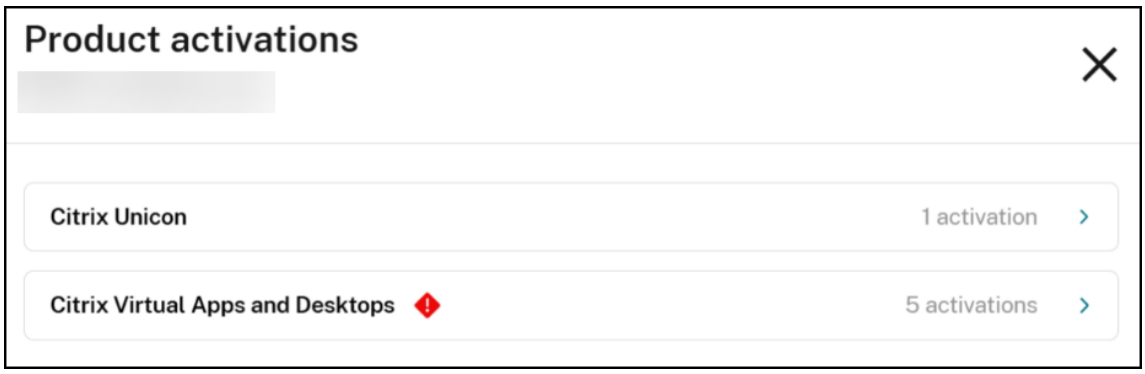
2. Delete the folder pointed by the **Uninstall String** in the registry key.

Troubleshooting

If the status of license server is showing anything other than green in Citrix Cloud, do the following to understand the granular details of the activations that could have issues:

1. In Citrix Cloud, navigate to **Licensing > Licensed deployments > License Servers**.
2. Click the expand button **>** across Citrix Virtual Apps and Desktops to see the list of Delivery Controllers that were activated.

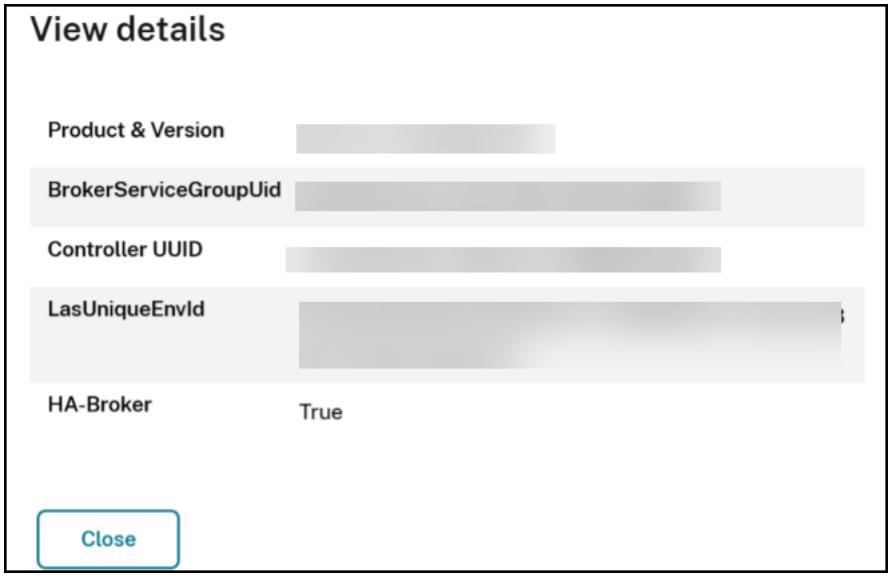
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **View details** across the activation to see the granular details.

   ID is the unique identifier to identify the activations.

   The following details are provided:



   - **Product & Version**: The Product_Edition_Model and the Burn In Date that the product is configured to use when activating with LAS. BurnInDate is usually the release date of the product.
   - **BrokerServiceGroupUid**: The UID for the Broker Service Group.
   - **Controller UUID**: The UUID of the Delivery Controller.
   - **LasUniqueEnvId**: The unique ID of the instance provided by LAS for activation.
   - **HA-Broker**: True or False indicating whether its a HA broker or main broker.

To map the activated host details with the actual host, run the following commands on the host.

- `Get-BrokerSite`: To compare the **BrokerServiceGroupUid** value displayed on the screen with the command's `BrokerServiceGroupId` output.
- `Get-BrokerController`: To compare the **Controller UUID** value displayed on the screen with the command's UUID output.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event viewer logs related to Licensing events

Event ID	Description
1112	The Citrix Broker Service failed to broker a connection for user to resource. The product and edition licensing configuration for the site does not allow this type of resource. Check that the correct license has been selected for this site.
1150	The Citrix Broker Service successfully contacted the license server.
1151	The Citrix Broker Service cannot contact the license server. Ensure that the license server is functioning correctly and that the details identifying the license server are correct in the XenDesktop configuration.
1152	This XenDesktop site does not have the required product licenses present on the license server. Use the License Administration Console to add the relevant product licenses to the license server.
1153	This XenDesktop site's license expired. The Citrix Broker service will request a new license from the license server.
1154	This controller has entered license caching mode because it could not contact the license server. You have 2 hour(s) remaining before this controller stops providing desktop and application sessions.
1155	The Citrix Broker Service will now stop providing desktop and application sessions. This controller is no longer in or could not enter a license caching mode due to sustained failure to communicate with the license server. Ensure that the license server is functioning and, if necessary, use the License Administration Console to add the relevant licenses to the license server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description
1156	The Citrix Broker Service is successfully communicating with the license server. This controller is no longer in license caching mode.
1157	The version of the license server running on is older than the version of the Citrix Broker Service, and is therefore incompatible. Upgrade your license server or specify a license server location with the correct version in your XenDesktop configuration.
1158	The Citrix Broker Service detected that you have exceeded the number of licenses available for this site on the license server for this edition. The license server granted you an overdraft license.
1159	The Citrix Broker Service denied a desktop connection because the maximum number of installed licenses for this site has been exceeded. There are three licenses installed for edition but the maximum allowed number of licenses for this edition is two. Remove the relevant licenses from the license server to comply with the license limit.
1160	The Citrix Broker service encountered an internal error while managing licenses. Ensure that the license server is functioning correctly and that the details identifying the license server are correct in the XenDesktop configuration. Restarting the Citrix Broker service may also resolve the problem. If this problem persists, reinstall the Citrix XenDesktop Controller. See Citrix Knowledge Base article CTX126990.
1161	Error initializing licensing. Check license server connectivity.
1162	Error stopping licensing. Check license server connectivity.
1163	No connection license available. To resolve, free licenses by closing sessions that are not needed, or add more licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description
1164	Error checking out a connection license. Check license server connectivity.
1165	Error checking in a connection license. Check license server connectivity.
1166	Error checking license availability. Check license server connectivity.
1167	Failed to start licensing. Check license server connectivity.
1168	Error reading licensing user notification settings. Check license server connectivity.
1169	This controller has entered the out-of-box license caching mode as no suitable licenses were found on the license server. You have 2 hour(s) remaining before this controller stops providing desktop and application sessions.
1170	The Citrix Broker Service has successfully detected suitable licenses on the license server. This controller is no longer in the out-of-box license caching mode.
1171	No license server has been specified. The Citrix Broker Service cannot provide desktops and applications to users until a valid license server is specified. You can specify a license server in Citrix Studio or with the Citrix PowerShell SDK cmdlet Set-ConfigSite.
1172	Error checking license server suitability. The Citrix broker service received an unexpected response when checking if a machine is suitable for use as a license server. Check that the machine can be contacted from the controller and that any firewall on the machine allows connections from the controller. If a license server is installed on the machine check that it is configured and operating correctly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description
1173	This XenDesktop site does not have the required start up licenses present on the license server. Use the License Administration Console to add the relevant licenses to the license server.
1174	The configured product edition for this XenDesktop site does not support applications; application resources will not be available.
1176	The configured product edition does not support multi-session machines. The registration was rejected.
1177	The configured product edition does not support single-session machines. The registration was rejected.
1178	The configured product edition does not support RemotePC. The registration was rejected.
1179	The configured product edition does not support machines provisioned into a cloud system. The registration was rejected.
1180	The configured product edition for this XenDesktop site does not support applications on single session (workstation OS) machines. Application resource was refused launch.
1181	The configured product edition for this XenDesktop site does not support applications on multi session (server OS) machines. Application resource was refused launch.
1182	The configured product edition for this XenDesktop site does not support desktops on single session (workstation OS) machines. Desktop resource was refused launch.
1183	The configured product edition for this XenDesktop site does not support desktops on multi session (server OS) machine. Desktop resource was refused launch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description
1196	This controller has entered a license burst mode due to exhausting all usable licenses on the license server. Add more licenses to resolve this. You have 2 hour(s) remaining before this controller stops providing desktop and application sessions.
1197	The Citrix Broker Service will now stop providing desktop and application sessions. This controller is no longer in or could not enter a license burst mode due to insufficient licenses on the license server. Use the License Administration Console to add the relevant licenses to the license server.
1198	The Citrix Broker Service is successfully consuming licenses from the license server. There are sufficient licenses on the server to satisfy current demand. This controller is no longer in a license burst mode caused by license exhaustion.
1199	The Citrix Broker Service will now stop providing desktop and application sessions. This controller is no longer in or could not enter a license caching mode since no licenses are installed on the license server. Use the License Administration Console to add the relevant licenses to the license server.
1205	Your software maintenance has expired. Your Citrix environment is currently unsupported. Check your license server for expired licenses and remove them. There is a 30-day license caching mode before users start getting warning messages.
1206	License certificate hash is invalid. Your Citrix License certificate hash is invalid.
1300	The Citrix Broker Service will now stop providing desktop and application sessions. There is a problem with the system clock of the license server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description
1301	Issues with the system clock of license server have been corrected. The Citrix Broker Service will now resume normal operation.
1302	This controller failed checking in or checking out a connection license again. Previously detected failures still exist. To avoid excessive event logging, the service is suppressing related messages (event ID 1163, 1164, 1165) until the problem is resolved. Licensing attempts will continue.
1303	This controller is no longer suppressing related messages (event ID 1163, 1164, 1165).
1304	The Citrix Broker Service successfully contacted LAS.
1305	The Citrix Broker Service cannot contact LAS. Ensure that the LAS is functioning correctly and that the details identifying LAS are correct in the XenDesktop configuration.

More information

For information on checking the LAS state of a site or verify if a site is in license caching mode, see:

- How can I check the LAS state of a site?
- How can I verify if a site is in license caching mode?

For detailed information on the commands, see:

- Get-BrokerController
- Get-ConfigSite

Citrix Virtual Apps and Desktops™ telemetry data elements

March 12, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Broker

Usage

Headers

Key	Description	Example
ver	Indicates the version of the telemetry event.	1
id	Indicates a unique identifier of the usage event.	d4ce7919-5d80-44de-a8fa-102923fe0ead
type	Indicates the event type used by Citrix Analytic Service to identify cloud usage events.	SendBrokerTelemetryData
st	Indicates the timestamp when the event is generated in Broker.	2011-08-12T20:17:46.384Z
prod	Identifies the originating product and deployment of the usage event.	XenDesktop.Broker (Cloud) OnPrem.Broker (OnPrem)
prodVer	Indicates the Citrix DaaS/Citrix Virtual Apps and Desktops product version.	7.25.0.0

Payload

Field	Description	Example
TotalPublishedApps	Indicates the total number of published Apps.	10
TotalPublishedDesktops	Indicates the total number of published Desktops.	10
VDAs.Total	Indicates the total number of VDAs.	10
VDAs.OSTypes	Indicates the total number of VDAs by OS types such as Windows, Linux, and Mac.	10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
VDAs.OSVersions	Indicates the total number of by OS versions such as Windows 10, 11, 2022, 2019.	10
VDAs.HostingLocations.Azure VDAs.HostingLocations.AWS VDAs.HostingLocations.Nutanix VDAs.HostingLocations.VMWare VDAs.HostingLocations.XenServer VDAs.HostingLocations.HyperV	Indicates the number of VDAs for each supported hosting locations such as Azure, AWS, GCP, Nutanix, VMWare, XenServer, and HyperV.	10
VDAs.ProvisionedMethod.MCS	Indicates the number of machines provisioned by Machine Creation Service (MCS).	10
VDAs.ProvisionedMethod.ManualOr3P	Indicates the number of machines manually or 3P provisioned.	10
VDAs.SessionSupport.StaticSingle	Indicates the number of machines statically assigned single session.	10
VDAs.SessionSupport.DynamicSingle	Indicates the number of machines dynamically assigned single session.	10
VDAs.SessionSupport.Multi	Indicates the total number of multi-session machines.	10
VDAs.RemotePCAccess.Windows VDAs.RemotePCAccess.Linux VDAs.RemotePCAccess.MacOS	Indicates the number of Remote PC Access machines by OS type (Win, Mac, Linux).	10
VDAs.ActiveSessionRecordingAgents	Indicates the number of VDAs with active session recording agents.	5
VDAs.Subscriptions	Indicates the number of public cloud subscriptions of VDAs.	2
VDAs.LocationTypes	Indicates the number of location types of VDAs.	2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
AutoScale.DGWithAutoscaleEnabled	Indicates the number of delivery groups with **Autoscale** Enabled.	2
AutoScale.TotalMachinesCtrlByAutoscale	Indicates the number of machines controlled by autoscale.	5
AutoScale.VerticalAutoscaleEnabledByDGandSite	Indicates the number of machines with **Vertical Autoscale** enabled by DG and Site.	2
AutoScale.TaggedBasedAutoscaledDG	Indicates the number of tagged-based autoscaled delivery groups.	2
DeliveryGroup.TotalRebootScheduleEnabled	Indicates the number of delivery groups with **Reboot Schedules** enabled.	2
DeliveryGroup.Total	Indicates the total number of delivery groups.	10
Policy.TotalPolicySets	Indicates the number of policy sets.	3
Policy.TotalPolicies	Indicates the number of group policies.	2
Policy.TotalPolicySettings	Indicates the number of group settings.	2
PublishedPackageApps.AppVSingleAdmin	Indicates the total number of packaged apps published in the AppV Single Admin mode.	2
PublishedPackageApps.AppVDualAdmin	Indicates the total number of packaged apps published in the AppV Dual Admin mode.	2
PublishedPackageApps.Msix	Indicates the total number of packaged apps published in the MSIX mode.	2
PublishedPackageApps.AppAttach	Indicates the total number of packaged apps published in the AppAttach mode.	2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
PublishedPackageApps.FlexApp	Indicates the total number of packaged apps published in the FlexApp mode.	2

Session

Headers

Field	Description	Example
ver	Indicates the version of the license usage event.	1
id	Indicates a unique identifier of the usage event.	d4ce7919-5d80-44de-a8fa-102923fe0ead
type	Indicates the event type used by Citrix Analytic Service to identify cloud usage events.	Cloud.Licensing
st	Indicates the timestamp when the event is generated in Broker.	2011-08-12T20:17:46.384Z
prod	Identifies the originating product and deployment of the usage event.	XenDesktop.Broker (Cloud) OnPrem.Broker (OnPrem)
prodVer	Indicates Citrix DaaS or Citrix Virtual Apps and Desktops product version.	7.25.0.0
user	Identifies the User ID to uniquely identify a user initiating the session launch. **The value is scrambled.**	fullName: C648FE671A44B3F7 **(always scrambled)** samName:C758LH671A44B3F7 **(always scrambled)** upn: C7948FE671A44B3F7 **(always scrambled)** userLicenseId:C265FE671A44B3F7 **(always scrambled)** userSid: C097FE671A44B3F7 **(always scrambled)**
tenant -> id	Indicates the Customer ID of the Citrix Cloud™ account. For the on-premises deployment, this field is not applicable and has no value.	joj1mh0598tj

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
dvc -> dvcId	Indicates the device ID to uniquely identify a device from where the session launch is initiated.	AE18C4D5
dvc -> dvcName	Indicates the friendly name for the device. **The value is scrambled.**	C758LH671A44B3F7 **(always scrambled)**

Payload

Field	Description	Example
appProtectionKeyLoggingRequired	Indicates whether the session is launched with Key Logging Protection enabled.	False
appProtectionScreenCaptureRequired	Indicates whether the session is launched with Screen Capture Protection enabled.	False
cspTenantCustomerId	Indicates the Customer ID of a CSP tenant's Citrix Cloud account. For the on-premises deployment, this field is not applicable and has no value.	6c2vtxgxyftt
isAnonymousUser	Indicates whether an unauthenticated session is launched.	False
licenseActivityTimeStamp	Indicates the timestamp when the payload is generated.	2011-08-12T20:17:46.384Z
licenseActivityType	Indicates the licensing event type. This field indicates if the licensing event type is for assignment or release action.	Connect
licenseModel	Indicates the license model of the deployment.	UserDevice
productEdition	Indicates the product edition of the deployment.	Premium

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
productId	Indicates the product ID of the product in the deployment.	CAVDS
protocol	Indicates the protocol used to launch the session.	HDX™
sessionKey	Indicates a unique identifier for the session.	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	Indicates the session support type.	SingleSession
sessionType	Indicates the session type.	Application
ver	Indicates the payload version.	1.3
workerSid	Indicates a unique identifier for the VDA used for the session.**The value is scrambled.**	1E5LH671A44B3F7 **(always scrambled)**
isWindows365	Denotes if the session is launched for Windows 365.	True
entitlementType	Indicates the Customer's license entitlement type.	Production
siteId	Indicates a unique identifier for the site.	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	Indicates a unique identifier for the Desktop or Delivery Group.	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Indicates the Citrix Workspace™ app type.	Windows
clientVersion	Indicates the Citrix Workspace app version.	23.5.1.83
workerCloudType	Indicates the public cloud type used for VDA provisioning.	Azure
enabledFeatures	Indicates the features that are enabled for the session. For example, in a session where `AppProtectionScreenCaptureRequired` and `SessionRecording` are enabled, the value of this field is 66.	66
launchRequestSource	Records the product that is used to request the launch. It can be either On-prem StoreFront™ or Cloud StoreFront.	0 (StoreFront or 3P)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
		1 (Workspace)
isEvents	Indicates the critical failures in .	Unable to create ST Database.
heartBeatTime	Indicates the License server heart beat time to CIS or Citrix Analytic Service.	1689058813
vdaTelemetry	Indicates the payload that is captured for App Layering, User Personalization Layer, User Profile management, Workspace Environment Management™, and HDX features.	vdaTelemetry SessionTelemetry CPM_feature: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1 CPM_version: 22.3.4000 wem_enableMethod: 1 wem_agentVersion: 2402.1

Studio

Usage

Headers

Field	Description	Example
ver	Indicates the version of the license usage event.	1
id	Indicates a unique identifier of the usage event.	8c2e20a5-ca3f-4401-ad69-d037933c40a0
type	Indicates the event type used by Citrix Analytic Service to identify cloud usage events	Studio.Usage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
st	Indicates the timestamp when the event is generated in Studio.	2024-03-22T01:32:23.4056195Z
prod	Identifies the originating product and deployment of the usage event.	XenDesktop.Studio
prodVer	Indicates the Citrix DaaS/Citrix Virtual Apps and Desktops product version	7.42.0.0

Payload

Field	Description	Example
AdminLoginList	Indicates the list of unique admins SamAccountName. **The value is scrambled.**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw==]}**(always scrambled)**
TotalApiRequests	Indicates the API requests of the Orchestration service.	{TotalApiRequests: 1000}
BackupCount	Indicates the count of backup which operated by Studio admin.	{BackupCount: 200}
RestoreCount	Indicates the count of restore which operated by Studio admin.	{RestoreCount: 20}

Director

Usage report

Headers

Field	Description	Example
ver	Indicates the version of the license usage event.	1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
id	Indicates a unique identifier of the usage event.	8c2e20a5-ca3f-4401-ad69-d037933c40a0
type	Indicates the event type used by Citrix Analytic Service to identify cloud usage events.	Telemetry
st	Indicates the timestamp when the event is generated in Studio.	2024-03-22T01:32:23.4056195Z
prod	Identifies the originating product and deployment of the usage event.	XenApp.Monitor
prodVer	Indicates the Director product version.	7.42.0.0
dvcName	Name of the server	C758LH671A44B3F7

Payload

Field	Description	Example
AdminLoginCount	This is a section of the payload which provides the count of admin logins.	type: AdminLogin stats 0: 1 1: 7
FeatureUsageCount	This section of the payload has the count of big rock features used in Director.	type: FeatureUsage stats 0: 15 1: 20 5: 10
OdataUsageCount	This section of the payload has the count of Odata API usage	type: OData_v3 stats 0: 1 2: 7 5: 9 type: OData_v4 stats 0: 1 2: 8 6: 7

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
AppUsage	Indicates the weekly usage metrics of the published applications.	type: AppUsage headers: application-Name,processName,totalDurationInMinutes period: 01/05/24-07/05/24 values: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]
UniqueAppUsers	Indicates the count of unique users along with total app launches in a month for published applications.	type: UniqueAppUsers headers: application-Name,totalLaunches,totalUniqueUsers period: 04/24 values: [Calc_AWTSVDA-1907R,100,10, Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	Indicates the weekly usage metrics of published desktops.	type: DesktopUsage headers: desktopGroup-Name,sessionSupport,totalDurationInMinute period: 01/05/24-07/05/24 values: [RdsDesktopAndApp-Group,1,10]
UniqueDesktopUsers	Indicates the count of unique users along with total launches in a month for published desktops.	type: UniqueDesktopUsers headers: desktopGroup-Name,totalLaunches,totalUniqueUsers period: 04/24 values: [RdsDesktopAndApp-Group,10,5]
AvgLogonDuration	Indicates the average logon duration.	type: AvgLogonDuration headers: totalUserLogons, avgLogonDurationInSeconds period: 01/05/24-07/05/24 values: [200,4]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
CostSaved	Indicates the cost saved by the customer in a month.	type: CostSaved headers: hypervisor,costSaved,currency period: 04/24 values: [1,221.02,1 2,301.02,2]

Storefront Configuration

Usage

Headers

Field	Description	Example
ver	Indicates the version of the license usage event	1.0
id	Indicates the unique identifier of the usage event	d4ce7919-5d80-44de-a8fa-102923fe0ead
type	Indicates the event type used by CAS to identify cloud usage events	Configuration
st	Indicates the timestamp when the event is generated in StoreFront	2011-08-12T20:17:46.384Z
prod	Identifies the originating product and deployment of the usage event	OnPrem.StoreFront
prodVer	Indicates the StoreFront version (internal)	3.30.0.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Payload

Field	Description	Example
serverName	Indicates the hostname of the service StoreFront is running on	storefront-01.storefront.local
deploymentId	Indicates the unique identifier of the deployment of StoreFront	f47ac10b-58cc-4372-a567-0e02b2c3d479
installedWithCVAD	Indicates whether the StoreFront was installed alongside CVAD	false
cpuCores	Indicates the total number of CPU cores	4
cpuModel	Indicates the CPU running StoreFront	12th Gen Intel(R) Core(TM) i7-1255U 1.70 GHz
ramGb	Indicates the total amount of RAM in GB	16
numServersInGroup	Indicates the number of servers in the server group	3
stores	Indicates the StoreFront Store configuration JSON blob. An array of Store objects. **Some values are scrambled**	Example
rfWebSites	Indicates the StoreFront RFWeb configuration JSON blob. An array of RFWeb Config objects	Example
gateways	Indicates the gateway configuration objects as JSON blob. An array of gateway objects	Example
authServices	Indicates the Auth service configuration objects as JSON blob. An array of auth services objects	Example
IsPiiScrambled		true

Example of field stores

```
[{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 2
 3              "BaseUrl": "baseUrl",
 4              "StorePath": "/",
 5              "EnabledFeatures": 21 bit bitmap,
 6              "ResourceTypeFilteringEnabled": "disabled|Citrix.MPS.
                   Application;Citrix.MPS.Desktop",
 7              "DefaultRfWebSite": "/Citrix/StoreWeb",
 8              "GatewaysUsed": [
 9                  "gatewayId"
10              ],
11              "VdaLogonDataProvider": "",
12              "ResourceFeeds": [
13                  {
14
15                      "FeedName": "<resourceFeedName>|scrambled",
16                      "Type": "CVAD",
17                      "LoadBalancingEnabled": true,
18                   }
19
20              ],
21              "AdvancedAggregation": {
22
23                   "Enabled": true,
24                   "GroupingCount": 1,
25                   "ControllersPushIdenticalResources": true,
26                   "LoadBalanced": true,
27                   "AnyPrimaryFarms": true,
28                   "AnyBackupFarms": true,
29               }
30
31   }
32   ]
```

If no Stores are found, it will be an empty array [].

Example of field rfWebSites

```
1  [{
2
3      "SiteId": "siteId",
4      "BaseUrl": "baseUrl",
5      "StorePath": "storePath",
6      "UiExperienced": 0,
7      "EnabledFeatures": 9 bit,
8      "AuthMethodsEnabled": [
9          "ad"
10     ],
11     "CanUsersDownloadApps": {
12
13         "Enabled": true,
14         "Windows": "exe",
15         "MacOS": "dmg"
16      }
17  ,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "WorkspaceControl": {

        "Enabled": true,
        "LogoffAction": 0,
        "AutoReconnectAtLogon": true,
        "ShowReconnectButton": true,
        "ShowDisconnectButton": true
     }
,
    "MultiClickTimeout": 1,
    "UiViews": [
        "apps",
        "desktops"
    ],
    "DefaultTab": 0,
}
]
```

If no rfWebSites are found, it will be an empty array [].

Example of field gateways

```
[{

            "GatewayId": "gatewayId",
            "IsCloudGateway": true,
            "LoadBalancingSTAEnabled": true,
            "SessionReliabilityEnabled": true,
            "RequestTicketsFromTwoSTA": true,
            "Version": "1234",
            "LogonType": "domain",
            "SmartCardFallbackEnabled": true
}
]
```

If no gateways are found, it will be an empty array [].

Example of field authServices

```
[{

    "SiteId": "SiteId",
    "Store": "StoreAuth",
    "AuthMethodsEnabled": [
        "ad"
    ],
    "PasswordChangeWhenExpired": 0,
    "PasswordRemindersForm": 1,
    "DelegateCredentialValidationToCitrix": true,
    "ValidatePasswordsOnDeliveryControllers": true
}
]
```

If no auth services found, it will be an empty array [].

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Storefront Login

Usage

Headers

Field	Description	Example
ver	Indicates the version of the license usage event	1.0
id	Indicates the unique identifier of the usage event	d4ce7919-5d80-44de-a8fa-102923fe0ead
type	Indicates the event type used by CAS to identify cloud usage events	Login
st	Indicates the timestamp when the event is generated in Broker	2011-08-12T20:17:46.384Z
prod	Identifies the originating product and deployment of the usage event	OnPrem.StoreFront
prodVer	StoreFront version (internal)	3.30.0.0

Payload

Field	Description	Example
user	The user that initiated the launch. **The value is scrambled**	fullName: C648FE671A44B3F7 **(always scrambled)** samName:C758LH671A44B3F7 **(always scrambled)** upn: C7948FE671A44B3F7 **(always scrambled)** userLicenseId:C265FE671A44B3F7 **(always scrambled)** userSid: C097FE671A44B3F7 **(always scrambled)**
serverName	Indicates the hostname of the service StoreFront is running on	storefront-01.storefront.local
loginMethodRfWeb	Indicates the method the user used to login to StoreFront from RFWeb	0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
loginMethodAuth	Indicates the method the user used to login to StoreFront from the Auth service	0
gatewayURL	Indicates the Netscaler Gateway used during login	netscaler-gateway.com
enabledFeatures	Indicates a bitmask of enabled features	12
userAgent	Indicates the UserAgent of the client used to login	CitrixReceiver/22.11.0.19 Linux/5.17.15 X1Class CWACapable CWA/22.11.0.19
baseUrl	Indicates the store that the user login to	storefront-dev.storefront.dev
storePath	Indicates the store that the user login to	/Citirx/StoreWeb
apiUsed	Indicates if the client is using the Store or PNAgent API	0
deviceId	Indicates the device that is used to log into StoreFront. **The values is scrambled**	john-doe
transactionId	Indicates the transaction ID that is sent/generated during a single transaction	773aba9e-5b91-4ef9-8782-c4afb75698e7

Delegated Admin

Usage

Headers

Key	Description	Example
ver	Indicates the version of the license usage event.	1
id	Indicates a unique identifier of the usage event.	8c2e20a5-ca3f-4401-ad69-d037933c40a0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key	Description	Example
type	Indicates the event type used by Citrix Analytic Service to identify cloud usage events.	DelegatedAdmin.Usage
st	Indicates the timestamp when the event is generated in Delegated Admin.	2024-03-22T01:32:23.4056195Z
prod	Identifies the originating product and deployment of the usage event.	XenDesktop.DelegatedAdmin (Cloud) OnPrem.DelegatedAdmin (OnPrem)
prodVer	Indicates the Citrix DaaS or Citrix Virtual Apps and Desktops product version.	7.42.0.0

Payload

Key	Description	Example
TotalCustomScopes	Indicates the number of total custom scopes.	2
TotalCustomRoles	Indicates the number of total custom roles.	4

Scramble licensing telemetry data

Considering the sensitivity of information sent in the license telemetry, Citrix provides you an option to scramble the data.

The following table lists the data that can be scrambled:

Field	Description	Example
user	Identifies the User ID to uniquely identify a user initiating the session launch.	• fullName: C648FE671A44B3F7 • samName: C758LH671A44B3F7 • upn: C7948FE671A44B3F7 • userLicenseId: C265FE671A44B3F7 • userSid: C097FE671A44B3F7

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description	Example
dvc -> dvcName	Indicates the friendly name for the device.	C758LH671A44B3F7
workerSid	Indicates a Unique identifier for the VDA used for the session.	1E5LH671A44B3F7
AdminLoginList	Indicates the list of unique admins SamAccountName	{ AdminLoginList: [UFMJ+ JvXOTHO9mQDsOweiw= =] }
stores	Indicates the StoreFront Store configuration JSON blob. An array of Store objects. **Some values are scrambled**	Example
deviceId	Indicates the device that is used to log into StoreFront.	john-doe

To enable or disable scrambling, run the following PowerShell commands on the Delivery Controller.

> **Note:**
>
> For a Citrix Service Provider™ (CSP) customer, scrambling is always disabled. CSP customers can't enable scrambling using PowerShell commands.

1. Open a PowerShell window from the Delivery Controller host.
2. Run the command `asnp citrix` to load Citrix-specific PowerShell modules.
3. Run the following command to enable or disable scrambling:

   By default, the value is 1, or **`true`**, which enables scrambling of license telemetry data.

   To disable:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData -
       SettingValue $false
   ```

   After you disable scrambling, you can enable it using the following command:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData -
       SettingValue $true
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQ for licensing

April 22, 2026

> **Note:**
>
> - For business continuity resources related to the COVID-19 pandemic, see CTX27055.
> - For general information about maintaining business continuity, see Business continuity — on demand.
> - For more information about the current Citrix License Server, see Licensing.

Citrix® licensing

What is License Activation Service?

The License Activation Service (LAS) is a modern, cloud-based licensing solution for on-premises Citrix License Servers. It offers a streamlined alternative to the traditional, file-based licensing method.

Instead of manually uploading license files, you can connect your license server to the Citrix Cloud™ for online activation. Your entitlements are then delivered to the license server automatically, eliminating the need for license file lifecycle management.

For license servers that can't connect to the cloud, LAS also provides an offline activation option, ensuring flexibility for various network environments. This service introduces a seamless and modern approach to managing your Citrix product licenses.

For more information please refer to License Activation Service.

How can I get my license file?

We send the license access code in an email. There are three ways to generate license files using the license access code:

- The **Manage Licenses** from your MyAccount page on `citrix.com`. For more information, see Manage licenses on citrix.com.
- Web Studio to allocate your purchase and the license file automatically installs on your Citrix License Server.
- Citrix Licensing Manager within the Citrix License Server to allocate your purchase and install your license file. For more information, see Install icenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to allocate license on myaccount?

See Allocate licenses.

How to add allocated licenses to the license server?

See Modify licenses.

What TCP ports does Citrix licensing use?

- License Server port number is 27000
- Vendor daemon port number is 7279
- Web Service for Licensing port is 8083

What is the Citrix License Server?

The Citrix License Server is a system that allows licenses to be shared across the network. For more information, see Licensing operations overview.

Can I virtualize or cluster the Citrix License Server?

Yes. You can virtualize or cluster the Citrix License Server. For more information, see Clustered License Servers.

What benefits are available to me if I virtualize the Citrix License Server?

Virtualizing the Citrix License Server provides a redundant solution. That solution allows for mobility between multiple physical servers without the need for downtime.

Are there any limitations to consider if I virtualize the Citrix License Server?

No.

Does the Citrix License Server manage all the licenses for my Citrix Virtual Apps and Desktops™ deployment?

The Citrix License Server manages all licenses you receive for Citrix Virtual Apps™ and Desktop, except licenses in the Premium Edition used with Citrix Gateway. License servers built in to the network appliances as required for those security-oriented network devices manage those licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What is the Citrix Licensing Manager?

The Citrix Licensing Manager enables downloading and allocation of license files from the License Server on which you installed the Citrix Licensing Manager. The Citrix Licensing Manager is the recommended License Server management method, which enables the following:

- Short code registration of the License Server to Citrix Cloud and easy removal of registration.
- Configure user and group accounts.
- Use the dashboard to display installed, in-use, expired and available licenses, and Customer Success Services dates.
- Export license use data for use in reporting.
- Configure the historical use data retention period. Default data retention period is 180 days.
- Simplified installation of license files on the License Server using a license access code or downloaded file.
- Enable and disable the License burst mode.
- Configure Customer Experience Improvement Program (CEIP) and Call Home.
- Automatically or manually checks for Customer Success Services renewal licenses and notifies you or installs the licenses if found.
- Notifies you of the License Server state - Missing startup license, time issues, uploader failures.
- Modify these ports:
    - License Server (default 27000)
    - Vendor Daemon (default 7279)
    - Web Services for Licensing (default 8083)

For more information, see Citrix Licensing Manager.

Where is the Citrix License Administration Console?

The License Administration Console is no longer supported and was removed from the License Server version 11.16.6. We recommend you use the Citrix Licensing Manager.

You can use Studio to manage and track licensing, provided the License Server is in the same domain as Studio, or in a trusted domain.

For more information, see Citrix Licensing Manager.

What is the license assignment period?

The license assignment period is the term that a Citrix Virtual Apps and Desktops license is assigned to a user or device. The default license assignment period is 90 days.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How do I know how many licenses my organization has purchased?

All purchased licenses are available to review and access at any time (24x7) from your secure **Manage Licenses** toolbox on your **My Account** page on https://www.citrix.com.

How do I know how many licenses are in use at any time?

The Citrix Licensing Manager and Studio provide details on real time license use.

License Server disaster recovery and maintenance

For information about disaster recovery and maintenance of your License Server, see Disaster recovery and maintenance in the Citrix Licensing documentation.

Citrix Virtual Apps and Desktops licensing

How is Citrix Virtual Apps and Desktops licensed?

The Citrix Virtual Apps and Desktops licensing offers user/device and concurrent license models.

User/device:

The flexible user/device model aligns with:

- Enterprise-wide desktop usage.
- Underlying Microsoft desktop virtualization licensing.
- Concurrent licensing for customers with users needing only occasional access to their virtual desktops and apps.

User/device licensing gives users access to their virtual desktops and apps from an unlimited number of devices. Device licenses give an unlimited number of user's access to their virtual desktops and apps from a single device. This approach provides you with maximum flexibility and improves alignment with Microsoft desktop virtualization licensing.

> **Important:**
>
> You can't manually allocate licenses to a user or device. The License Server or cloud service assigns licenses. With user/device licensing, once a license is assigned it can't be assigned to another user until after 90 days of inactivity.

Concurrent:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Concurrent licenses allow one connection to an unlimited number of virtual apps and desktops for any user and any device. A license is consumed only during an active session. If the session disconnects or is terminated, the license is checked back into the pool.

For more information about user/device licensing, see User/device license and concurrent licenses see, Concurrent license.

Is it possible to try Citrix Virtual Apps and Desktops before purchasing licenses?

Yes. You can download the Citrix Virtual Apps and Desktops software and run it in trial mode. Trial mode lets you use Citrix Virtual Apps and Desktops on-premises for 30 days, for 10 connections, without a license. For more information, see Evaluation licenses.

Citrix DaaS™ (formerly Citrix Virtual Apps and Desktops service) for Citrix Cloud is available for trial service based on approval. Check with your Citrix representative for further details.

How does Citrix define concurrency for Citrix Virtual Apps and Desktops?

The Citrix Virtual Apps and Desktops concurrent model allows one connection to an unlimited number of virtual apps and desktops for any user and any device. A license is consumed only during an active session. If the session disconnects or is terminated, the license is checked back into the pool for reissue. For more information, see Concurrent license.

Can I deploy multiple editions of Citrix Virtual Apps and Desktops licenses on a common License Server?

Yes. The License Server manages licenses for both Citrix Virtual Apps and Desktops simultaneously. We recommend that you install the latest License Server version. If you are unsure if your License Server version is current, verify it by comparing your version with the number on the Citrix downloads site.

Can a single site use both Citrix Virtual Apps and Citrix Virtual Apps and Desktops licenses?

Depending on the version, a single Citrix Virtual Apps or Citrix Virtual Apps and Desktops site can support both licensing models - user/device or concurrent. A single Citrix Virtual Apps or Citrix Virtual Apps and Desktops site can support only one edition. For more information, see Multi-type licensing.

The minimum versions that support multi-type licensing are XenApp and XenDesktop 7.15 Long Term Service Release (LTSR) and Citrix Virtual Apps and Desktops 7 1808.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Can I select Citrix Virtual Apps concurrent as a product model if I have Citrix Virtual Apps and Desktops user/device or Citrix Virtual Apps and Desktops concurrent licenses installed on the License Server?

If you use Citrix Virtual Apps as a feature of Citrix Virtual Apps and Desktops Advanced or Premium Edition, your Citrix Virtual Apps license model is the same as your Advanced or Premium Edition of Citrix Virtual Apps and Desktops. If you have purchased Citrix Virtual Apps and Desktops, configure your licensing as Citrix Virtual Apps and Desktops even if you plan to use only the Citrix Virtual Apps functionality. Select Citrix Virtual Apps as a product model only if you have Citrix Virtual Apps concurrent standalone licenses installed on the License Server.

What product components are included with each Citrix Virtual Apps and Citrix Virtual Apps and Desktops edition?

For a full feature matrix by edition, see Citrix Virtual Apps and Desktops features.

How do I license Citrix Virtual Desktops™ environments in compliance with the Citrix Virtual Apps and Desktops EULA?

To deploy Citrix Virtual Apps and Desktops under the user/device or the concurrent license model in compliance with the Citrix Virtual Apps and Desktops EULA, apply the license files to your License Server. The License Server then controls and monitors license compliance. We recommend that you configure your product based on what you purchased. For example, if you purchase Citrix Virtual Apps and Desktops Premium but only want to use the Citrix Virtual Apps feature, configure the product to Citrix Virtual Apps and Desktops to meet compliance. For more information, see the Product License Compliance Center.

How do I license Citrix Virtual Apps environments in compliance with the Citrix Virtual Apps EULA?

To deploy Citrix Virtual Apps under the concurrent license model in compliance with the Citrix Virtual Apps EULA, apply the license files to your License Server. The License Server then controls and monitors license compliance.

Is there a licensing requirement for Citrix Virtual Apps and Desktops Servicing Options: Long Term Service Release (LTSR) or Current Release (CR)?

Citrix Virtual Apps and Desktops Servicing Options, such as Long-Term Service Release, are a benefit of the Customer Success Services program. You must have active Customer Success Services to qualify

© 1997–2026 Citrix Systems, Inc. All rights reserved.

for the benefits of LTSR. For more information, see [Citrix Virtual Apps, Citrix Virtual Apps and Desktops, and XenServer Servicing Options.

How do the Remote Browser Isolation (RBI) Service pooled hours work?

When you purchase a minimum of 25 users of the service, you receive 5000 of hours of rights to use the service, pooled across all users. Subsequent purchases of user rights don't increase the pooled hours entitlement. To increase the entitlement of service hours, buy add-on packs.

Can I use Remote PC Access with CCU licenses?

Yes.

For information about Remote PC Access, see Remote PC Access.

What happens when software maintenance expires for my Citrix environment?

When your Software Maintenance (SWM) or subscription expires, access to software upgrades and technical support is paused. Also, depending on your license type and product version, end users and administrators will receive specific warning notifications indicating that the environment is unsupported.

These notifications are triggered only when all licenses on the server have expired.

End user experience Users will receive a warning message after launching a session. The message states:

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
    environment is currently unsupported. Please contact your IT
    department to resolve.
```

Administrator experience Administrators will see warning alerts within the Citrix Studio console alerting them of the upcoming or active expiration.

Expiration behavior by license type The timing of these messages depends on the license type and the version of Citrix Virtual Apps and Desktops installed.

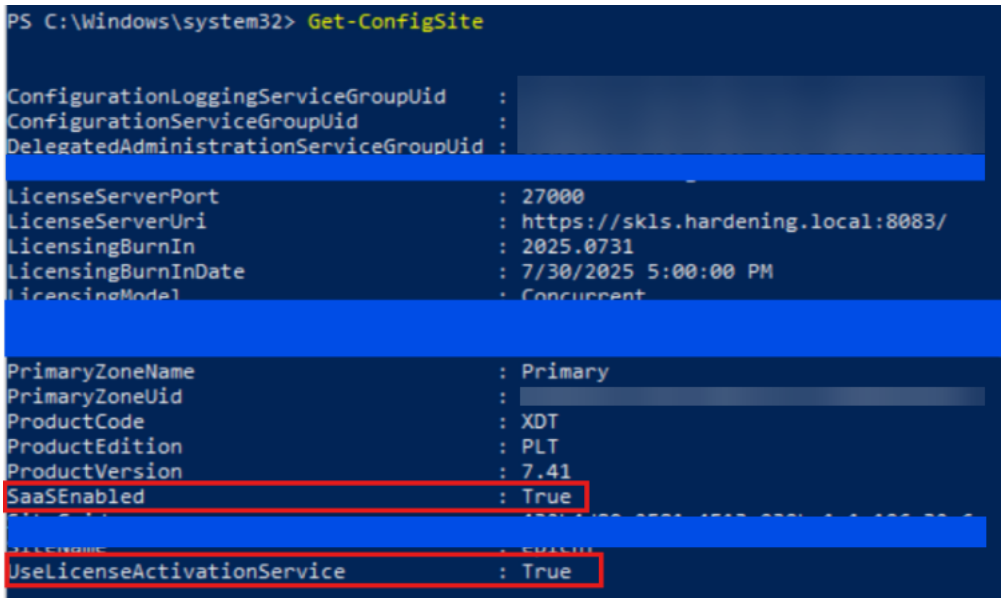
© 1997–2026 Citrix Systems, Inc. All rights reserved.

On-premises subscription licenses

- End User Warning: Appears after the subscription expires, during the grace period.
- Administrator Warning: Appears in Studio 30 days before the subscription expires.
- Supported Versions:
  - Current Release: Citrix Virtual Apps and Desktops 2411 and higher.
  - LTSR: 2203 CU6, and 2402 CU1 and l

How can I check the LAS state of a site?

Run `Get-configsite` to check the LAS activation state and SaaS bit status.

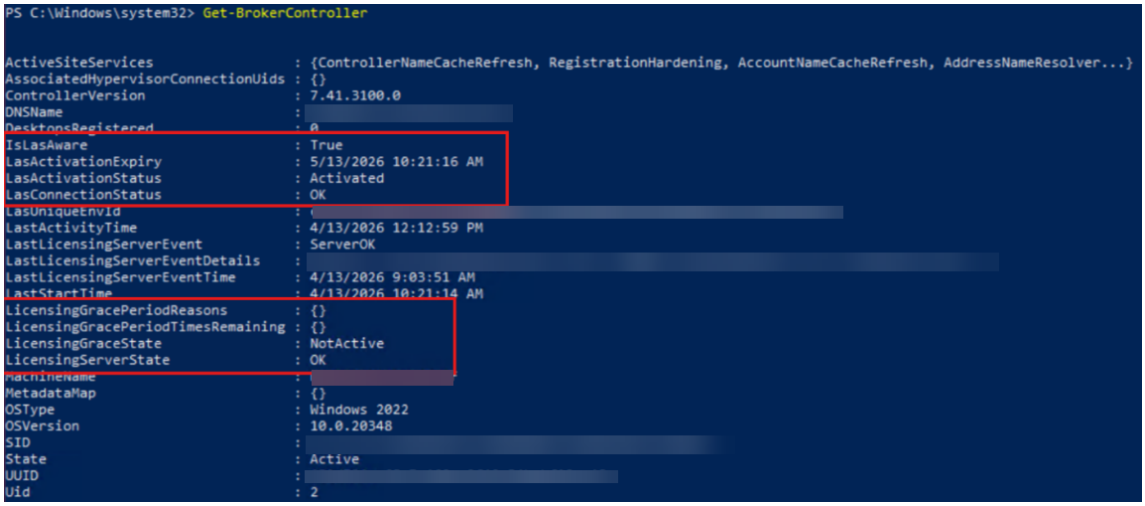


How can I verify if a site is in license caching mode?

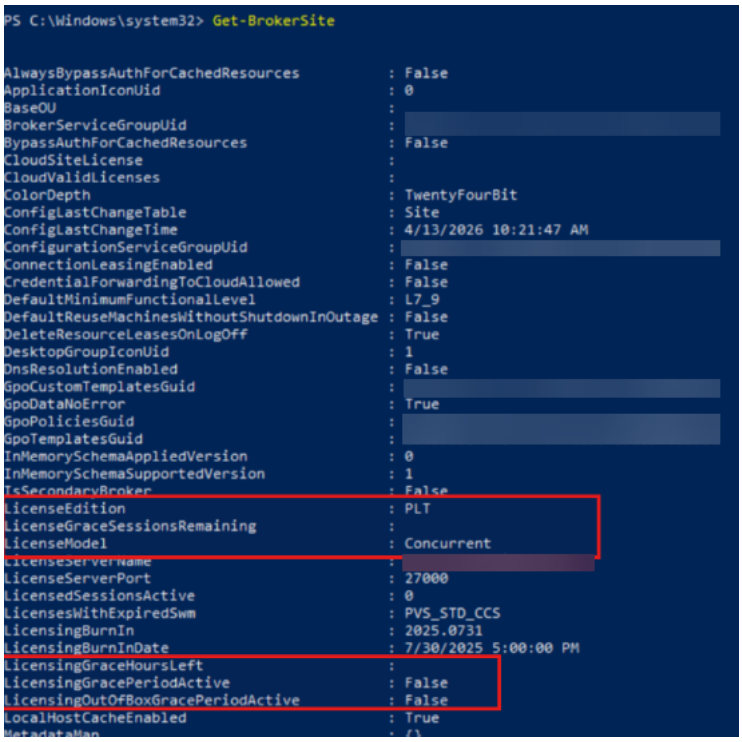
Run `Get-Brokercontroller` and `Get-brokersite` to get details on caching mode and remaining time.

- `Get-Brokercontroller` output:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- `Get-brokersite` output:



For detailed information on the commands, see:

- Get-BrokerController
- Get-ConfigSite

For information on Delivery Controller event viewer logs regarding licensing, see Event viewer logs related to Licensing events.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User or device licenses

How does Citrix allocate licenses to users in the user/device licensing model?

With the user/device license model, the License Server assigns the license to a unique user ID. It allows that single user unlimited connections from unlimited devices. If a user connects to a desktop or device, the user requires one license assigned to that user to access a virtual desktop or application. The License Server or cloud service assigns the license. You can't assign these licenses manually. The license is assigned to the user, not the shared device. Once a license is assigned, it can't be assigned to another user until after 90 days of inactivity. For more information, see User/Device license.

How does Citrix define a licensed device in the user/device licensing model?

A licensed device requires a unique endpoint device ID. Under the user/device model, a device is any piece of equipment that you authorized for use by any individuals to access instances of Citrix Virtual Apps and Desktops. For a shared device, a single Citrix Virtual Apps and Desktops user/device license can support multiple users that share the device. For example, a shared device can be a classroom workstation or a clinical workstation in a hospital.

Can I convert my Citrix Virtual Desktops Standard Edition concurrent licenses to the user/device model?

You cannot convert Citrix Virtual Desktops Standard Edition concurrent licenses to Citrix Virtual Desktops Standard Edition user/device licenses. Similarly, you cannot convert Citrix Virtual Desktops Standard Edition user/device licenses to Citrix Virtual Desktops Standard Edition concurrent licenses.

If you have Citrix Virtual Desktops Standard Edition concurrent licenses and you want the user/device license model, upgrade to either Citrix Virtual Apps and Desktops Advanced or Premium Edition.

From	To Standard concurrent	To Standard user/device	To Advanced user/device	To Premium user/device
Citrix Virtual Desktops Standard Edition concurrent licenses	N/A	Concurrent to user/device conversion NOT allowed	You cannot convert license models, but you can upgrade to Citrix Virtual Apps and Desktops Advanced or Premium Edition.	You cannot convert license models, but you can upgrade to Citrix Virtual Apps and Desktops Advanced or Premium Edition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

From	To Standard concurrent	To Standard user/device	To Advanced user/device	To Premium user/device
Citrix Virtual Desktops Standard Edition user/device licenses	User/device to concurrent conversion NOT allowed	N/A	N/A	N/A

How does concurrent licensing work differently from user/device licensing?

We base concurrent licensing on concurrent device connections. A concurrent license is in use only when a device has established an active connection. Once the connection ends, the concurrent license returns to the license pool for immediate use. We recommend this licensing model for occasional usage. User/device licenses are leased for a period and are not available for other users until the lease expires.

Under the user/device model, can we allocate licenses to both users and devices in the same enterprise?

Yes. Both types can be present in the same enterprise. The License Server optimally assigns licenses to users or devices based on usage. You can't assign these licenses manually.

How do I decide how many users or devices to license?

Assess the use case requirements to determine the appropriate number of licenses. User/device licensing enables unlimited access to unlimited virtual desktops and virtual apps from an unlimited number of devices. Concurrent licensing enables unlimited access to unlimited virtual desktops and virtual apps from a single device that an unlimited number of users can use. Consider the following formula:

```
(Number of total users) – (number of users that only access exclusively
 with shared devices) + (number shared devices) = total number of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the number of
licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Under the user/device model, what is the maximum number of devices a licensed user can use to connect to my environment?

Each licensed user is entitled to use an unlimited number of connected or offline devices.

Under the user/device model, what is the maximum number of users who can access a licensed device?

Each licensed device can service an unlimited number of users within an organization.

Under the user/device model, what is the maximum number of virtual desktops or RBI web applications a licensed user can consume at any given time?

Each licensed user can connect to an unlimited number of virtual desktops or web applications.

Can I purchase Citrix Virtual Apps and Desktops licenses to increase the number of licensed users/devices in my existing Citrix Virtual Apps and Desktops environment?

Yes. You can purchase Citrix Virtual Apps and Desktops licenses to increase the number of licensed users/devices in your existing Citrix Virtual Apps and Desktops environment.

How do I release an authorized user/device license?

To release the assignment of an authorized user/device, use the `udadmin` utility in accordance with the EULA terms. The License Server then assigns the license to the next appropriate user/device. For more information, see Display or release licenses for users or devices.

What happens if I exceed my purchased user/device license count?

User/device licenses include a 10% overdraft, which is included when licenses are generated. The overdraft is also included in the installed license count. If the usage spike exceeds the installed count including overdraft, access for more users is denied. Purchase and deploy a new license to enable access for more users.

If all licenses are in use, including the license overdraft, the License burst mode enables unlimited connections to a product. The License burst mode gives you time to determine why you exceeded the maximum license count and to purchase more licenses without disrupting your users. This period lasts until 15 days elapses or you install more retail licenses, whichever comes first. For more information, see License burst mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director displays the License caching mode states. For more information, see Panels on the Director Dashboard.

What is the maximum number of virtual applications a licensed user can consume at any given time?

Each licensed user can connect to an unlimited number of virtual applications.

What happens if a licensed user leaves my organization?

When an existing licensed user leaves your organization, you can release the departing user's license without notifying Citrix. Use the `udadmin` utility to release the license. If you don't release the license, the License Server automatically releases any license after 90 days of inactivity. This information is subject to the terms specified in the EULA.

What happens if a licensed user is absent for a protracted period?

If an existing licensed user is absent for a protracted period, you can release the license without notifying Citrix, so that it becomes available for reassignment. Use the `udadmin` utility to release the license.

What happens if we replace a licensed device in my organization?

If you replace an existing licensed device, you can release the license without notifying Citrix so that it becomes available for reassignment. Use the `udadmin` utility to release the license.

What happens if a licensed device is out of service for an extended period?

When an existing licensed device is out of service for an extended period, you can release the license without notifying Citrix, so that it becomes available for reassignment. Use the `udadmin` utility to release the licenses. If you don't release the license, the License Server automatically releases any license after 90 days of inactivity. This information is subject to the terms specified in the EULA.

Can I switch user licenses to device licenses and conversely after I've assigned the licenses to a device or user?

Yes. This change happens automatically. The License Server assigns licenses to either users or devices based on usage patterns. If usage patterns change, the License Server might switch the assignment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

based on the new usage. The License Server always assigns licenses in the most economical fashion for the customer. Also, the License Server monitors licenses to identify **unused** licenses after their 90-day assignment period. You can reassign licenses identified as unused after the 90-day assignment period to other users or devices.

Concurrent licenses

Under the concurrent model, what is the maximum number of virtual desktops a Citrix Virtual Apps and Desktops licensed user can consume at any given time?

An endpoint can service many users and allows for unlimited connections.

Can I deploy concurrent licenses from a previous version of Citrix Virtual Apps and Desktops and new user/device or concurrent licenses to a single License Server?

Yes. You can continue to use the same License Server to support user/device or concurrent licensed deployments.

Can I deploy concurrent licenses and user/device or concurrent licenses to a single License Server?

Yes. You can continue to use the same License Server to support concurrent and user/device or concurrent licensed deployments.

Do Citrix Virtual Apps and Desktops Advanced and Premium editions include Citrix Virtual Apps concurrent licenses?

Citrix Virtual Apps and Desktops Advanced and Premium user/device licenses include concurrent Citrix Virtual Apps licenses for compatibility only. These concurrent licenses are for use only with earlier product versions that are incompatible with user/device licenses. Use of the concurrent compatibility licenses included with user/device licenses is permissible only with these versions - XenApp versions earlier than 6.5 and XenDesktop versions earlier than 5.0 Service Pack 1.

What happens if I exceed my purchased concurrent license count?

If all licenses are in use, the License burst mode enables unlimited connections to a product. The License burst mode gives you time to determine why you exceeded the maximum license count and to purchase more licenses without disrupting your users. This period lasts until 15 days elapses or you install more retail licenses, whichever comes first. For more information, see License burst mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director displays the grace period states. For more information, see Panels on the Director Dashboard.

Overdraft licenses

How do I get overdraft licenses?

Products (excluding Citrix Cloud) that support user/device, user, or device license models include a license overdraft feature that enables you to use a limited number of extra licenses to prevent access denial. We offer any overdraft feature as a convenience, not as a license entitlement. Concurrent and server licenses do not contain overdraft. Any overdraft licenses used must be purchased within 30 days of first use, but use is not limited to 30 days. Citrix reserves the right to remove any overdraft feature in new product releases. For more information, see License overdraft.

How can I identify a license overdraft?

You can view usage information, including the number of licenses in overdraft in the Citrix Licensing Manager. Studio also contains overdraft usage information.

What happens when an overdraft license is consumed?

A license is assigned from your installed licenses to enable access to your Citrix Virtual Apps and Desktops environment. This overdraft license provides as much access and functionality as your other licenses.

Can I get an alert when my overdraft licenses are consumed?

Currently, there are no specific alerts provided when overdraft licenses are consumed.

How long can an overdraft license be consumed?

Purchase any overdraft licenses used within 30 days of the first use.

Other product-specific licensing information

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Gateway
- XenServer
- Citrix Licensing

Local Host Cache

September 6, 2025

To ensure that the Citrix Virtual Apps and Desktops site database is always available, Citrix recommends starting with a fault-tolerant SQL Server deployment, by following high availability best practices from Microsoft. (For supported SQL Server high availability features, see Databases.) However, network issues and interruptions can result in users not being able to connect to their applications or desktops.

The Local Host Cache feature allows connection brokering operations in a site to continue when an outage occurs. An outage occurs when the connection between a Delivery Controller™ and the site database fails in an on-premises Citrix® environment. Local Host Cache engages when the site database is inaccessible for 90 seconds.

As of XenApp and XenDesktop 7.16, the connection leasing feature (a predecessor high availability feature in earlier releases) was removed from the product, and is no longer available.

Data content

Local Host Cache includes the following information, which is a subset of the information 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 Receiver™ machines being actively used to connect to published resources.

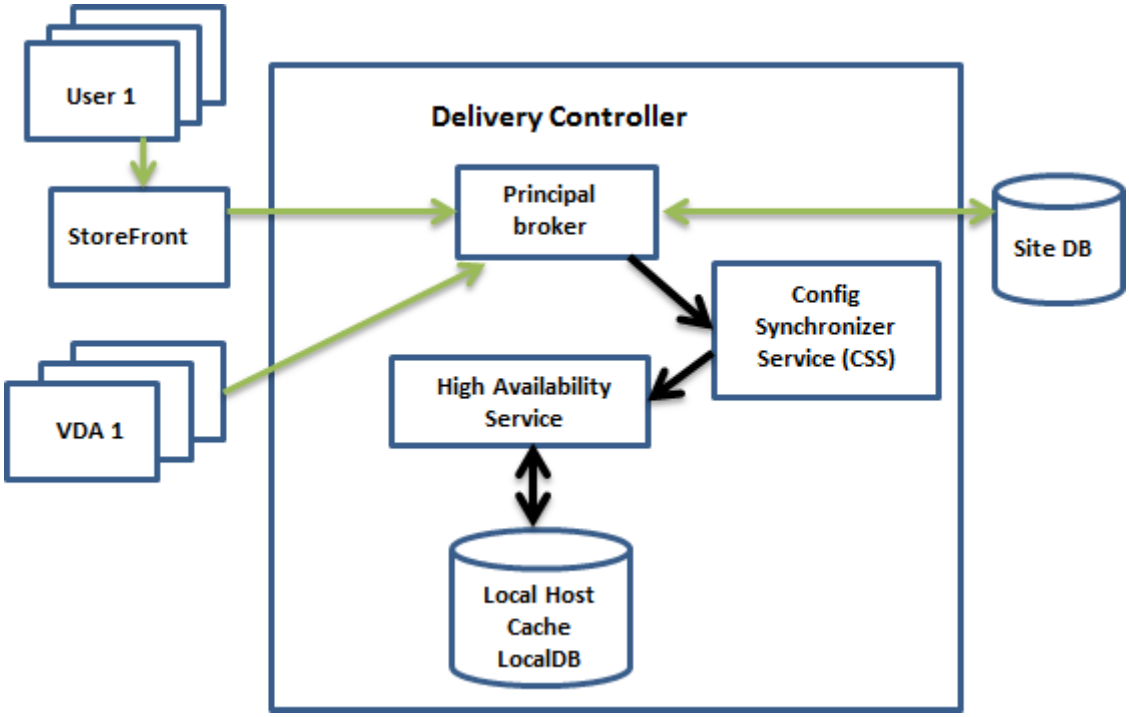
It also contains information for currently active connections that were established while the main database was unavailable:

- Results of any client machine endpoint analysis performed by Citrix Receiver.
- Identities of infrastructure machines (such as NetScaler Gateway and StoreFront™ servers) involved with the site.
- Dates and times and types of recent activity by users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How it works

The following graphic illustrates the Local Host Cache components and communication paths during normal operations.



During normal operations

- The *principal broker* (Citrix Broker Service) on a Controller accepts connection requests from StoreFront. The broker communicates with the site database to connect users with VDAs that are registered with the Controller.
- The Citrix Config Synchronizer Service (CSS) checks with the broker approximately every 5 minutes to see if any changes were made. Those changes can be administrator-initiated (such as changing a delivery group property) or system actions (such as machine assignments).
- If a configuration change occurred since the previous check, the CSS synchronizes (copies) information to a secondary broker on the Controller. (The secondary broker is also known as the High Availability Service.)

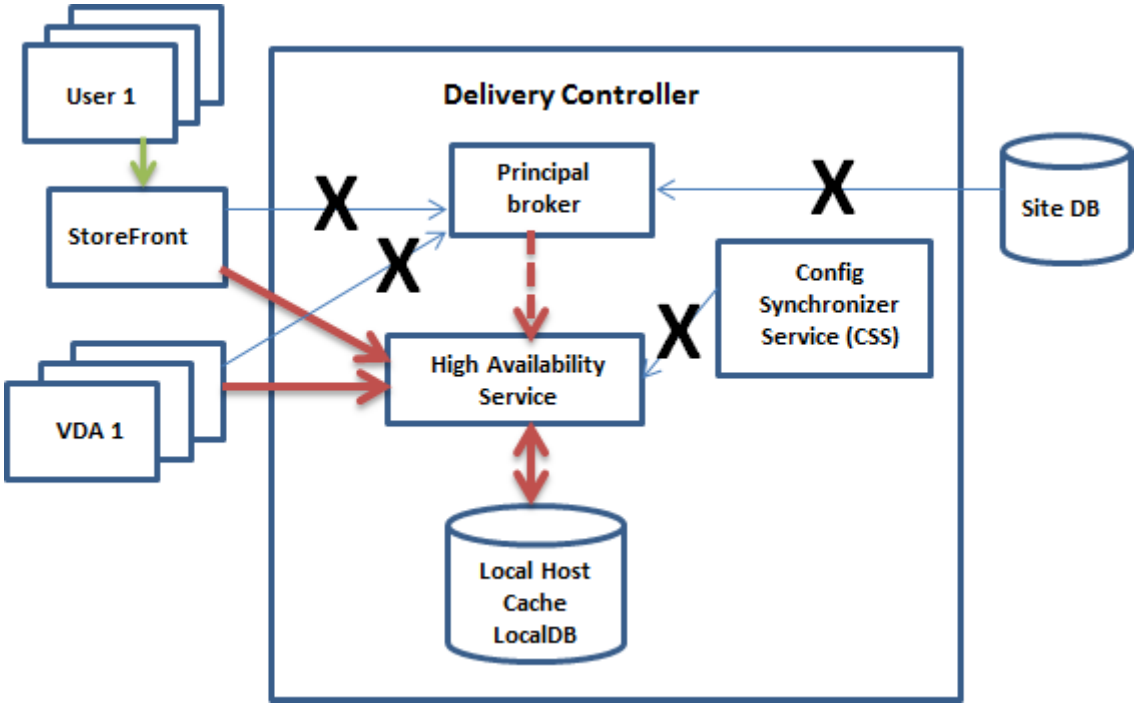
  All configuration data is copied, not just items that changed since the previous check. The CSS imports the configuration data into a Microsoft SQL Server Express LocalDB database on the Controller. This database is referred to as the Local Host Cache database. The CSS ensures that the information in the Local Host Cache database matches the information in the site database. The Local Host Cache database is re-created each time synchronization occurs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft SQL Server Express LocalDB (used by the Local Host Cache database) is installed automatically when you install a Controller. (You can prohibit this installed when installing a Controller from the command line.) The Local Host Cache database cannot be shared across Controllers. You do not need to back up the Local Host Cache database. It is recreated every time a configuration change is detected.

- If no changes have occurred since the last check, no data is copied.

The following graphic illustrates the changes in communications paths if the principal broker loses contact with the site database (an outage begins).



During an outage

When an outage begins:

- The secondary broker starts listening for and processing connection requests.
- When the outage begins, the secondary broker does not have current VDA registration data, but when a VDA communicates with it, a registration process is triggered. During that process, the secondary broker also gets current session information about that VDA.
- While the secondary broker is handling connections, the Brokering Principal continues to monitor the connection. When the connection is restored, the Brokering Principal instructs the secondary broker to stop listening for connection information, and the Brokering Principal resumes brokering operations. The next time a VDA communicates with the Brokering Principal, a registration process is triggered. The secondary broker removes any remaining VDA registrations

© 1997–2026 Citrix Systems, Inc. All rights reserved.

from the previous outage. The CSS resumes synchronizing information when it learns that configuration changes have occurred in the deployment.

In the unlikely event that an outage begins during a synchronization, the current import is discarded and the last known configuration is used.

The event log provides information about synchronizations and outages.

There is no time limit imposed for operating in outage mode.

The transition between normal and outage mode does not affect existing sessions. It affects only the launching of new sessions.

You can also intentionally trigger an outage. See Force an outage for details about why and how to do this.

Sites with multiple Controllers

Among its other tasks, the CSS routinely provides the secondary broker with information about all Controllers in the zone. (If your deployment does not contain multiple zones, this action affects all Controllers in the site.) Having that information, each secondary broker knows about all peer secondary brokers running on other Controllers in the zone.

The secondary brokers communicate with each other on a separate channel. Those brokers use an alphabetical list of FQDN names of the machines they're running on to determine (elect) which secondary broker will be broker operations in the zone if an outage occurs. During the outage, all VDAs register with the elected secondary broker. The non-elected secondary brokers in the zone actively reject incoming connection and VDA registration requests.

If an elected secondary broker fails during an outage, another secondary broker is elected to take over, and VDAs register with the newly elected secondary broker.

During an outage, if a Controller is restarted:

- If that Controller is not the elected broker, the restart has no impact.
- If that Controller is the elected broker, a different Controller is elected, causing VDAs to register. After the restarted Controller powers on, it automatically takes over brokering, which causes VDAs to register again. In this scenario, performance can be affected during the registrations.

If you power off a Controller during normal operations and then power it on during an outage, Local Host Cache cannot be used on that Controller if it is elected as the broker.

The event logs provide information about elections.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What is unavailable during an outage, and other differences

There is no time limit imposed for operating in outage mode. However, Citrix recommends restoring connectivity as quickly as possible.

During an outage:

- You cannot use Studio.
- You have limited access to the PowerShell SDK.
  - You must first:
    - Add a registry key `EnableCssTestMode` with a value of 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    - Use port 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
  - After running those commands, you can access:
    - All `Get-Broker*` cmdlets.
- Hypervisor credentials cannot be obtained from the Host Service. All machines are in the unknown power state, and no power operations can be issued. However, VMs on the host that are powered-on can be used for connection requests.
- An assigned machine can be used only if the assignment occurred during normal operations. New assignments cannot be made during an outage.
- Automatic enrollment and configuration of Remote PC Access machines is not possible. However, machines that were enrolled and configured during normal operation are usable.
- Server-hosted applications and desktop users might use more sessions than their configured session limits, if the resources are in different zones.
- Users can launch applications and desktops only from registered VDAs in the zone containing the currently active/elected secondary broker. Launches across zones (from a secondary broker in one zone to a VDA in a different zone) are not supported during an outage.
- If a site database outage occurs before a scheduled restart begins for VDAs in a delivery group, the restarts begin when the outage ends. This can have unintended results. For more information, see Scheduled restarts delayed due to database outage.
- Zone preference cannot be configured. If configured, preferences are not considered for session launch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tag restrictions where tags are used to designate zones are not supported for session launches. When such tag restrictions are configured, and a StoreFront store's advanced health check option is enabled, sessions might intermittently fail to launch.

Application and desktop support

LHC supports the following types of VDAs and delivery models:

VDA type	Delivery model	VDA availability during LHC events
Multi-session OS	Applications and desktops	Always available.
Single-session OS static (assigned)	Desktops	Always available.
Power-managed single-session OS random (pooled)	Desktops	Not available by default. All session launch attempts to power-managed VDAs in pooled delivery groups will fail by default.

> **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 the LHC event is complete. 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.

pooled machines can cause data and changes from previous user sessions being present in subsequent sessions.

Enable LHC for power-managed single-session OS pooled VDAs using Web Studio

Using Web Studio, you can make those machines available for new connections during LHC events 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 Web Studio only for pooled desktop delivery groups that deliver power-managed VDAs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

RAM size considerations

The LocalDB service can use approximately 1.2 GB of RAM (up to 1 GB for the database cache, plus 200 MB for running SQL Server Express LocalDB). The secondary broker can use up to 1 GB of RAM if an outage lasts for an extended interval with many logons occurring (for example, 12 hours with 10K users). These memory requirements are in addition to the normal RAM requirements for the Controller, so you might need to increase the total amount of RAM capacity.

If you use a SQL Server Express installation for the site database, the server will have two sqlserver.exe processes.

CPU core and socket configuration considerations

A Controller's CPU configuration, particularly the number of cores available to the SQL Server Express LocalDB, directly affects Local Host Cache performance, even more than memory allocation. This CPU overhead is observed only during the outage period when the database is unreachable and the secondary broker is active.

While LocalDB can use multiple cores (up to 4), it's limited to only a single socket. Adding more sockets will not improve the performance (for example, having 4 sockets with 1 core each). Instead, Citrix recommends using multiple sockets with multiple cores. In Citrix testing, a 2x3 (2 sockets, 3 cores) configuration provided better performance than 4x1 and 6x1 configurations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Storage considerations

As users access resources during an outage, the LocalDB grows. For example, during a logon/logoff test running at 10 logons per second, the database grew by 1 MB every 2-3 minutes. When normal operation resumes, the local database is recreated and the space is returned. However, sufficient space must be available on the drive where the LocalDB is installed to allow for the database growth during an outage. Local Host Cache also incurs more I/O during an outage: approximately 3 MB of writes per second, with several hundred thousand reads.

Performance considerations

During an outage, one secondary broker handles all the connections, so in sites (or zones) that load balance among multiple Controllers during normal operations, the elected secondary broker might need to handle many more requests than normal during an outage. Therefore, CPU demands will be higher. Every secondary broker in the site (zone) must be able to handle the additional load imposed by the Local Host Cache database and all the affected VDAs, because the secondary broker elected during an outage can change.

VDI limits:

- In a single-zone VDI deployment, up to 10,000 VDAs can be handled effectively during an outage.
- In a multi-zone VDI deployment, up to 10,000 VDAs in each zone can be handled effectively during an outage, to a maximum of 40,000 VDAs in the site. For example, each of the following sites can be handled effectively during an outage:
  - A site with four zones, each containing 10,000 VDAs.
  - A site with seven zones, one containing 10,000 VDAs, and six containing 5,000 VDAs each.

During an outage, load management within the site can be affected. Load evaluators (and especially, session count rules) can be exceeded.

During the time it takes all VDAs to register with a secondary broker, that service might not have complete information about current sessions. So, a user connection request during that interval can result in a new session being launched, even though reconnection to an existing session was possible. This interval (while the ‘‘new’’secondary broker acquires session information from all VDAs during re-registration) is unavoidable. Sessions that are connected when an outage starts are not impacted during the transition interval, but new sessions and session reconnections might be.

This interval occurs whenever VDAs must register:

- An outage starts: When migrating from a principal broker to a secondary broker.
- Secondary broker failure during an outage: When migrating from a secondary broker that failed to a newly elected secondary broker.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Recovery from an outage: When normal operations resume, and the principal broker resumes control.

You can decrease the interval by lowering the Citrix Broker Protocol's `HeartbeatPeriodMs` registry value (default = 600000 ms, which is 10 minutes). This heartbeat value is double the interval the VDA uses for pings, so the default value results in a ping every 5 minutes.

For example, the following command changes the heartbeat to five minutes (300000 milliseconds), which results in a ping every 2.5 minutes:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

Use caution when changing the heartbeat value. Increasing the frequency results in greater load on the Controllers during both normal and outage modes.

The interval cannot be eliminated entirely, no matter how quickly the VDAs register.

The time it takes to synchronize between secondary brokers increases with the number of objects (such as VDAs, applications, groups). For example, synchronizing 5000 VDAs might take 10 minutes or more to complete.

Differences from XenApp 6.x releases

Although this Local Host Cache implementation shares the name of the Local Host Cache feature in XenApp 6.x and earlier XenApp releases, there are significant improvements. This implementation is more robust and immune to corruption. Maintenance requirements are minimized, such as eliminating the need for periodic `dsmaint` commands. This Local Host Cache is an entirely different implementation technically.

Manage Local Host Cache

For Local Host Cache to work correctly, the PowerShell execution policy on each Controller must be set to RemoteSigned, Unrestricted, or Bypass.

SQL Server Express LocalDB

The Microsoft SQL Server Express LocalDB software that Local Host Cache uses is installed automatically when you install a Controller or upgrade a Controller from a version earlier than 7.9. Only the secondary broker communicates with this database. You cannot use PowerShell cmdlets to change anything about this database. The LocalDB cannot be shared across Controllers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The SQL Server Express LocalDB database software is installed regardless of whether Local Host Cache is enabled.

To prevent its installation, install or upgrade the Controller using the `XenDesktopServerSetup.exe` command, and include the `/exclude "Local Host Cache Storage (LocalDB)"` option. However, keep in mind that the Local Host Cache feature will not work without the database, and you cannot use a different database with the secondary broker.

Installation of this LocalDB database has no effect on whether you install SQL Server Express for use as the site database.

For information about replacing an earlier SQL Server Express LocalDB version with a newer version, see Replace SQL Server Express LocalDB.

Default settings after product installation and upgrade

During a new installation of Citrix Virtual Apps and Desktops (minimum version 7.16), Local Host Cache is enabled.

After an upgrade (to version 7.16 or later), Local Host Cache is enabled if there are fewer than 10,000 VDAs in the entire deployment.

Enable and disable Local Host Cache

- To enable Local Host Cache, enter:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  To determine whether Local Host Cache is enabled, enter `Get-BrokerSite`. Check that the `LocalHostCacheEnabled` property is `True`.

- To disable Local Host Cache, enter:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

Remember: As of XenApp and XenDesktop 7.16, connection leasing (the feature that preceded Local Host Cache beginning with version 7.6) was removed from the product, and is no longer available.

Verify that Local Host Cache is working

To verify that Local Host Cache is set up and working correctly:

- Ensure that synchronization imports complete successfully. Check the event logs.
- Ensure that the SQL Server Express LocalDB database was created on each Delivery Controller. This confirms that the secondary broker can take over, if needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - On the Delivery Controller server, browse to `C:\Windows\ServiceProfiles\NetworkService`.
  - Verify that `HaDatabaseName.mdf` and `HaDatabaseName_log.ldf` are created.

- Force an outage on the Delivery Controllers. After you've verified that Local Host Cache works, remember to place all the Controllers back into normal mode. This can take approximately 15 minutes.

Event logs

Event logs indicate when synchronizations and outages occur. In event viewer logs, outage mode is referred to as *HA mode*.*

Config Synchronizer Service:

During normal operations, the following events can occur when the CSS imports the configuration data into the Local Host Cache database using the Local Host Cache broker.

- 503: The Citrix Config Sync Service received an updated configuration. This event indicates the start of the synchronization process.
- 504: The Citrix Config Sync Service imported an updated configuration. The configuration import completed successfully.
- 505: The Citrix Config Sync Service failed an import. The configuration import did not complete successfully. If a previous successful configuration is available, it is used if an outage occurs. 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 an outage. In this case, see the Troubleshoot section, and contact Citrix Support.
- 507: The Citrix Config Sync Service abandoned an import because the system is in outage mode and the Local Host Cache broker is being used for brokering. The service received a new configuration, but the import was abandoned because an outage occurred. This is expected behavior.
- 510: No Configuration Service configuration data received from primary Configuration Service.
- 517: There was a problem communicating with the primary Broker.
- 518: Config Sync script aborted because the secondary Broker (High Availability Service) is not running.

High Availability Service:

This service is also known as the Local Host Cache broker.

- 3502: An outage occurred and the Local Host Cache broker is performing brokering operations.
- 3503: An outage was resolved and normal operations have resumed.
- 3504: Indicates which Local Host Cache broker is elected, plus other Local Host Cache brokers involved in the election.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 3507: Provides a status update of Local Host Cache every 2 minutes which indicates that Local Host Cache mode is active on the elected broker. Contains a summary of the outage including outage duration, VDA registration, and session information.
- 3508: Announces Local Host Cache is no longer active on the elected broker and normal operations have been restored. Contains a summary of the outage including outage duration, number of machines that registered during the Local Host Cache event, and number of successful launches during the LHC event.
- 3509: Notifies that Local Host Cache is active on the non-elected broker(s). Contains an outage duration every 2 minutes and indicates the elected broker.
- 3510: Announces Local Host Cache is no longer active on the non-elected broker(s). Contains the outage duration and indicates the elected broker.

Force an outage

You might want to deliberately force an outage.

- If your network is going up and down repeatedly. Forcing an outage until the network issues are resolved prevents continuous transition between normal and outage modes (and the resulting frequent VDA registration storms).
- To test a disaster recovery plan.
- To help ensure that Local Host Cache is working correctly.
- While replacing or servicing the site database server.

To force an outage, edit the registry of each server containing a Delivery Controller. In `HKLM\Software\Citrix\DesktopServer\LHC`, create and set `OutageModeForced` as `REG_DWORD` to `1`. This setting instructs the Local Host Cache broker to enter outage mode, regardless of the state of the database. Setting the value to `0` takes the Local Host Cache broker out of outage mode.

To verify events, monitor the `Current_HighAvailabilityService` log file in `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`.

Troubleshoot

Several troubleshooting tools are available when a synchronization import to the Local Host Cache database fails and a 505 event is posted.

CDF tracing: Contains options for the `ConfigSyncServer` and `BrokerLHC` modules. Those options, along with other broker modules, will likely identify the problem.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Report: If a synchronization import fails, you can generate a report. This report stops at the object causing the error. This report feature affects synchronization speed, so Citrix recommends disabling it when not in use.

To enable and produce a CSS trace report, enter the following command:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

The HTML report is posted at `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`.

After the report is generated, enter the following command to disable the reporting feature:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

Export the broker configuration: Provides the exact configuration for debugging purposes.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

For example, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

Local Host Cache PowerShell commands

You can manage Local Host Cache(LHC) on your Delivery Controllers using PowerShell commands.

The PowerShell module is located at the following location on the Delivery Controllers:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Important:**
>
> Run this module only on the Delivery Controllers.

Import PowerShell module To import the module, run the following on your Delivery Controller.

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-
Module .\HighAvailabilityServiceControl.psm1
```

PowerShell commands to manage LHC The following commands help you to activate and manage the LHC mode on the Delivery Controllers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cmdlets	Function
`Enable-LhcForcedOutageMode`	Place the Broker in LHC mode. LHC database files must have been successfully created by the ConfigSync Service for `Enable-LhcForcedOutageMode` to function properly. This cmdlet only forces LHC on the Delivery Controller that it was run on. For LHC to become active, this command must be run on all the Delivery Controllers within the zone.
`Disable-LhcForcedOutageMode`	Takes the Broker out of the LHC mode. This cmdlet only disables LHC mode on the Delivery Controller that it was run on. `Disable-LhcForcedOutageMode` must be run on all the Delivery Controllers within the zone.
`Set-LhcConfigSyncIntervalOverride`	Sets the interval at which the Citrix Config Synchronizer Service (CSS) checks for configuration changes within the site. The time interval can range from 60 seconds(one minute) to 3600 seconds (one hour). This setting only applies to the Delivery Controller on which it was run. For consistency across Delivery Controllers, consider running this cmdlet on each Delivery Controller. For example: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Sets the interval at which the Citrix Config Synchronizer Service (CSS) checks for configuration changes within the site to the default value of 300 seconds (five minutes). This setting only applies to the Delivery Controller on which it was run. For consistency across Delivery Controllers, consider running this cmdlet on each Delivery Controller.
`Enable-LhcHighAvailabilitySDK`	Enables access to all the `Get-Broker*` cmdlets within the Delivery Controller that it was run on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cmdlets	Function
`Disable-LhcHighAvailabilitySDK`	Disables access to the Broker cmdlets within the Delivery Controller that it was run on.

> **Note:**
>
> - Use port 89 when running the `Get-Broker*` cmdlets on the Delivery Controller. For example:
>   - `Get-BrokerMachine -AdminAddress localhost:89`
> - When not in LHC mode, the LHC Broker on the Delivery Controller only holds configuration information.
> - During LHC mode, the LHC Broker on the elected Delivery Controller holds the following information:
>   - Resource states
>   - Session details
>   - VDA registrations
>   - Configuration information

Monitor and manage machines and sessions using Search

September 6, 2025

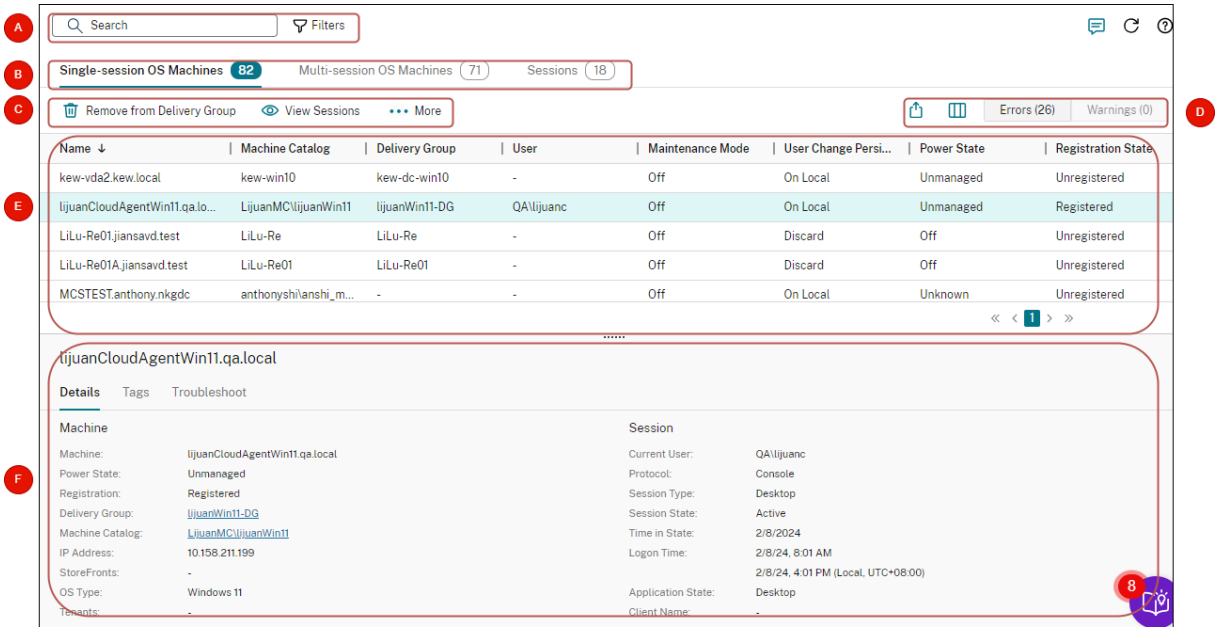
> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

This article guides you through how to monitor and manage machines and sessions using the **Search** node in Web Studio.

Learn about the node

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.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Callout	Area	Description
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 causes, and suggested solutions

Search for instances

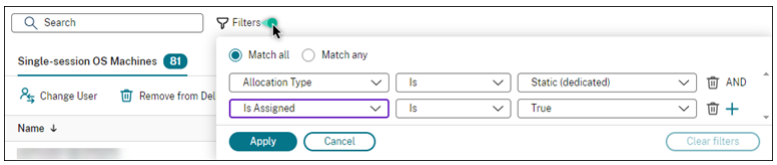
Use the search function to locate specific machines and sessions:

- 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.

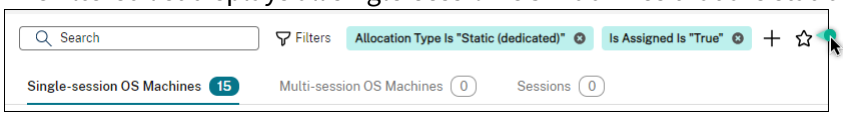


3. Select **Match all** (AND operator) if you want the search to return results that match all filter criteria. Select **Match any** (OR operator) if you want the search to return results that match any of the filter criteria.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Apply**.

   The filtered list displays all single-session OS machines that are static and assigned to users.

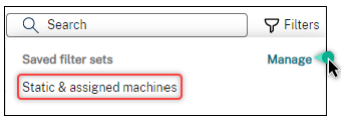


Save the current filter set for a quick search

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.

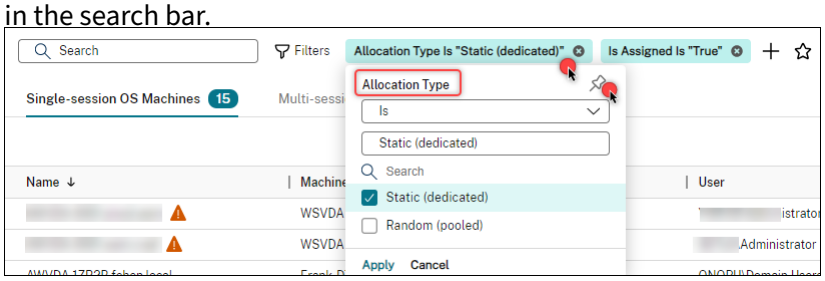


> **Note:**
>
> Filter sets are saved on a per user account basis. To manage saved filter sets, select **Manage**.

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.

- 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

   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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

September 6, 2025

This article lists machine actions and columns with descriptions for your reference.

Actions

View the actions you can perform on machines and their descriptions.

Action	Description	Applies to
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Action	Description	Applies to
	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.	
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, Delivery Controllers store the memory contents of the machine in a file and then shuts down the machine.	Single-session OS machines
Resume	Resume a suspended machine. When you resume a suspended machine, Delivery Controllers start the machine and restores it to the previous state.	Single-session OS machines

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Action	Description	Applies to
Force Restart	Force restart a machine.	Single-session OS machines
Force Shut Down	Force shut down a machine.	Single-session OS machines

Columns

View all machine columns and their descriptions by type:

- Machine
- Machine details
- Applications
- Hosting
- Connection
- Registration
- Session Details
- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
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
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: **Permanent**, when allocated to a user permanently. **Random**, when allocated randomly.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
Maintenance Mode	Indicates whether the machine is in maintenance mode.	Single-session and multi-session
Windows Connection Setting	Logon mode reported by Windows. Possible values: LogonEnabled, Draining, DrainingUntilRestart, and LogonDisabled.	Multi-session only
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 Delivery Controllers. `False` indicates otherwise.	Single-session and multi-session
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 unavailable for new sessions. In Progress: Actively undergoing a scheduled reboot. Natural: Natural reboot in progress. The machine is awaiting a restart.	Single-session and multi-session
Zone	The name of the zone where the machine is located.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
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. Possible states: Off, Unregistered, Available, Disconnected, InUse, and Preparing.	Single-session and multi-session
Tags	The list of tags associated with the machine.	Single-session and multi-session
VDA Upgrade	The machine state for VDA package upgrade actions. Possible values: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate, and 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 overall effective load index (percentage) for the machine. For more information, see CTX202150.	Multi-session only
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
	Note: The machine doesn't shut down if it's in maintenance mode. It shuts down only after it's off maintenance mode.	

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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
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
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
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.

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. Discard: Non-persistent. User changes are discarded.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
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

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.	Single-session and multi-session

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
	Possible values are: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description	Applies to
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 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.	Single-session and multi-session

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 session. Always null for multi-session machines.	Single-session and multi-session
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

September 6, 2025

This article lists machine actions and columns with descriptions for your reference.

Actions

View the actions you can perform on sessions and their descriptions.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Action	Description	Applies to sessions on
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 Delivery Controllers.	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

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) 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description
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.
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 Delivery Controllers. `False` indicates otherwise.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description
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: 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.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description
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.

Manage security keys

September 13, 2025

> **Important:**
>
> - You must use this feature in combination with StoreFront™ 1912 LTSR CU2 or later.
> - The Secure XML feature is only supported on Citrix ADC and Citrix Gateway release 12.1 and later.
>
> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

This feature lets you allow only approved StoreFront and Citrix Gateway machines to communicate with 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. Enable Web Studio to show the feature settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

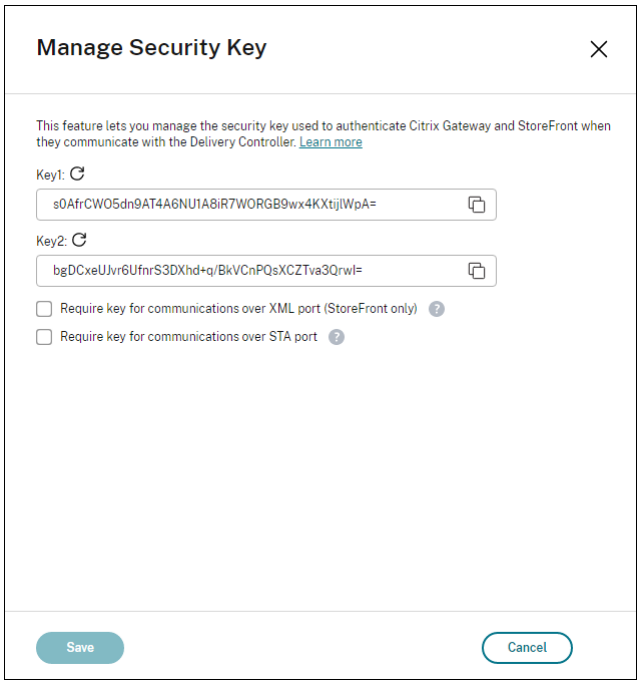
2. Configure settings for your site.
3. Configure settings for StoreFront.
4. Configure settings for Citrix ADC.

Configure settings for the site

You can use Web Studio or PowerShell to configure security key settings for your site.

Use Web Studio

1. Sign in to Web Studio, select **Settings** in the left pane.
2. Locate the **Manage security key** tile and click **Edit**. The **Manage Security Key** page appears.



3. Click the refresh icon to generate the keys.

> **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.

4. Select where a key is required for communications:

© 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.

5. Click **Save** to apply your changes and close the window.

Use PowerShell

The following are PowerShell steps equivalent to Web Studio operations.

1. Run the Citrix Virtual Apps and Desktops 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 for StoreFront

After completing the configuration for your site, you need to configure relevant settings for 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	https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/Set-STFStoreFarm.html]. 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`
- `STA URL`
- `Secret`

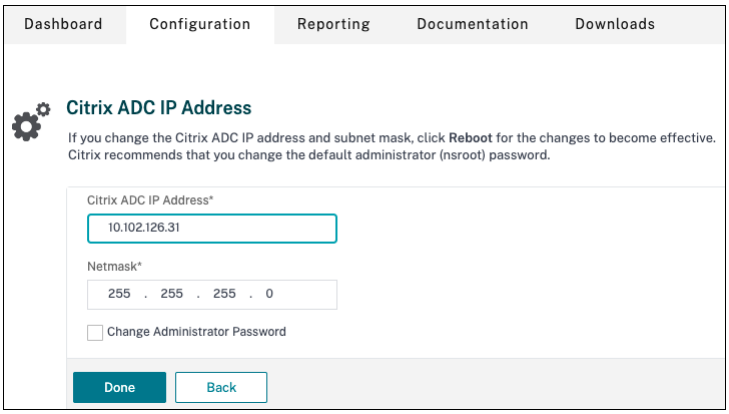
See the PowerShell command help for guidance and syntax.

Configure settings for Citrix ADC

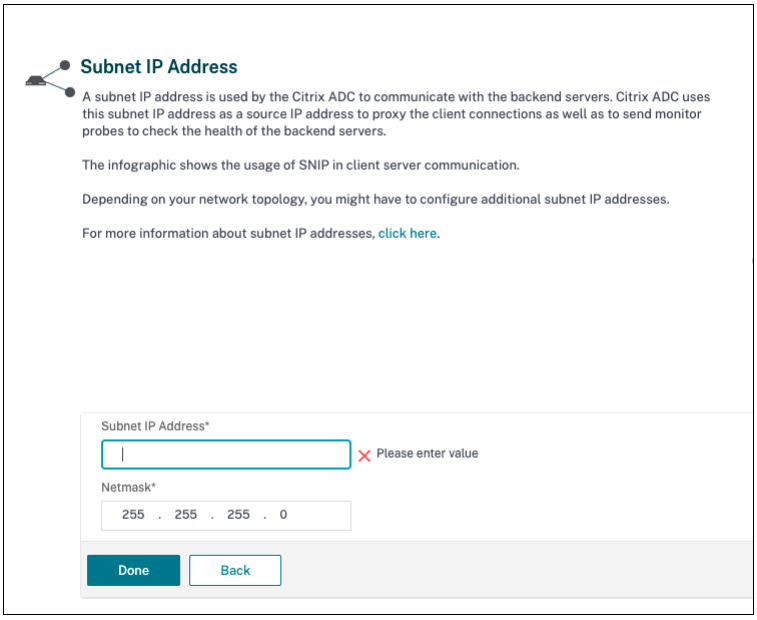
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Configuring this feature for Citrix ADC is not required unless you use Citrix ADC as your gateway. If you use Citrix ADC, follow these steps:

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.

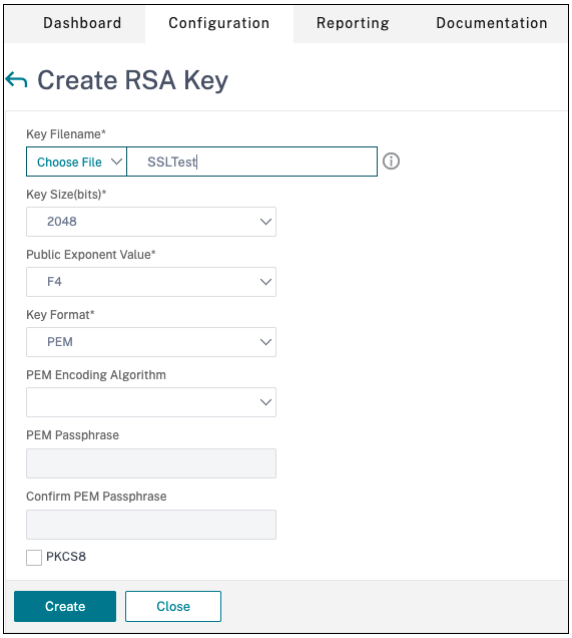


    - The required modes and features in the Citrix ADC appliance are enabled.

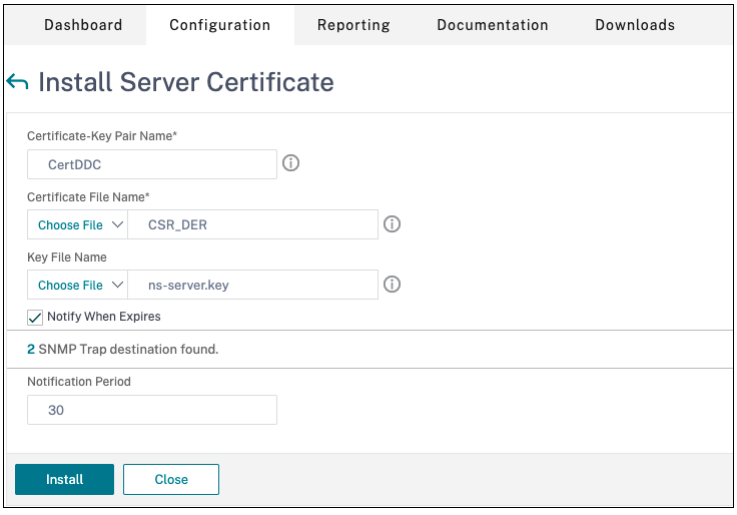
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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**.

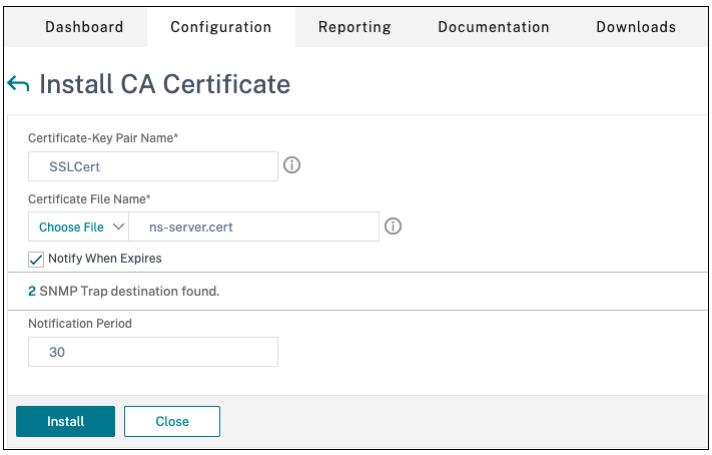
- Certificates related configurations are complete.
  - The Certificate Signing Request (CSR) is created. For details, see Create a certificate.



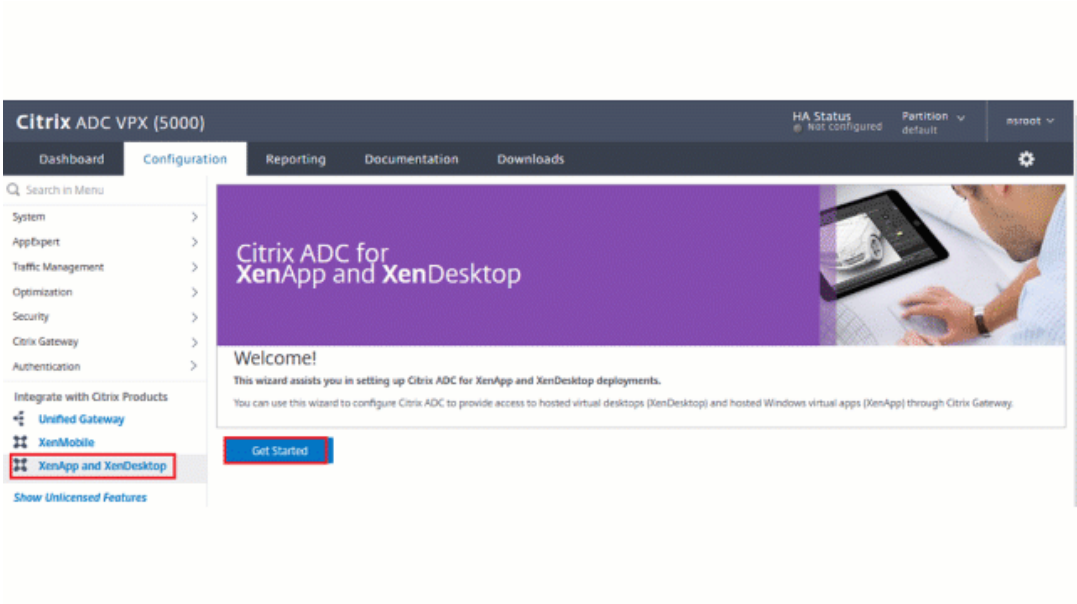
  - The server and CA certificates and root certificates are installed. For details, see Install, link, and updates.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



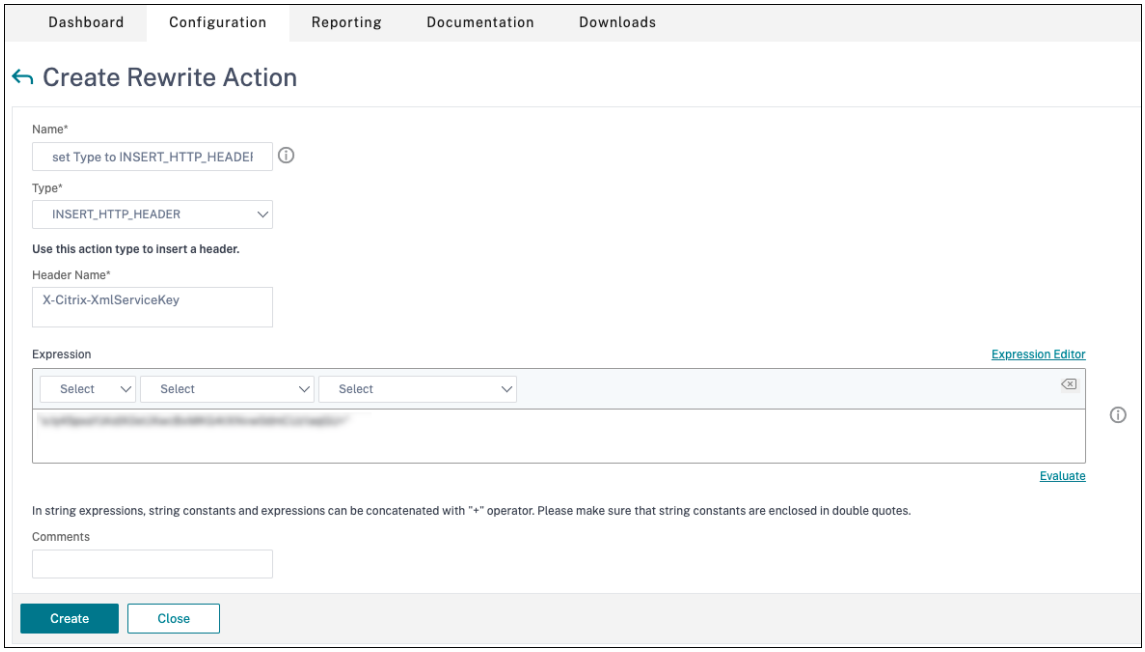
- A Citrix Gateway has been created for Citrix Virtual Desktops. Test the connectivity by clicking the **Test STA Connectivity** button to confirm that the virtual servers are online. For details, see Setting up Citrix ADC for Citrix Virtual Apps and Desktops.



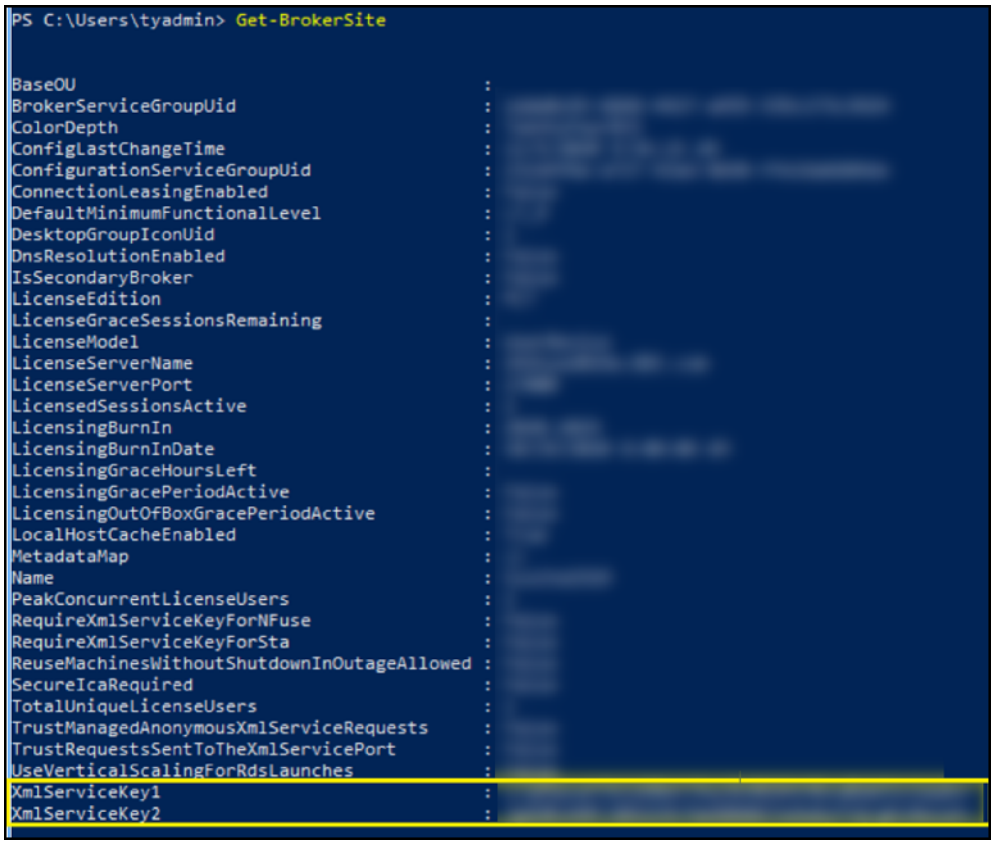
2. Add a rewrite action. For details, see Configuring a Rewrite Action.

   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".

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

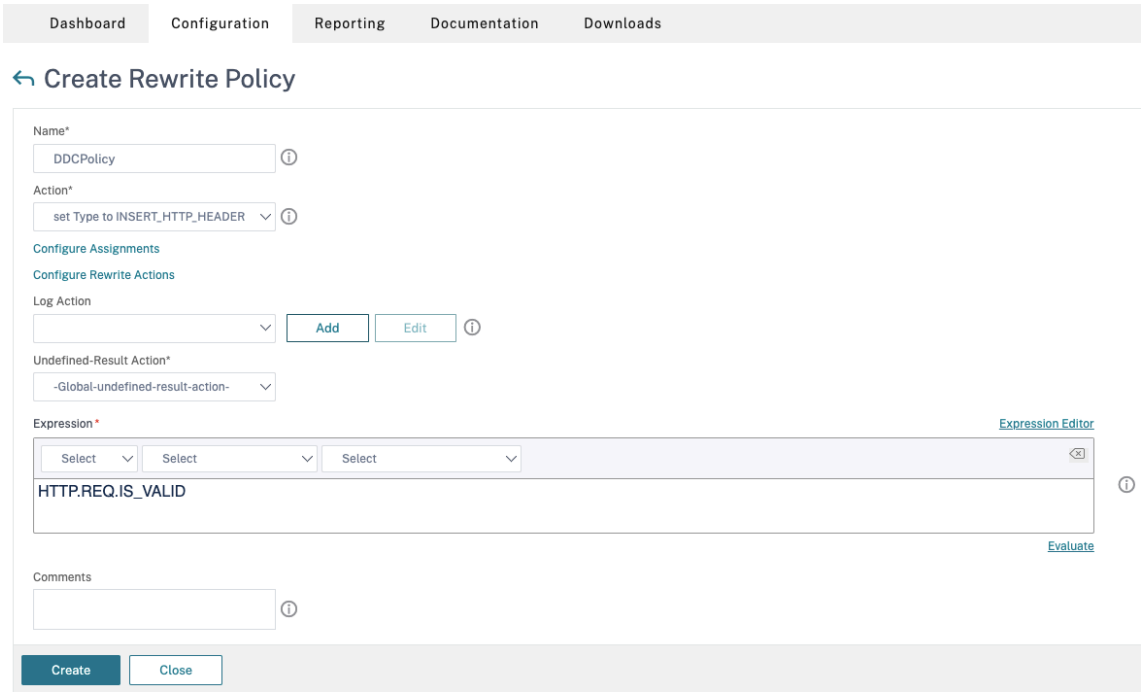


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



   a) In **Action**, select the action created in the earlier step.
   b) In **Expression**, add HTTP.REQ.IS_VALID.
   c) Click **OK**.

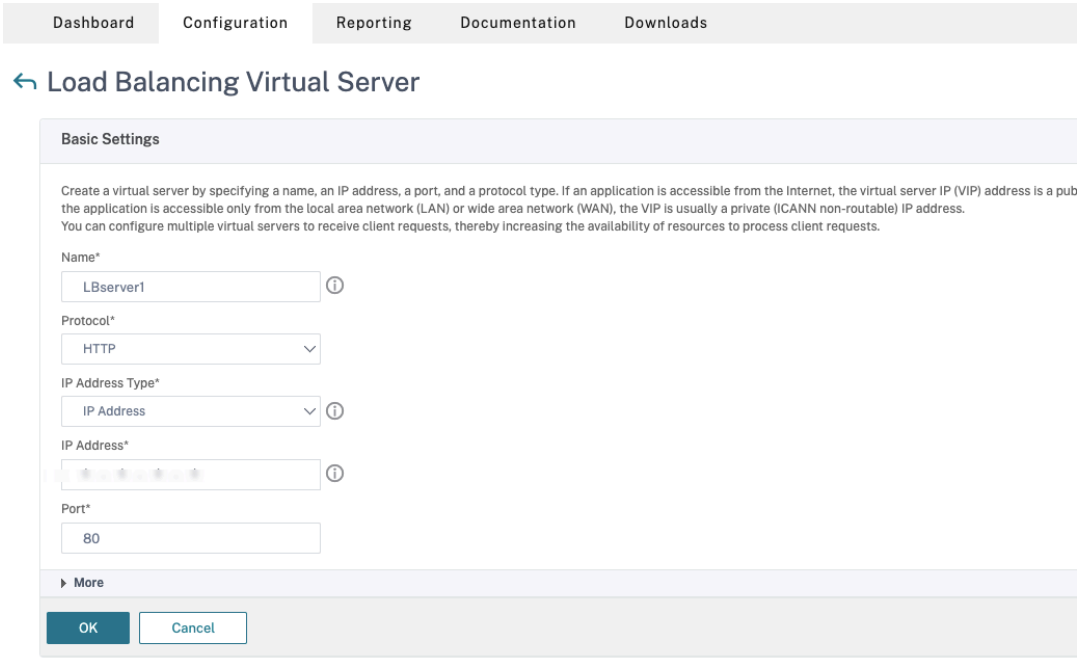
4. Set up load balancing. You must configure one load balancing virtual server per STA server. If not the sessions fail to launch.

   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**.

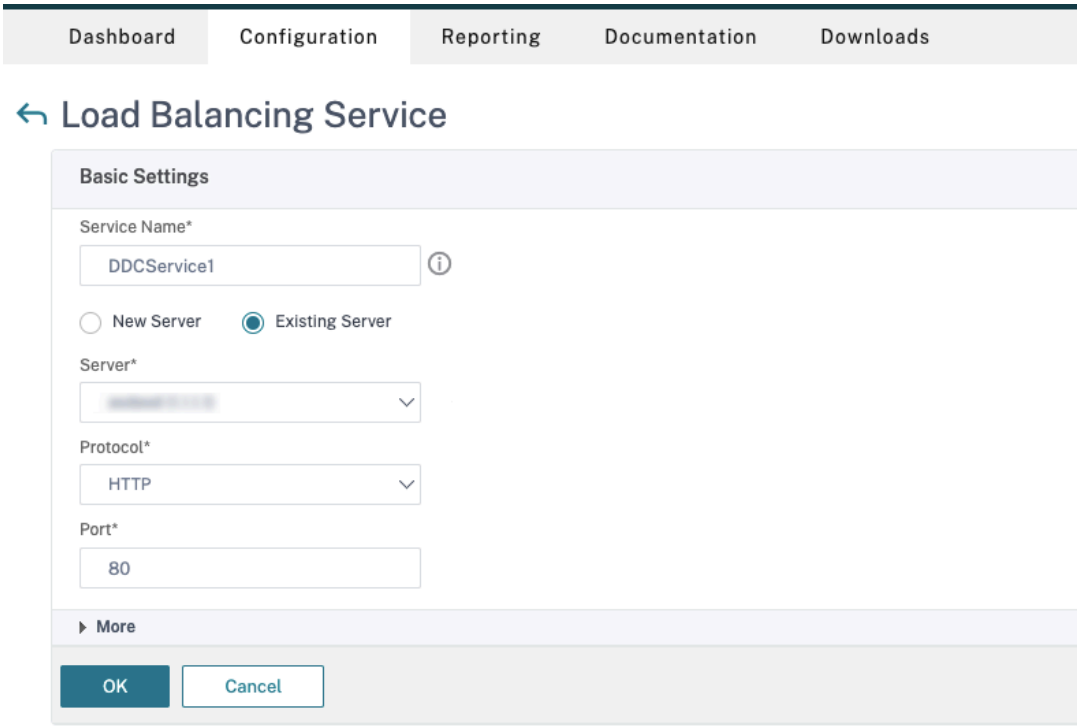
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 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**.

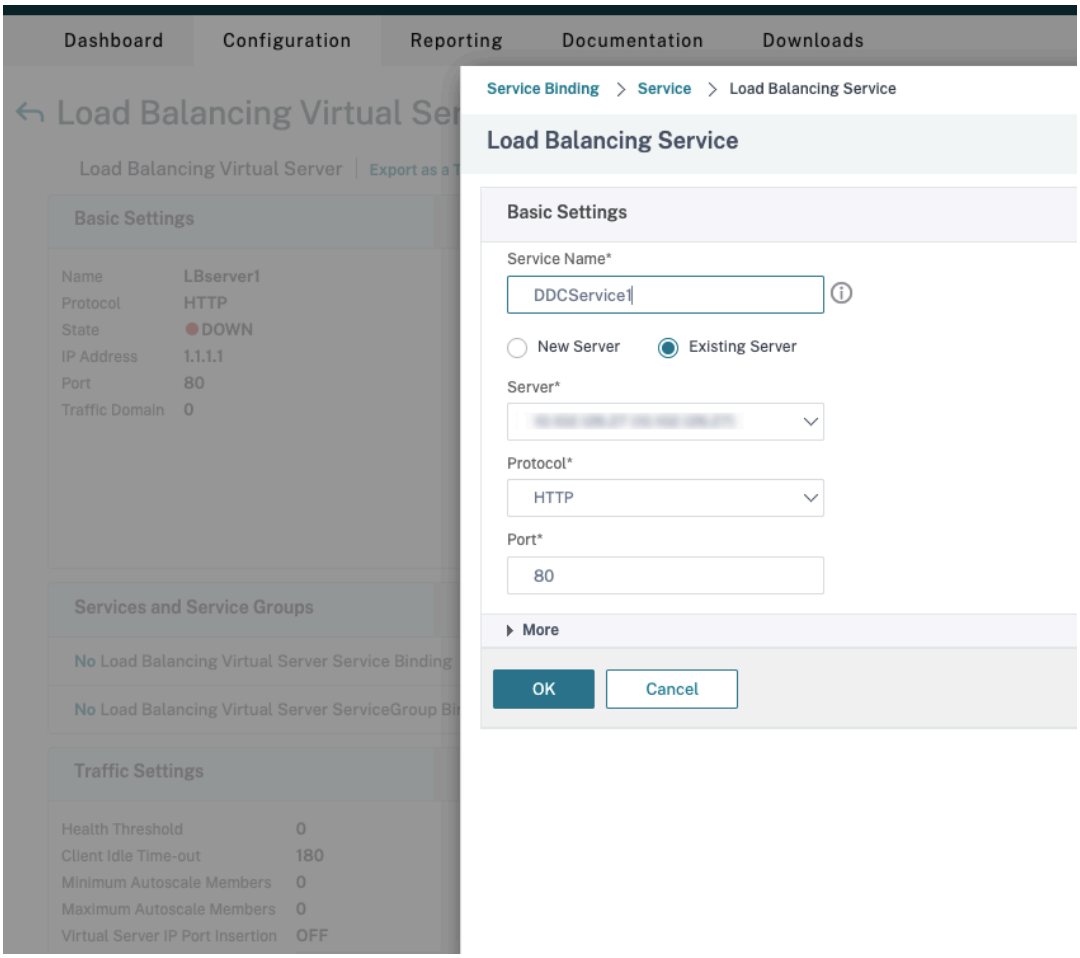


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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**.

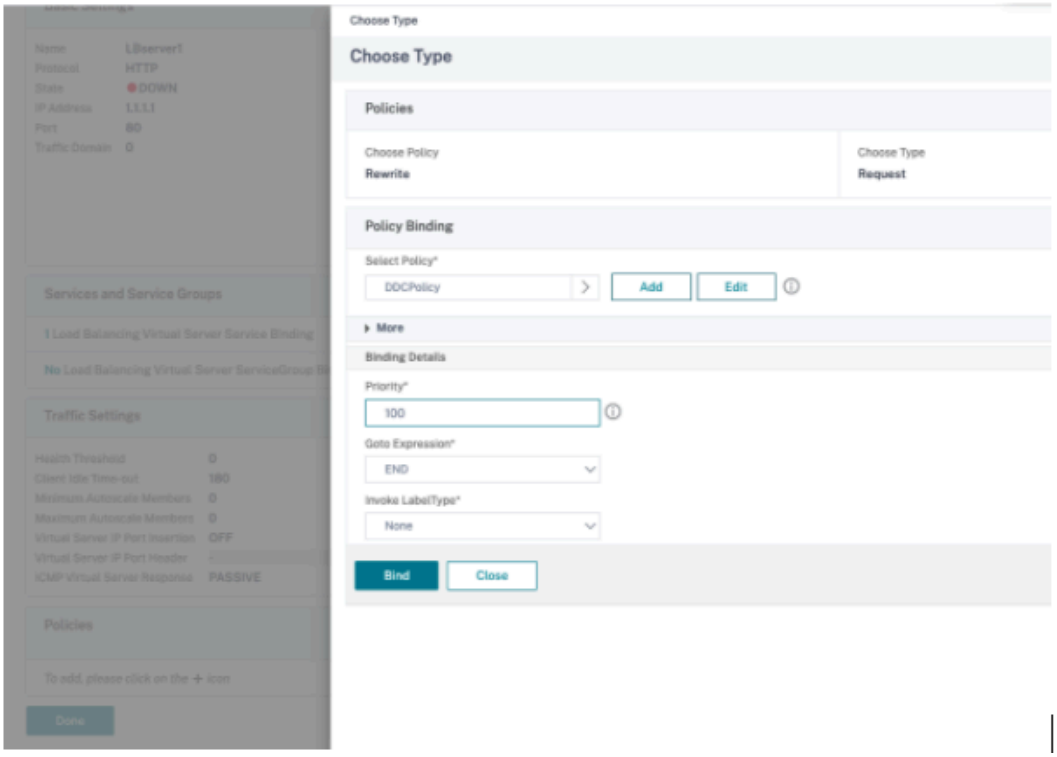


- In **Service Binding**, select the service created earlier.
- Click **Bind**.

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 **+**.

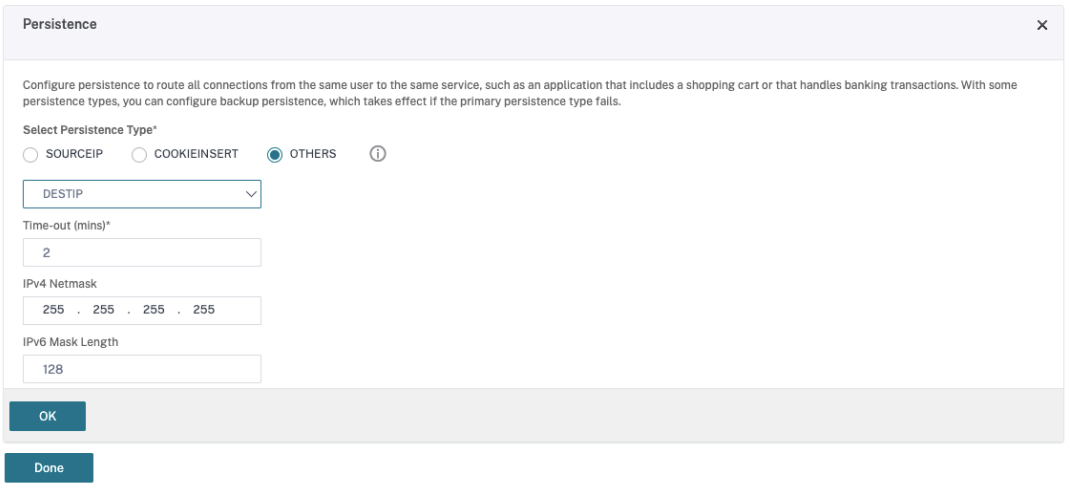
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 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**.



- Select persistence type as **Others**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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**.

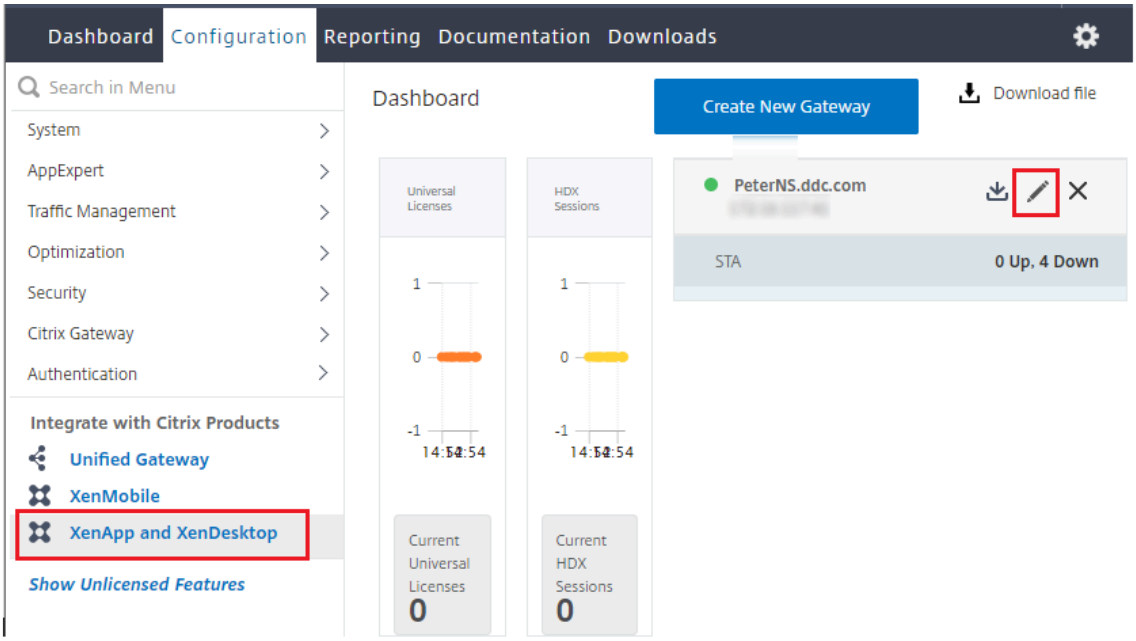
f) Repeat these steps for the other virtual server as well.

Configuration changes if the Citrix ADC appliance is already configured with Citrix Virtual Desktops™

If you have already configured the Citrix ADC appliance with Citrix Virtual Desktops, then to use the Secure XML feature, you must make the following configuration changes.

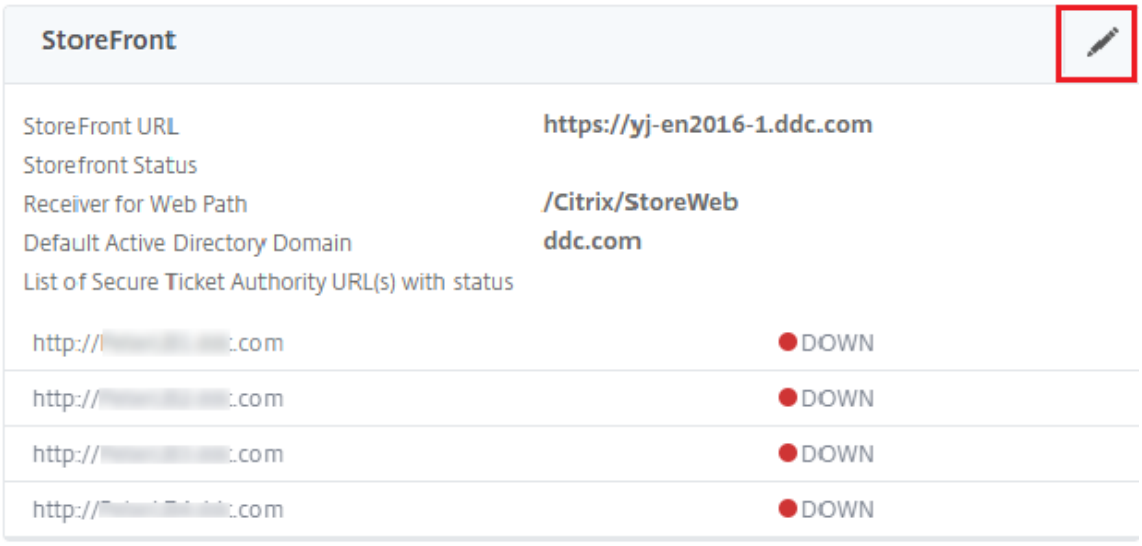
- Before the session launch, change the **Security Ticket Authority URL** of the gateway to use the FQDNs of the load balancing virtual servers.
- Ensure that the `TrustRequestsSentToTheXmlServicePort` parameter is set to False. By default, `TrustRequestsSentToTheXmlServicePort` parameter is set to False. However, if the customer has already configured the Citrix ADC for Citrix Virtual Desktops, 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.



3. In the StoreFront pane, click the edit icon.

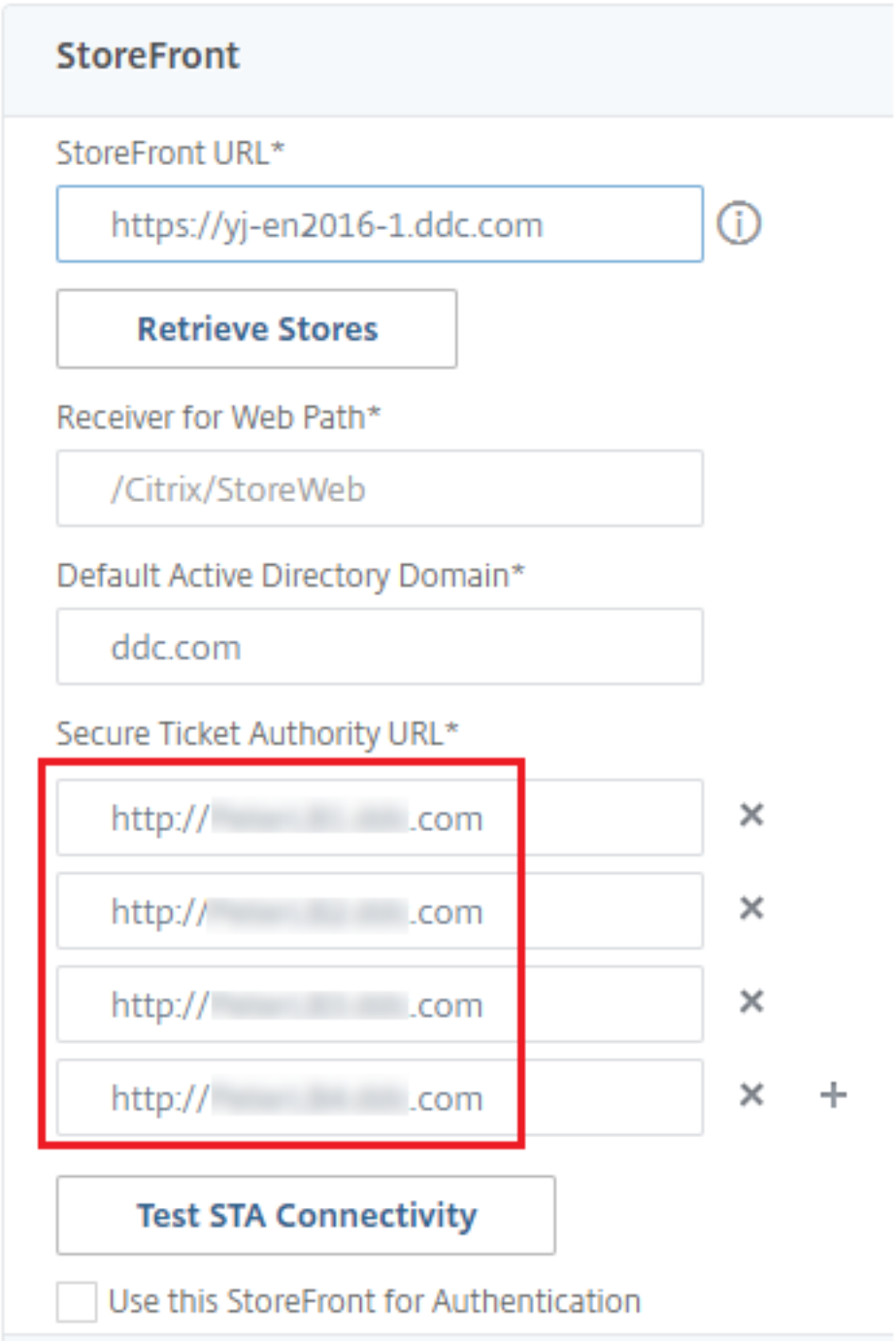
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

September 6, 2025

Maintaining session activity is critical to providing the best user experience. Losing connectivity due

© 1997–2026 Citrix Systems, Inc. All rights reserved.

to unreliable networks, highly variable network latency, and range limitations of wireless devices can lead to user frustration. Moving quickly between devices and accessing the same applications at each logon is a priority for many mobile workers such as healthcare workers.

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 they are using until network connectivity resumes.

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 lost connectivity, 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. Therefore, it 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 might get distracted and walk away from the user device. Those actions can potentially leave 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.
- To prevent users from reconnecting 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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 period, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period is five minutes. To change this period, edit the following registry setting on the user device (where `seconds` is the number of seconds after which no more attempts are made to reconnect the session).

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

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.

> **Note:**
>
> Auto Client Reconnect without reauthentication is supported only for password authentication. If you use Federated Authentication Service or smart card authentication, Auto Client Reconnect without reauthentication is not supported. In such cases, users are redirected to the login screen.

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. The

© 1997–2026 Citrix Systems, Inc. All rights reserved.

server also 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.

Cookies are not used if you enable the Auto Client Reconnect 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 earlier. 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 new 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, this feature prevents Remote Desktop Services from disconnecting that session. Examples of no activity include no clock change, no mouse movement, no screen updates. 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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 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, plus 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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, or 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 only for Citrix Workspace app users who access desktops and applications through a Citrix StoreFront connection. 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, a healthcare worker logs off from a device in the emergency room and then logs on to a workstation in the 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.

Session roaming

> **Note:**
>
> The following information guides you to configure session roaming using PowerShell. You can use Web 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 available on both 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 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 use of a printer.

- When 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.
- When 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 will be 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.

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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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`

- Value: `AutoLogonTimeout`
- Type: `DWORD`
- Specify a decimal time in seconds, in the range 0-3600.

If you change a master image, update the catalog.

This setting applies only to VMs with desktop VDAs. Microsoft controls the logon timeout on machines with server VDAs.

Settings

September 6, 2025

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

You can use Web Studio to manage these settings:

- Manage Authentication
- Set a default domain name for the Studio login page

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Customer Experience Improvement Program
- Remove Delivery Controllers
- Change database locations
- Set date and time
- Centralize site management
- Enable automatic assignment of multiple users for Remote PC Access
- Enable DNS resolution
- Enable XML trust
- Manage security key
- Set the inactivity timeout for the Studio console
- Centralize site management
- Set a custom notice on the Studio login page
- Display the FQDN of active DDC on the Studio login page

Manage authentication

By default, users log on to Web Studio using their domain username and password. You can also choose a different authentication method for users, such as the smart card authenticaiton or integrated Windows authentication.

Manage using Studio

To choose an authentication method for users, follow these steps:

1. Sign in to Web Studio and select **Settings** in the left pane.
2. Locate the **Authentication** tile and click **Edit** to select an option:
    - **Domain credentials**
    - **Domain credentials or integrated Windows authentication**

      With integrated Windows authentication enabled, users can access Web Studio using their Windows credentials (Kerberos/NTLM) or a client certificate.

      When the Web Studio and the Delivery Controller™ are installed on different machines, for integrated Windows authentication to work, enable Allow cross-origin access and add the URL of the Web Studio server to the allow list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important**
>
> Integrated Windows authentication does not work when Web Studio is configured as a proxy for Delivery Controllers.

- **Smart card authentication**
- **Domain credentials or smart card authentication**

  Enable smart card authentication requires additional configuration. For more information, see Set up smart card authentication for Web Studio.

Manage using the PowerShell script

The authentication method is configured in the Delivery Controller database. You can use the following PowerShell script to set the authentication method:

1. Get the current site ID by running the following command on the Delivery Controller:

   ```
   Get-ConfigSite | Select SiteGuid
   ```

2. Set the authentication method by running the following script:

```
# Generate a new bearer token
$bearerData = New-TrustBearerToken
# Define the Delivery Controller DNS name and Site ID
$ddc = "ddc.dc.com" # replace this with the Delivery Controller's
    DNS name
$siteid = "c68a8f89-42af-4bea-a6e9-c8c936353f49" # replace this
    with the site ID you get from step #1
# Define the URL and headers
$url = "https://$ddc/citrix/orchestration/api/CitrixOnPremises/
    Sites/$siteid/Settings"
$headers = @{

"Content-Type" = "application/json"
"Authorization" = "Bearer $($bearerData.Token)"
 }

# Define the JSON body
$body = @{

SupportedAuthenticators = "BasicAndSmartCard" # replace this with
    a required authentication method: "Basic" for "Domain
    credentials"; "BasicAndIntegratedWindowsAuthentication" for "
    Domain credentials or integrated Windows authentication"; "
    BasicAndSmartCard" for "Domain credentials or smart card
    authentication"; "SmartCard" for "Smart card authentication"
 }
  | ConvertTo-Json -Depth 10
# Send the PATCH request
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
21 Invoke-RestMethod -Uri $url -Method Patch -Headers $headers -Body
      $body
```

Configure the browsers for Integrated Windows authentication

If you enable *Integrated Windows authentication* using **Domain credentials or Integrated Windows authentication**, the next time your users sign in, they are automatically signed in. As a user, if you are unable to sign in automatically, follow these steps to configure your web browser to allow integrated Windows authentication.

For Google Chrome:

1. From the Control Panel, select **Internet Options**.
2. Select the **Advanced** tab.
3. Select **Enable Integrated Windows Authentication**.
4. Select the **Security** tab.
5. Select **Local Intranet > Sites > Advanced**.
6. In the **Add this website to the zone** box:
   - If the Web Studio and the Delivery Controller reside on the same server, type the URL of the host running the Web Studio.
   - If not, type a wildcard domain. Example: if the Delivery Controller is at `ddc.domain.com`, type `*.domain.com`.
7. Click **Add > Close**

For Mozilla Firefox:

1. From the browser, type `about:config` in the URL box.
2. In the **Search** box, type `network negotiate`.
3. Right-click **network.negotiate-auth.trusted-uris** and select **Modify**.
4. In the **Enter string value** box:
   - If the Web Studio and the Delivery Controller reside on the same server, add a comma-separated list of URLs and/or aliases referencing the name of the server hosting the Web Studio.
   - If not, add the URLs this way. Example: if the Delivery Controller is at `ddc.domain.com`, type `*.domain.com`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you configure your browser, you can click **Windows integrated sign-in** on the sign-in page to try again.

When the Web Studio and the Delivery Controller are installed on different machines, for integrated Windows authentication to work, you need to enable **Allow cross-origin access**.

Follow these steps to enable **Allow cross-origin access**:

1. Select the **Allow cross-origin access** checkbox.
2. Add the URL of the Web Studio server to the allow list.
3. In the **Enter URL** field, enter the URL. Click **Add** to add more if necessary.

   > **Note**
   >
   > - The URL must follow the correct format:`<scheme>://<hostname>`. Make sure that it does not include any paths or trailing slashes.
   > - IP addresses and FQDNS are supported. When adding a URL, ensure that it corresponds to how you access the Web Studio. For example, if accessing the Web Studio using an IP address, add the IP address-based URL to the list.
   > - If you use a non-default port, be sure to include the port number.

4. Click **Add** to add more if necessary.
5. After you have finished, click **Done** to save and exit.

Set a default domain name for the Studio login page

To auto-populate the **Domain** field on the Studio login page with a domain name, follow these steps:

1. Sign in to Web Studio and select Settings in the left pane.
2. On the **Configure domain name** tile, type a domain name as needed.
3. Click **Apply**.

   When an administrator accesses the Studio login page, the *Domain* field is automatically populated with the domain name you set.

Set up the time zone

Configure the default time zone, date format, and time format for your DaaS site. Studio uses these settings for time displays and scheduling such as scheduled restart and autoscaling.

If needed, you can change the time zone for individual delivery groups. For more information, see Change user settings in a delivery group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> This setting is specific to each Citrix user account.

To set the default time zone, follow these steps:

1. From Web Studio, go to **Settings > Date and Time**.
2. Click **Edit**.
3. Configure the following settings:
   - **Date format**: Select how to display the date (for example, yyyy/MM/dd).

     > **Note:**
     >
     > To use the date format associated with the language you chose for Studio, select **Use local**.

   - **Time format:** Select to display the time using a 12-hour clock (09:00 PM, for example) or a 24-hour clock (21:00, for example).

     > **Note:**
     >
     > To use the time format associated with the language you chose for Studio, select **Use local**.

   - **Time zone:** Select a time zone.

     > **Note:**
     >
     > To use your computer's time zone setting, select **Use local**.

4. Click **Save**.

   > **Note:**
   >
   > Throughout Web Studio, you can hover over any displayed time to see its equivalent in your local time zone.

Enable DNS resolution

To present DNS names instead of IP addresses in the ICA® file, follow these steps:

1. Sign in to Web Studio and select **Settings** in the left pane.
2. Turn on the **Enable DNS resolution** setting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set the inactivity timeout for the Studio console

You can set the inactivity duration after which administrators are automatically signed out of the Studio console.

1. Sign in to Web Studio and select **Settings** in the left pane.
2. Type a duration ranging from 10 minutes to 24 hours.
3. To apply this setting, refresh the page or sign out and then sign back in.

Centralize site management

This feature lets you use one Web Studio console to manage multiple Citrix Virtual Apps and Desktops sites. For more information, see Enable multiple site management.

Set a custom notice on the Studio login page

To set a sign-in page notice, follow these steps:

1. Sign in to Web Studio and select **Settings** in the left pane.
2. Locate the **Login page notice** tile and select the **Show notice on login page** checkbox.
3. Click **Edit** to open the **Login page notice** page and type a login page notice as needed.
4. Click **Save**.

Display the FQDN of active DDC on the Studio login page

To display the FQDN of DDC used for the current session on the Studio sign-in page, follow these steps:

1. Sign in to Web Studio and select **Settings** in the left pane.
2. Turn on **Show connected Controller**.

Tags

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

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 to only items that have a specified tag.

- Tailor search displays in Web 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 Web Studio 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 or can be helpful when isolating and troubleshooting a subset of machines in a delivery group.

- Schedule periodic restarts for a subset of machines in a delivery group.

  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 a subset of machines in delivery groups, delivery group types, or OUs that have (or do not 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Machines
- Applications
- Machine catalogs (PowerShell only; see Tags on machine catalogs)
- Delivery groups
- Application groups

You can configure a tag restriction can be configured when creating or editing the following in Web 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:

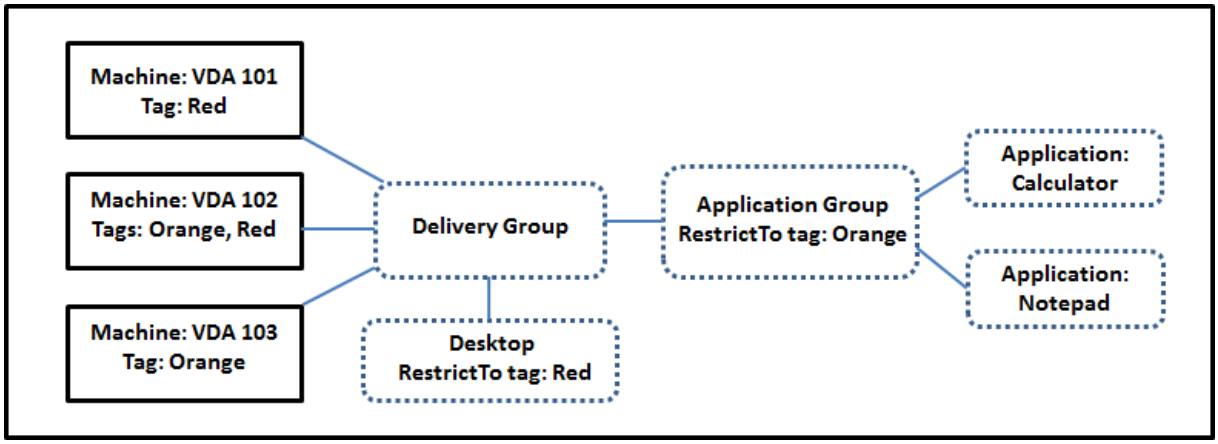
- Create the tag and then add (apply) it to machines.
- Create or edit a group with the tag restriction (in other words, "restrict launches to machines with tag x").

A tag restriction extends the broker's machine selection process. The broker 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 broker 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. The site has one shared delivery group, one published desktop, and one application group configured with two applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Tags have been added to each of the three machines (VDA 101–103).
- The desktop in the shared delivery group was created with a tag restriction named "Red". A 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.

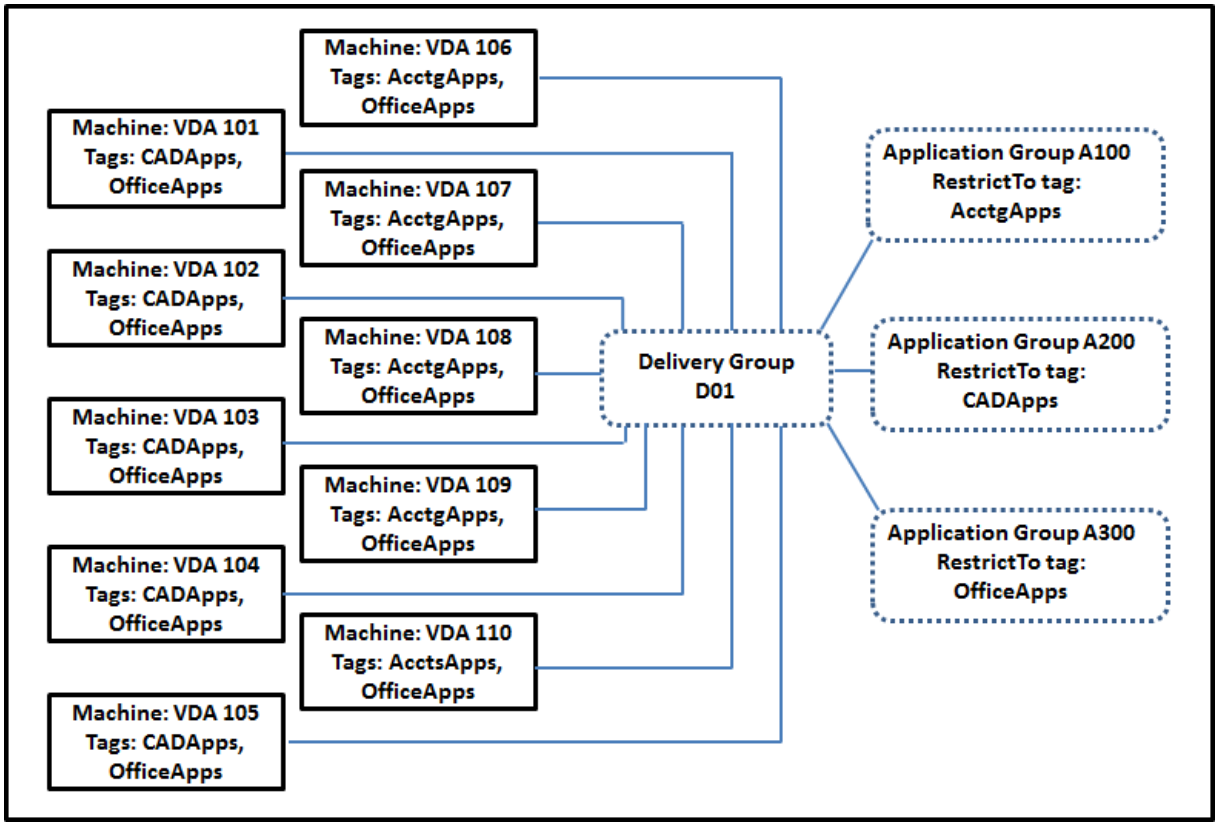
Machine VDA 102 has both tags (Red and Orange), so it can be considered for launching the applications and the desktop.

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 Web Studio.

(Exception: Tags used for policy assignments are created, edited, and deleted through the **Manage Tags** action in Web Studio. However, tags are applied (assigned) when you create the policy. See Create policies for details.)

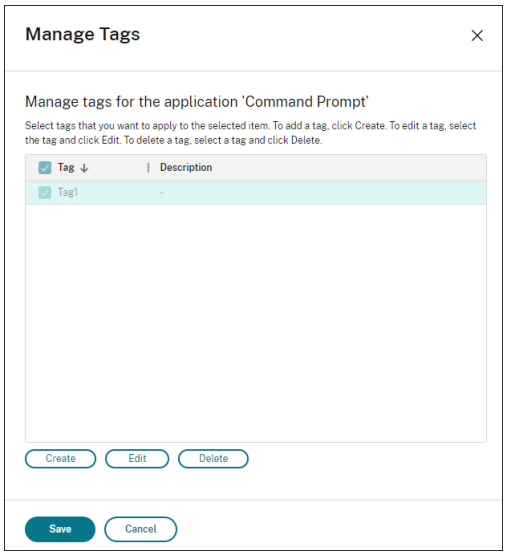
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 dialogs in Web Studio

In Web Studio, select the items you want to apply a tag to (one or more machines, applications, a desktop, a delivery group, or an application group) and then select **Manage Tags** in the action bar. The dialog box lists all the tags that have been created in the Site, not just for the items you selected.

- A check box containing a check mark indicates that the tag has already been added to the selected items. (In the screen capture below, the selected machine has the tag named "Tag1" applied.)
- If you selected more than one item, a check box containing a hyphen indicates that some, but not all selected items have that tag added.



The following actions are available from the **Manage Tags** dialog box. Be sure to review Cautions when working with tags.

- **To create a tag:**

  Click **Create.** Enter a name and description. Tag names must be unique and are not case-sensitive. Then click **OK**. (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. If you selected multiple items and the check box next to a tag contains a hyphen (indicating that some, but not all selected items already have the tag applied), changing it to a check mark affects all selected machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you attempt to add a tag to one or more machines, and that tag is being used as a restriction in an application group, you are warned that the action can result in making those machines available for launch. If that's what you intended, proceed.

- **To remove one or more tags:**

  Clear the check box next to the tag name. If you selected multiple items and the check box next to a tag contains a hyphen (indicating that some, but not all selected items already have the tag applied), clearing the check box removes the tag from all selected machines.

  If you attempt to remove a tag from a machine that is using that tag as a restriction, you are warned that the action can affect which machines are considered for launch. If that's what you intended, proceed.

- **To edit a tag:**

  Select a tag and then click **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 click **Delete**. The Delete Tag dialog box indicates how many items currently use the selected tags (for example "2 machines"). Click an item to display more information. For example, clicking a "2 machines"item displays the names of the two machines that have that tag applied. Confirm whether you want to delete the tags.

  You cannot use Web Studio to 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, click **Save**.

To see if a machine has any tags applied: Select **Delivery Groups** in the left pane. Select a delivery group in the middle pane and then select **View Machines** in the action bar. Select a machine in the middle pane and then select the **Tags** tab on the **Details** pane.

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 affected by the tag restriction, using the **Manage Tags** actions described earlier.

- **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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. Click **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, click **Edit**. In the dialog box, either select a different tag from the lists 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, so keep in mind that adding, removing, and deleting a tag can have unintended effects. You can use a tag to sort machine displays in the Web Studio search field. You can use the same tag as a restriction when configuring an application group or a desktop. The tag limits launch consideration to only machines in specified delivery groups that have that tag.

When you try to add a tag to machines after that tag has been configured as a tag restriction for a desktop or an application group, a warning appears. Adding that tag might make the machines available for launching additional applications or desktops. If that is what you intended, proceed. If not, you can cancel the operation.

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 attempt to add the "Red"tag to those machines, Web Studio displays 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, if an application group uses a tag to restrict launches, Web Studio warns that you cannot delete the tag until you edit the group to remove it as a restriction. (If you were allowed to delete a tag that's used as a restriction in an application group, that 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 are 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 are 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 second example.

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. In Web Studio, 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, click **Create** and then create a tag named `CADApps`. Click **OK**.
4. Click **Create** again and create a tag named OfficeApps. Click **OK**.
5. While still in the **Manage Tags** dialog box, add (apply) the newly created tags to the selected machines by enabling the check boxes next to each tag's name (`CADApps` and `OfficeApps`). When you're done, 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, click **Create**. Create a tag named `AcctgApps`. Click **OK**.
9. Apply the newly created `AcctgApps` tag and the `OfficeApps` tag to the selected machines by clicking the check boxes next to each tag's name, and then close the dialog box.

Create the application groups with tag restrictions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In Web Studio, select **Applications** in the left pane, select the **Application Groups** tab, and then select **Create Application Group** in the action bar. The Create Application Group wizard launches.
2. On the **Delivery Groups** page of the wizard, select delivery group D01. Select **Restrict launches to machines with tag** and then select the `AcctgApps` tag from the list.
3. 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`.
4. Repeat the preceding steps to create application group `A200`, specifying machines that have the `CADApps` tag, plus the appropriate users and applications.
5. Repeat steps to create application group `A300`, specifying machines that have the `OfficeApps` tag, plus the appropriate users and applications.

Tags on machine catalogs

You can use tags on machine catalogs. The overall sequence of creating a tag and then applying it to a catalog is the same as described previously. However, applying tags to catalogs is supported only through the PowerShell interface. You cannot use Web Studio to apply a tag to a catalog or remove a tag from a catalog. Catalog displays in Web Studio do not indicate if a tag is applied.

Summary: You can use Web Studio or PowerShell to create or delete a tag for use on a catalog. Use PowerShell to apply the tag to the catalog.

Here are some examples of using tags with catalogs:

- A delivery group has 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.
- In an application group, you want to limit application sessions to machines in a specific catalog. Applying a tag to that catalog accomplishes that.

Affected PowerShell cmdlets:

- 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 tag named `fy2018` to the catalog named `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. (The tag was previously created using either Web Studio or PowerShell.)

See the PowerShell cmdlet help for more guidance and syntax.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
- **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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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
```

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.

User profiles

September 13, 2025

By default, Citrix Profile Management is installed silently on master images when you install the Virtual Delivery Agent, but you do not have to use Profile Management as a profile solution.

To suit your users’ varying needs, you can use Citrix Virtual Apps and Desktops™ policies to apply different profile behavior to the machines in each Delivery Group. For example, one Delivery Group might require Citrix mandatory profiles, whose template is stored in one network location, while another Delivery Group requires Citrix roaming profiles stored in another location with several redirected folders.

- If other administrators in your organization are responsible for Citrix Virtual Apps and Desktops policies, work with them to ensure that they set any profile-related policies across your Delivery Groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Profile Management policies can also be set in Group Policy, in the Profile Management .ini file, and locally on individual virtual machines. These multiple ways of defining profile behavior are read in the following order:

  1. Group Policy (.adm or .admx files)
  2. Citrix Virtual Apps and Desktops policies in the Policy node
  3. Local policies on the virtual machine that the user connects to
  4. Profile Management .ini file

  For example, if you configure the same policy in both Group Policy and the Policy node, the system reads the policy setting in Group Policy and ignores the Citrix Virtual Apps and Desktops policy setting.

Whichever profile solution you choose, Director administrators can access diagnostic information and troubleshoot user profiles. For more information, see the Director documentation.

Automatic configuration

The desktop type is automatically detected, based on the Virtual Delivery Agent installation and, in addition to the configuration choices you make in Studio, sets Profile Management defaults accordingly.

The policies that Profile Management adjusts are shown in the following table. Any non-default policy settings are preserved and are not overwritten by this feature. Consult the Profile Management documentation for information about each policy. The types of machines that create profiles affect the policies that are adjusted. The primary factors are whether machines are persistent or provisioned, and whether they are shared by multiple users or dedicated to just one user.

Persistent systems have some type of local storage, the contents of which can be expected to persist when the system turns off. Persistent systems might employ storage technology such as SANs to provide local disk mimicking. In contrast, provisioned systems are created "on the fly"from a base disk and some type of identity disk. Local storage is usually mimicked by a RAM disk or network disk, the latter often provided by a SAN with a high speed link. The provisioning technology is generally Citrix Provisioning or Machine Creation Services™ (or a third-party equivalent). Sometimes provisioned systems have persistent local storage. These are classed as persistent.

Together, these two factors define the following machine types:

- **Both persistent and dedicated**. Examples are single-session OS machines with a static assignment and persistent local storage that are created with Machine Creation Services, physical workstations, and laptops.
- **Both persistent and shared**. Examples are multi-session OS machines that are created with Machine Creation Services, and Citrix Virtual Apps servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Both provisioned and dedicated**. Examples are single-session OS machines with a static assignment but without persistent storage that are created with Citrix Provisioning Service (in Citrix Virtual Desktops™).
- **Both provisioned and shared**. Examples are single-session OS machines with a random assignment that are created with Citrix Provisioning™ Service (in Citrix Virtual Desktops) and Citrix Virtual Apps servers.

The following Profile Management policy settings are suggested guidelines for the different machine types. They work well in most cases, but you might want to deviate from them as your deployment requires.

> **Important:**
>
> **Delete locally cached profiles on logoff**, **Profile streaming**, and **Always cache** are enforced by the auto-configuration feature. Adjust the other policies manually.

Persistent machines

Policy	Both persistent and dedicated	Both persistent and shared
Delete locally cached profiles on logoff	Disabled	Enabled
Profile streaming	Disabled	Enabled
Always cache	Enabled (note 1)	Disabled (note 2)
Active write back	Disabled	Disabled (note 3)
Process logons of local administrators	Enabled	Disabled (note 4)

Provisioned machines

Policy	Both provisioned and dedicated	Both provisioned and shared
Delete locally cached profiles on logoff	Disabled (note 5)	Enabled
Profile streaming	Enabled	Enabled
Always cache	Disabled (note 6)	Disabled
Active write back	Enabled	Enabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy	Both provisioned and dedicated	Both provisioned and shared
Process logons of local administrators	Enabled	Enabled (note 7)

1. Because **Profile streaming** is disabled for this machine type, the **Always cache** setting is always ignored.
2. Disable **Always cache**. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
3. Disable **Active write back** except to save changes in profiles of users who roam between Citrix Virtual Apps servers. In this case, enable this policy.
4. Disable **Process logons of local administrators** except for Hosted Shared Desktops. In this case, enable this policy.
5. Disable **Delete locally cached profiles on logoff**. This setting retains locally cached profiles. Because the machines are reset at logoff but are assigned to individual users, logons are faster if their profiles are cached.
6. Disable **Always cache**. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
7. Enable **Process logons of local administrators** except for profiles of users who roam between Citrix Virtual Apps and Desktops servers. In this case, disable this policy.

Folder redirection

Folder redirection lets you store user data on network shares other than the location where the profiles are stored. Folder redirection reduces profile size and load time but it might impact network bandwidth. Folder redirection does not require that Citrix user profiles are employed. You can choose to manage user profiles on your own, and still redirect folders.

Configure folder redirection using Citrix policies in Studio.

- Ensure that the network locations used to store the contents of redirected folders are available and have the correct permissions. The location properties are validated.
- Redirected folders are set up on the network and their contents populated from users' virtual desktops at logon.

Configure folder redirection using only Citrix Policies or Active Directory Group Policy Objects, not both. Configuring folder redirection using both policy engines might result in unpredictable behavior.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Advanced folder redirection

In deployments with multiple operating systems (OSs), you might want some of a user's profile to be shared by each OS. The rest of the profile is not shared and is used only by one OS. To ensure a consistent user experience across the OSs, you need a different configuration for each OS, that is, advanced folder redirection. For example, different versions of an application running on two OSs might need to read or edit a shared file, so you decide to redirect it to a single network location where both versions can access it. Alternatively, because the **Start Menu** folder contents are structured differently in two OSs, you decide to redirect only one folder, not both. This approach separates the **Start Menu** folder and its contents on each OS, ensuring a consistent experience for users.

If your deployment requires advanced folder redirection, you must understand the structure of your users' profile data and determine which parts of it can be shared between OSs. Unpredictable behavior can result unless folder redirection is used correctly.

To redirect folders in advanced deployments:

- Use a separate Delivery Group for each OS.
- Understand where your virtual applications, including those on virtual desktops, store user data and settings, and understand how the data is structured.
- For shared profile data that can safely roam (because it is structured identically in each OS), redirect the containing folders in each Delivery Group.
- For non-shared profile data that cannot roam, redirect the containing folder in only one of the Desktop Groups, typically the one with the most used OS or the one where the data is most relevant. Alternatively, for non-shared data that cannot roam between OSs, redirect the containing folders on both systems to separate network locations.

Example advanced deployment

The deployment has applications, including versions of Microsoft Outlook and Internet Explorer, running on Windows 10 desktops and applications, including other versions of Outlook and Internet Explorer, delivered by Windows Server 2019. You have already set up two Delivery Groups for the two OSs. Users want to access the same set of **Contacts** and **Favorites** in both versions of the two applications.

Important: The following decisions and advice are valid for the OSs and deployment described. In your organization, the folders you choose to redirect and whether your decide to share them depend on various factors that are unique to your specific deployment.

- Using policies applied to the Delivery Groups, you choose the following folders to redirect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Folder	Redirected in Windows 10?	Redirected in Windows Server 2019?
My Documents	Yes	Yes
Application Data	No	No
Contacts	Yes	Yes
Desktop	Yes	No
Downloads	No	No
Favorites	Yes	Yes
Links	Yes	No
My Music	Yes	Yes
My Pictures	Yes	Yes
My Videos	Yes	Yes
Searches	Yes	No
Saved Games	No	No
Start Menu	Yes	No

- For the shared, redirected folders:
  - After analyzing the structure of the data saved by the different versions of Outlook and Internet Explorer, you decide it is safe to share the **Contacts** and **Favorites** folders.
  - You know the structure of the **My Documents**, **My Music**, **My Pictures**, and **My Videos** folders is standard across OSs. So it is safe to store these folders in the same network location for each Delivery Group.
- For the non-shared, redirected folders:
  - You do not redirect the Desktop, Links, Searches, or **Start Menu** folder in the Windows Server Delivery Group because data in these folders is organized differently in the two OSs. It therefore cannot be shared.
  - To ensure predictable behavior of this non-shared data, you redirect it only in the Windows 10 Delivery Group. Windows 10 are used more often by users in their day-to-day work. Users only occasionally access the applications delivered by the Windows Server. Also, in this case the non-shared data is more relevant to a desktop environment rather than an application environment. For example, desktop shortcuts are stored in the **Desktop** folder and might be useful if they originate from a Windows 10 machine but not from a Windows Server machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For the non-redirected folders:
  - You do not want to clutter your servers with users' downloaded files, so you choose not to redirect the Downloads folder
  - Data from individual applications can cause compatibility and performance issues, so you decide not to redirect the Application Data folder

For more information on folder redirection, see Folder Redirection, Offline Files, and Roaming User Profiles overview.

Folder redirection and exclusions

In Citrix Profile Management (but not in Studio), a performance enhancement allows you to prevent folders from being processed using exclusions. If you use this feature, do not exclude any redirected folders. The folder redirection and exclusion features work together. Ensuring no redirected folders are excluded allows Profile Management to move them back into the profile folder structure and preserves data integrity if you later decide not to redirect them. For more information on exclusions, see Include and exclude items.

VDA registration

September 6, 2025

Introduction

> **Note:**
>
> In an on-premises environment, VDAs register with a Delivery Controller. In a Citrix Cloud service environment, VDAs register with a Cloud Connector. In a hybrid environment, some VDAs register with a Delivery Controller while others register with a Cloud Connector.

Before a VDA can be used, it must register (establish communication) with one or more Controllers or Cloud Connectors on the site. The VDA finds a Controller or Connector by checking a list called the `ListofDDCs`. The `ListOfDDCs` on a VDA contains DNS entries that point that VDA to Controllers or Cloud Connectors on the site. For load balancing, the VDA automatically distributes connections across all Controllers or Cloud Connectors in the list.

Why is VDA registration so important?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- From a security perspective, registration is a sensitive operation. You're establishing a connection between the Controller or Cloud Connector and the VDA. For such a sensitive operation, the expected behavior is to reject the connection if everything is not in perfect shape. You are effectively establishing two separate communication channels: VDA to Controller or Cloud Connector, and Controller or Cloud Connector to VDA. The connection uses Kerberos, so time synchronization and domain membership issues are unforgiving. Kerberos uses Service Principal Names (SPNs), so you cannot use load-balanced IP\hostname.
- If a VDA does not have accurate and current Controller or Cloud Connector information as you add and remove Controllers (or Cloud Connectors), the VDA might reject session launches that are brokered by an unlisted Controller or Cloud Connector. Invalid entries can delay the startup of the virtual desktop system software. A VDA won't accept a connection from an unknown and untrusted Controller or Cloud Connector.

In addition to the `ListofDDCs`, the `ListOfSIDs` (Security IDs) indicates which machines in the `ListofDDCs` are trusted. The `ListofSIDs` can be used to decrease the load on Active Directory or to avoid possible security threats from a compromised DNS server. For more information, see ListOfSIDs.

If a `ListofDDCs` specifies more than one Controller or Cloud Connector, the VDA attempts to connect to them in random order. In an on-premises deployment, the `ListofDDCs` can also contain Controller groups. The VDA attempts to connect to each Controller in a group before moving to other entries in the `ListofDDCs`.

Citrix Virtual Apps and Desktops™ automatically tests the connectivity to configured Controllers or Cloud Connectors during VDA installation. Errors are displayed if a Controller or Cloud Connector cannot be reached. If you ignore a warning that a Controller or Cloud Connector cannot be contacted (or when you do not specify Controller or Cloud Connector addresses during VDA installation), messages remind you.

Methods for configuring Controller or Cloud Connector addresses

The administrator chooses the configuration method to use when the VDA registers for the first time (the initial registration). During the initial registration, a persistent cache is created on the VDA. During subsequent registrations, the VDA retrieves the list of Controllers or Cloud Connectors from this local cache, unless a configuration change is detected.

The easiest way to retrieve that list during subsequent registrations is by using the auto-update feature. Auto-update is enabled by default. For more information, see Auto-update.

There are several methods for configuring Controller or Cloud Connector addresses on a VDA.

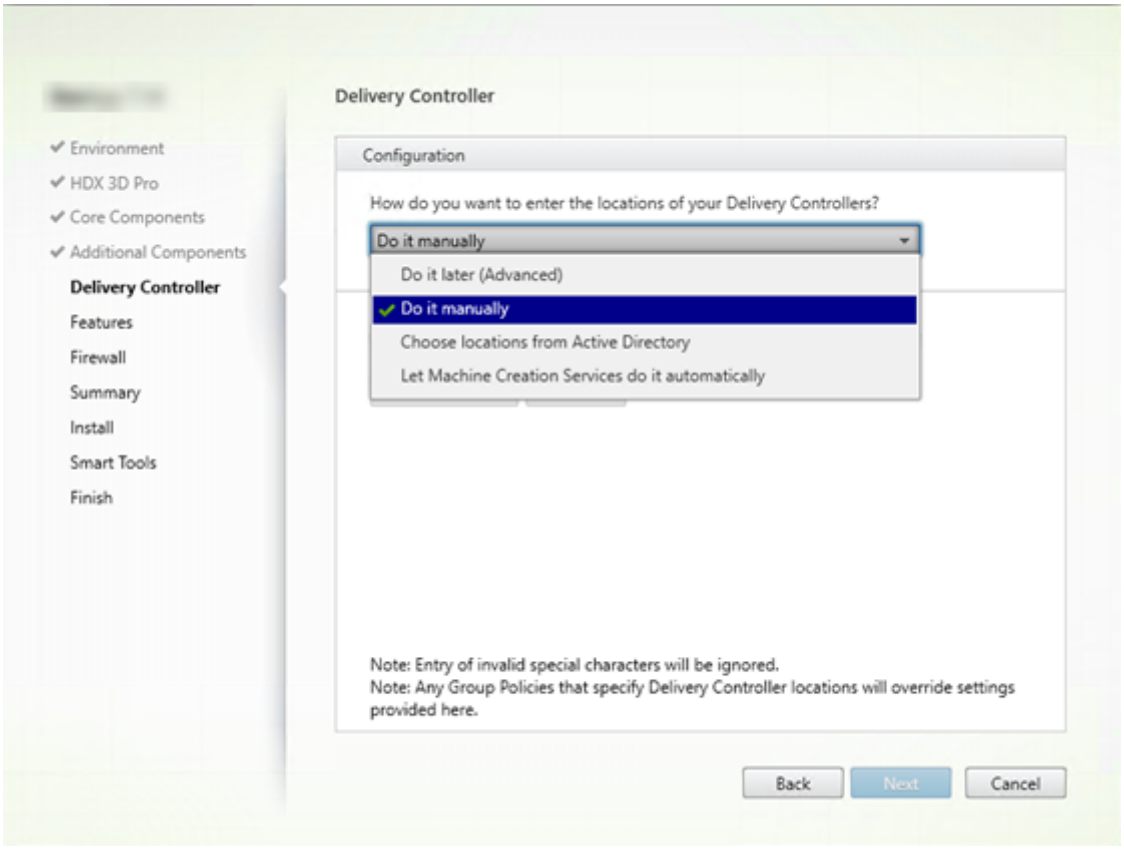
- Policy-based (LGPO or GPO)
- Registry-based (manual, Group Policy Preferences (GPP), specified during VDA installation)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Active Directory OU-based (legacy OU discovery)
- MCS-based (personality.ini)

You specify the initial registration method when you install a VDA. (If you disable auto-update, the method you select during VDA installation is used for subsequent registrations.)

The following graphic shows the **Delivery Controller** page of the VDA installation wizard.



Policy-based (LGPO\GPO)

Citrix® recommends using GPO for initial VDA registration. It has the highest priority. (Although auto-update is listed as the highest priority, auto-update is used only after the initial registration.) Policy-based registration offers the centralizing advantages of using Group Policy for configuration.

To specify this method, complete both of the following steps:

- On the **Delivery Controller** page in the VDA installation wizard, select **Do it later (advanced)**. The wizard reminds you several times to specify Controller addresses, even though you're not specifying them during VDA installation. (VDA registration is that important.)
- Enable or disable policy-based VDA registration through Citrix policy with the `Virtual Delivery Agent Settings > Controllers` setting. (If security is your top priority, use the `Virtual Delivery Agent Settings > Controller SIDs` setting.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This setting is stored under HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs).

Registry-based

To specify this method, complete one of the following steps:

- On the **Delivery Controller** page in the VDA installation wizard, select **Do it manually**. Then, enter the FQDN of an installed Controller and then click **Add**. If you've installed more Controllers, add their addresses.
- For a command-line VDA installation, use the /controllers option and specify the FQDNs of the installed Controllers or Cloud Connectors.

This information is stored in registry value ListOfDDCs under registry key HKLM\Software\Citrix\VirtualDesktopAgent or HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAge
.

You can also configure this registry key manually or use Group Policy Preferences (GPP). This method might be preferable to the policy-based method (for example, if you want conditional processing of different Controllers or Cloud Connectors, such as: use XDC-001 for computer names that begin with XDW-001-).

Update the ListOfDDCs registry key, which lists the FQDNs of all the Controllers or Cloud Connectors in the site. (This key is the equivalent of the Active Directory site OU.)

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

If the HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent registry location contains both the ListOfDDCs and FarmGUID keys, ListOfDDCs is used for Controller or Cloud Connector discovery. The FarmGUID is present if a site OU was specified during VDA installation. (This might be used in legacy deployments.)

Optionally, update the ListOfSIDs registry key (for more information, see ListOfSIDs:

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

Remember: If you also enable policy-based VDA registration through Citrix policy that overrides settings you specify during VDA installation, because it is a higher-priority method.

Active Directory OU-based (legacy)

This method is supported primarily for backward compatibility and is not recommended. If you're still using it, Citrix suggests changing to another method.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To specify this method, complete both of the following steps:

- On the **Delivery Controller** page in the VDA installation wizard, select **Choose locations from Active Directory.**
- Use the `Set-ADControllerDiscovery.ps1` script (available on every Controller). Also, configure the `FarmGuid` registry entry on each VDA to point to the right OU. This setting can be configured using Group Policy.

MCS-based

If you use MCS to provision VMs, MCS sets up the list of Controllers or Cloud Connectors. This feature works with auto-update. When creating the catalog, MCS injects the list of Controllers or Cloud Connectors into the `Personality.ini` file during initial provisioning. Auto-update keeps the list current.

To specify this method, on the **Delivery Controller** page in the VDA installation wizard, select **Let Machine Creation Services™ do it**.

Review and recommendations

As best practice:

- Use the Group Policy registration method for initial registration.
- Use auto-update (enabled by default) to keep your list of Controllers up-to-date.
- In a multi-zone deployment, use Group Policy for initial configuration (with at least two Controllers or Cloud Connectors). Point VDAs to Controllers or Cloud Connectors local to (in) their zone. Use auto-update to keep them up-to-date. Auto-update automatically optimizes the `ListofDDCs` for VDAs in satellite zones.
- List more than one controller on the `ListOfDDCs` registry key, separated by a space, to prevent registration issues if a Controller is not available. For example:

```
DDC7x.xd.local DDC7xHA.xd.local

32-bit: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs

HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs (REG_SZ)
```

- Ensure all values listed under `ListofDDCs` map to a valid fully qualified domain name to prevent startup registration delays.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auto-update

Auto-update (introduced in XenApp and XenDesktop 7.6) is enabled by default. It is the most efficient method for keeping your VDA registrations up-to-date. Although not used for initial registration, the auto-update software downloads and stores the `ListofDDCs` in a persistent cache on the VDA when initial registration occurs. This process is done for each VDA. The cache also holds machine policy information, which ensures that policy settings are retained across restarts.

Auto-update is supported when using MCS or Citrix Provisioning™ to provision machines, except for Citrix Provisioning server-side cache. Server-side cache is not a common scenario because there is no persistent storage for auto-update cache.

To specify this method:

- Enable or disable auto-update through a Citrix policy containing the setting `Virtual Delivery Agent Settings` > `Enable auto update of Controllers`. This setting is enabled by default.

How it works:

- Each time a VDA re-registers (for example, after a machine restart), the cache is updated. Each Controller or Cloud Connector also checks the site database every 90 minutes. If a Controller or Cloud Connector has been added or removed since the last check, or if a policy change occurred that affects VDA registration, the Controller or Cloud Connector sends an updated list to its registered VDAs and the cache is updated. The VDA accepts connections from all the Controllers or Cloud Connectors in its most recently cached list.
- If a VDA receives a list that does not include the Controller or Cloud Connector it is registered with (in other words, that Controller or Cloud Connector was removed from the site), the VDA re-registers, choosing among the Controllers or Cloud Connectors in the `ListofDDCs`.

Example:

- A deployment has three Controllers: A, B, and C. A VDA registers with Controller B (which was specified during VDA installation).
- Later, two Controllers (D and E) are added to the site. Within 90 minutes, VDAs receive updated lists and then accept connections from Controllers A, B, C, D, and E. (The load is not spread equally to all Controllers until the VDAs are restarted.)
- Later still, Controller B is moved to another site. Within 90 minutes, VDAs in the original site receive updated lists because there has been a Controller change since the last check. The VDA that originally registered with Controller B (which is no longer on the list) re-registers, choosing among the Controllers in the current list (A, C, D, and E).

In a multi-zone deployment, auto-update in a satellite zone automatically caches all local Controllers first. All Controllers in the primary zone are cached in a backup group. If no local Controllers in the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

satellite zone are available, registration is attempted with Controllers in the primary zone.

As shown in the following example, the cache file contains host names and a list of Security IDs (`ListofSIDs`). The VDA does not query SIDs and thus, reduces the Active Directory load.

You can retrieve the cache file with a WMI call. However, it is stored in a location that's readable only by the SYSTEM account.

> **Important:**
>
> This information is provided only for information purposes. DO NOT MODIFY THIS FILE. Any modification to this file or folder results in an unsupported configuration.

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation"-Class "
Citrix_VirtualDesktopInfo"-Property "PersistentDataLocation"
```

If you need to manually configure the `ListofSIDs` for security reasons (as distinct from reducing Active Directory load), you cannot use the auto-update feature. For details, see ListOfSIDs.

Exception to auto-update priority

Although auto-update usually has the highest priority of all VDA registration methods and overrides settings for other methods, there is an exception. The `NonAutoListOfDDCs` elements in the cache specify the initial VDA configuration method. Auto-update monitors this information. If the initial registration method changes, the registration process skips auto-update, and uses the next-highest configured priority method. This process can be helpful when you move a VDA to another site (for example, during disaster recovery).

Configuration considerations

View a common VDA registration configuration.

This is an embedded video. Click the link to watch the video

View VDA registration steps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This is an embedded video. Click the link to watch the video

Consider the following when configuring items that can affect VDA registration.

Controller or Cloud Connector addresses

Regardless of which method you use to specify Controllers or Cloud Connectors, Citrix recommends using an FQDN address. An IP address is not considered a trusted configuration, because it's easier to compromise an IP than a DNS record. If you populate the `ListofSIDs` manually, you can use an IP in a `ListofDDCs`. However, FQDN is still recommended.

Load balancing

As noted earlier, the VDA automatically distributes connections across all Controllers or Cloud Connectors in the `ListofDDCs`. Failover and load balancing functionality is built into the Citrix Brokering Protocol (CBP). If you specify multiple Controllers or Cloud Connectors in your configuration, registration automatically fails over between them, if needed. With auto-update, automatic failover occurs automatically for all VDAs.

For security reasons, you cannot use a network load balancer, such as Citrix ADC. VDA registration uses Kerberos mutual authentication, where the client (VDA) must prove its identity to the service (Controller). However, the Controller or Cloud Connector must prove its identity to the VDA. This means that the VDA and the Controller or Cloud Connector are acting as server and client at the same time. As noted at the beginning of this article, there are two communications channels: VDA to Controller/-Cloud Connector and Controller/Cloud Connector to VDA.

A component in this process is called Service Principal Name (SPN), which stored as a property in an Active Directory computer object. When your VDA connects to a Controller or Cloud Connector, it must specify who it wants to communicate with. This address is an SPN. If you use a load-balanced IP, mutual Kerberos authentication correctly recognizes that the IP does not belong to the expected Controller or Cloud Connector.

For more information, see:

- Introduction to Kerberos
- Mutual authentication using Kerberos

Auto-update replaces CNAME

The auto-update feature replaces the CNAME (DNS alias) function from XenApp and XenDesktop versions earlier than 7.x. CNAME functionality is disabled, beginning with XenApp and XenDesktop 7.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use auto-update instead of CNAME. (If you must use CNAME, see CTX137960. For DNS aliasing to work consistently, do not use both auto-update and CNAME at the same time.)

Controller/Cloud Connector groups

In certain scenarios, you might want to process Controllers or Cloud Connectors in groups, with one group being preferred and the other group used for a failover if all Controllers/Cloud Connectors fail. Remember that Controllers or Cloud Connectors are randomly selected from the list, so grouping can help enforce preferential use.

These groups are intended for use within a single site (not multiple sites).

Use parentheses to specify groups of Controllers/Cloud Connectors. For example, with four Controllers (two primary and two backups), a grouping might be:

```
(XDC-001.cdz.lan XDC-002.cdz.lan)(XDC-003.cdz.lan XDC-004.cdz.lan)
```

In this example, the Controllers in the first group (001 and 002) are processed first. If both fail, Controllers in the second group (003 and 004) are processed.

For XenDesktop 7.0 or higher, there is an extra step you need to perform to use **Registration Groups** feature. You need to **Prohibit** the **Enable Auto Update of Controller** policy from Studio.

ListOfSIDs

The list of Controllers that a VDA can contact for registration is the `ListofDDCs`. A VDA must also know which Controllers to trust because VDAs do not automatically trust the Controllers in the `ListofDDCs`. The `ListofSIDs` (Security IDs) identify the trusted Controllers. VDAs attempt to register only with trusted Controllers.

In most environments, the `ListofSIDs` is generated automatically from the `ListofDDCs`. You can use a CDF trace to read the `ListofSIDs`.

Generally, there is no need to manually modify the `ListofSIDs`. There are several exceptions. The first two exceptions are no longer valid because newer technologies are available.

- **Separate roles for Controllers:** Before zones were introduced in XenApp and XenDesktop 7.7, the `ListofSIDs` was manually configured when only a subset of Controllers was used for registration. For example, if you were using XDC-001 and XDC-002 as XML brokers, and XDC-003 and XDC-004 for VDA registration, you specified all Controllers in the `ListofSIDs`, and XDC-003 and XDC-004 in the `ListofDDCs`. This is not a typical or recommended configuration. Do not use it in newer environments. Instead, use zones.
- **Reducing Active Directory load:** Before the auto-update feature was introduced in XenApp and XenDesktop 7.6, the `ListofSIDs` was used to reduce the load on domain controllers. By

© 1997–2026 Citrix Systems, Inc. All rights reserved.

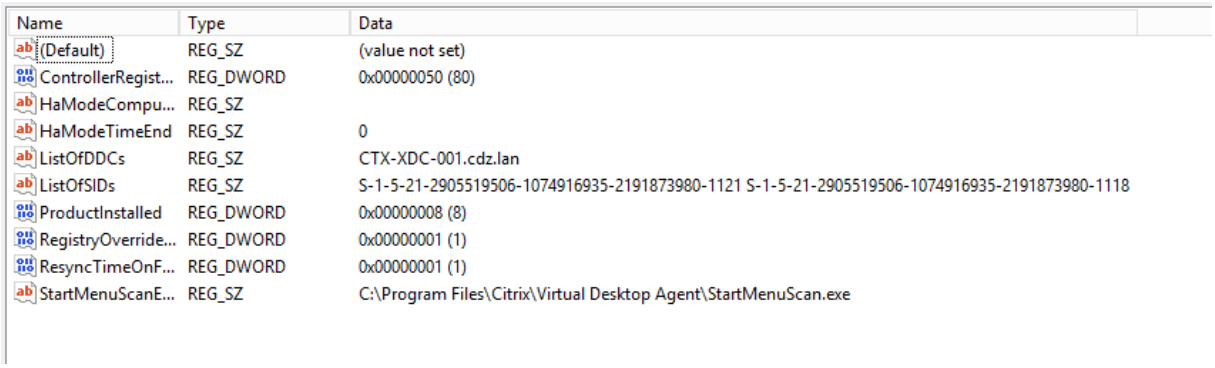
pre-populating the `ListofSIDs`, the resolution from DNS names to SIDs can be skipped. However, the auto-update feature removes the need for this work, because this persistent cache contains SIDs. Citrix recommends keeping the auto-update feature enabled.

- **Security:** In some highly secured environments, the SIDs of trusted Controllers were manually configured to avoid possible security threats from a compromised DNS server. However, if you do this, you must also disable the auto-update feature. Otherwise, the configuration from a persistent cache is used.

So, unless you have a specific reason, do not modify the `ListofSIDs`.

If you must modify the `ListofSIDs`, create a registry key named `ListOfSIDs` (`REG_SZ`) under `HKLM\Software\Citrix\VirtualDesktopAgent`. The value is a list of trusted SIDs, separated by spaces if you have more than one.

In the following example, one Controller is used for VDA registration (`ListofDDCs`), but two Controllers are used for brokering (List OfSIDs).



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

Controller search during VDA registration

When a VDA tries to register, the Broker Agent first performs a DNS lookup in the local domain to ensure that the specified Controller can be reached.

If that initial lookup doesn't find the Controller, the Broker Agent can start a fallback top-down query in AD. That query searches all domains, and repeats frequently. If the Controller address is invalid (for example, the administrator entered an incorrect FQDN when installing the VDA), that query's activity can potentially lead to a distributed denial of service (DDoS) condition on the domain controller.

The following registry key controls whether the Broker Agent uses the fallback top-down query when it cannot locate a Controller during the initial search.

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- Name: `DisableDdcWildcardNameLookup`
- Type: `DWORD`
- Value: `0` (default) or any non-zero value

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When set to `0`, the fallback search is enabled. If the initial search for the Controller fails, the fallback top-down search is started. This is the default behavior. However, if set to any non-zero value, the fallback search is disabled. If the initial search for the Controller fails, the Broker Agent stops looking.

LDAP binding sequencing during VDA registration using a read-only domain controller

When a VDA registers with a read-only domain controller (RODC), the Broker Agent must select which Light Directory Access Protocol (LDAP) binding or bindings to ignore. To make this selection, the Broker Agent requires a suitable registry key.

If a registry key is not provided, or the registry key field is empty, VDA registration with the RODC takes longer because it is required to go through the original LDAP binding sequence.

To modify the LDAP binding sequence, the registry key `ListofIgnoredBindings` has been added to `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`. Use of `ListofIgnoredBindings` lets you modify the LDAP binding sequence as necessary, and thereby speed up VDA registration with a RODC.

- Name: `ListofIgnoredBindings`
- Type: `REG_SZ`
- Values: `DefaultPath`, `DomainPath`, `PDCPath`

The value is a list of binding path options, each separated by a comma. The registry key ignores values that it does not recognize as valid.

Troubleshoot VDA registration issues

As noted previously, a VDA must be registered with a Delivery Controller or Cloud Connector to be considered when launching brokered sessions. Unregistered VDAs can result in underutilization of otherwise available resources. There are various reasons a VDA might not be registered, many of which an administrator can troubleshoot. Studio provides troubleshooting information in the catalog creation wizard, and after you create a Delivery Group.

- **Identifying issues during machine catalog creation:** 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 was not obtained about a machine (perhaps because it had never registered), you might choose to add the machine anyway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A catalog's functional level controls which product features are available to machines in the catalog. Using features introduced in new product versions might require a new VDA. Setting a functional level makes all features introduced in that version (and later, if the functional level does not change) available to machines in the catalog. However, machines in that catalog with an earlier VDA version will not be able to register.

- **Identifying issues after creating Delivery Groups:** After you create a Delivery Group, Studio displays details about machines associated with that group.

  The details pane for a Delivery Group indicates the number of machines that must be registered but are not. In other words, there might be one or more machines that are powered on and not in maintenance mode, but are not currently registered with a Controller. When viewing a "not registered, but must be"machine, review the **Troubleshoot** tab in the details pane for possible causes and recommended corrective actions.

More information about troubleshooting VDA registration

- For more information about functional levels, see VDA versions and functional levels.
- For more information about VDA registration troubleshooting, see CTX136668.
- You can also use Citrix Scout health checks to troubleshoot VDA registration and session launch. For details, see About health checks.

Virtual IP and virtual loopback

September 6, 2025

> **Important:**
>
> - Windows 10 Enterprise multi-session doesn't support Remote Desktop IP Virtualization (Virtual IP) and we don't support Remote Desktop IP Virtualization or virtual loopback on Windows 10 Enterprise multi-session.
> - Remote Desktop IP Virtualization (Virtual IP) isn't supported on cloud-hosted machines. For more information, see Microsoft documentation.

Remote Desktop IP Virtualization and virtual loopback features are supported on Windows Server 2016, Windows Server 2019, and Windows Server 2022 machines. These features do not apply to Windows desktop OS machines.

The Microsoft Remote Desktop IP Virtualization address feature provides a published application with a unique dynamically assigned IP address for each session. With the Citrix virtual loopback feature,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.*).

Certain applications, such as CRM and Computer Telephony Integration (CTI), use an IP address for addressing, licensing, identification, or other purposes that require a unique IP address or loopback address. Other applications might bind to a static port, so attempts to launch additional instances of an application in a multiuser environment fail because the port is in use. For such applications to function correctly in a Citrix Virtual Apps™ environment, a unique IP address is required for each device.

Remote Desktop IP Virtualization and virtual loopback are features independent of each other. You can use either or both.

Administrator action synopsis:

- To use Microsoft Remote Desktop IP Virtualization, enable and configure it on the Windows server. (Citrix® policy settings aren't needed.)
- To use Citrix virtual loopback, configure two settings in a Citrix policy.

Remote Desktop IP Virtualization (Virtual IP)

When Remote Desktop IP Virtualization 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 that they access any other published application. A process requires Remote Desktop IP Virtualization 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 Remote Desktop IP Virtualization addresses:

1. Obtain the **TCPView** tool from Microsoft. This tool lists all applications that bind specific IP addresses and ports. For more information on TCPView, see Microsoft documentation.
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 the application opens 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 another instance of the application.

How Microsoft Remote Desktop (RD) IP virtualization works

- Virtual IP addressing must be enabled on the Microsoft server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. For more information on configuring Remote Desktop IP Virtualization, see Microsoft documentation.

- After enabling the feature, at session startup, 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: `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 correct IP address to 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. 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 a Windows policy controls), if the local host IP address is requested, Remote Desktop IP Virtualization looks at the returned IP address and changes it to the Remote Desktop IP Virtualization address of the session. Applications that attempt to get the IP address of the local server through such name functions see only the unique Remote Desktop IP Virtualization 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 can't launch more than one instance of the application. The Remote Desktop IP Virtualization address feature also looks for 0.0.0.0 in these call types. It changes the call to listen on the specific Remote Desktop IP Virtualization address, which enables more than one application to listen on the same port on the same computer because they're all listening on different addresses. The call is changed only if it is in an ICA session and the Remote Desktop IP Virtualization 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're bound to VIPAddress1:9000 and VIPAddress2:9000 and there's no conflict.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual loopback

Enabling the **Citrix Remote Desktop IP Virtualization 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

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.
- Virtual IP loopback port exclusion. When an application calls the loopback address on the ports specified in this setting, virtual loopback does not change the call to the session-specific loopback address.

Related feature

You can use the following registry settings to ensure that virtual loopback is given preference over virtual IP. This feature is called preferred loopback. However, proceed with caution:

- Use preferred loopback only if both Virtual IP and virtual loopback are enabled. Otherwise, you might have unintended results.
- Editing the registry incorrectly can cause serious problems that may 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 the 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Name: PreferLoopback, Type: REG_DWORD, Data: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <list of processes>

Zones

February 23, 2026

> **Note:**
>
> You can manage your Citrix Virtual Apps and Desktops™ deployment using two management consoles: Web Studio (web-based) and Citrix Studio (Windows-based). This article covers only Web Studio. For information about Citrix Studio, see the equivalent article in Citrix Virtual Apps and Desktops 7 2212 or earlier.

Deployments that span widely dispersed locations connected by a WAN can face challenges due to network latency and reliability. There are two options that mitigate those challenges:

- Deploy multiple sites, each with their own SQL Server site database.

  This option is recommended for large enterprise deployments. Multiple sites are managed separately, and each requires its own SQL Server site database. Each site is a separate Citrix Virtual Apps™ deployment.

- Configure multiple zones within a single site.

  Configuring zones can help users in remote regions connect to resources without necessarily forcing their connections to traverse large segments of the WAN. Using zones allows effective site management from a single Web Studio console, Citrix Director, and the site database. This saves the costs of deploying, staffing, licensing, and operating more sites containing separate databases in remote locations.

  Zones can be helpful in deployments of all sizes. You can use zones to keep applications and desktops closer to end users, which improves performance. A zone can have one or more Controllers installed locally for redundancy and resiliency, but it is not required.

  The number of Controllers configured in the site can affect the performance of some operations, such as adding new Controllers to the site itself. To avoid this, we recommend that you limit the number of zones in your Citrix Virtual Apps or Citrix Virtual Desktops™ site to no more than 50.

  When the network latency of your zones is more than 250 ms RTT, we recommend that you deploy multiple sites instead of zones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Throughout this article the term local refers to the zone being discussed. For example, "A VDA registers with a local Controller"means that a VDA registers with a Controller in the zone where the VDA is located.

Zones in this release are similar, but not identical to zones in XenApp version 6.5 and earlier. For example, in this implementation of zones, there are no data collectors. All Controllers in the site communicate with one site database in the primary zone. Also, failover and preferred zones work differently in this release.

Zone types

A site always has one primary zone. It can also optionally have one or more satellite zones. Satellite zones can be used for disaster recovery, geographically distant data centers, branch offices, a cloud, or an availability zone in a cloud.

Primary zone:

The primary zone has the default name "Primary". This zone contains the SQL Server site database (and high availability SQL servers, if used), Web Studio, Director, Citrix StoreFront™, Citrix License Server, and Citrix Gateway. Always keep the site database in the primary zone.

The primary zone should have at least two Controllers for redundancy. The primary zone can have VDAs with applications that are tightly coupled with the database and infrastructure.

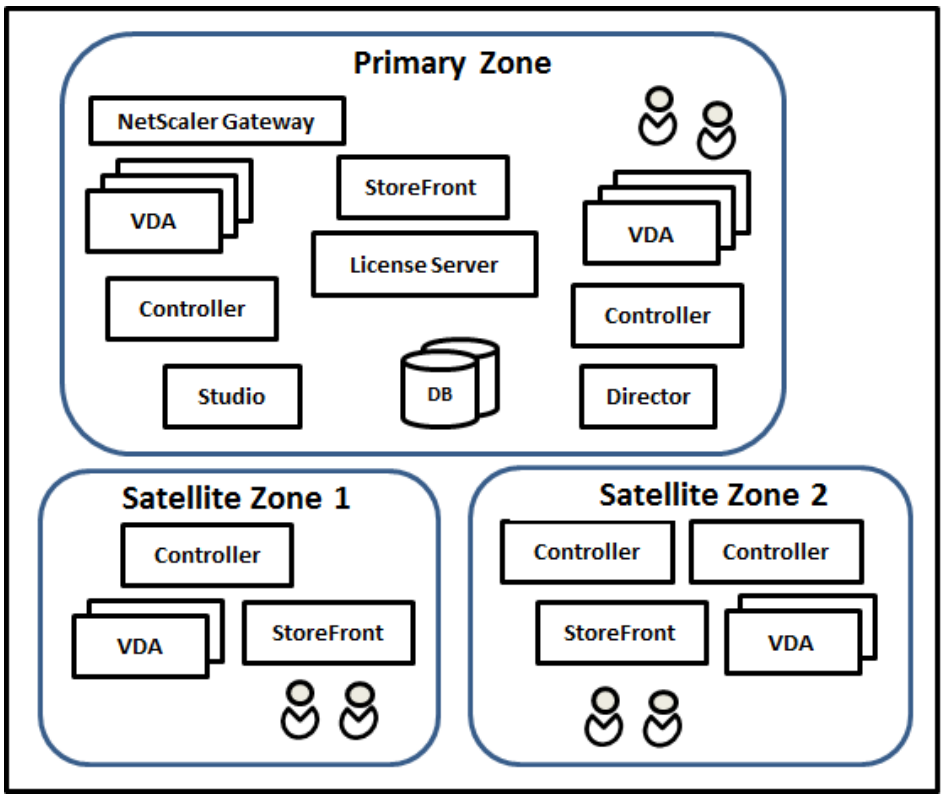
Satellite zone:

A satellite zone contains one or more VDAs, Controllers, StoreFront servers, and Citrix Gateway servers. Under normal operations, Controllers in a satellite zone communicate directly with the database in the primary zone.

A satellite zone, particularly a large one, might also contain a hypervisor that is used to provision and store machines for that zone. When you configure a satellite zone, you can associate a hypervisor or other service connection with it. (Be sure any catalogs that use that connection are in the same zone.)

A site can have satellite zones of different configurations, based on your unique needs and environment. The following figure illustrates a primary zone and examples of satellite zones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In the illustration:

- **Primary zone:** Contains two Controllers, Web Studio, Director, StoreFront, License Server, and the site database (plus high availability SQL Server deployments). The Primary zone also contains several VDAs and a Citrix Gateway.
- **Satellite zone 1: VDAs with Controller:** Satellite zone 1 contains a Controller, VDAs, and a StoreFront server. VDAs in this satellite zone register with the local Controller. The local Controller communicates with the site database and license server in the primary zone.

  If the WAN fails, the Local Host Cache feature allows the Controller in the satellite zone to continue brokering connections to VDAs in that zone. Such a deployment can be effective in an office where workers use a local StoreFront site and the local Controller to access their local resources.
- **Satellite zone 2: VDAs with redundant Controllers:** Satellite zone 2 contains two Controllers, VDAs, and a StoreFront server. This is the most resilient zone type, offering protection against a simultaneous failure of the WAN and one of the local Controllers.

Where VDAs register and where Controllers fail over

In a site containing primary and satellite zones, with VDAs at minimum version 7.7:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A VDA in the primary zone registers with a Controller in the primary zone. A VDA in the primary zone never attempts to register with a Controller in a satellite zone.
- A VDA in a satellite zone registers with a local Controller, if possible. (This is considered the preferred Controller.) If no local Controllers are available (for example, because they cannot accept more VDA registrations or they have failed), the VDA will attempt to register with a Controller in the primary zone. In this case, the VDA stays registered in the primary zone, even if a Controller in a satellite zone becomes available again. A VDA in a satellite zone never attempts to register with a Controller in another satellite zone.
- When auto-update is enabled for VDA discovery of Controllers, and you specify a list of Controller addresses during VDA installation, a Controller is randomly selected from that list for initial registration (regardless of which zone the Controller resides in). After the machine with that VDA is restarted, the VDA will start to prefer registering with a Controller in its local zone.
- If a Controller in a satellite zone fails, it fails over to another local Controller, if possible. If no local Controllers are available, it fails over to a Controller in the primary zone.
- If you move a Controller in or out of a zone, and auto-update is enabled, VDAs in both zones receive updated lists indicating which Controllers are local and which are in the primary zone, so they know with whom they can register and accept connections from.
- If you move a catalog to another zone, the VDAs in that catalog re-register with Controllers in the zone where you moved the catalog. (When you move a catalog to another zone, make sure this zone and the zone with the associated host connection are well connected. If there is limited bandwidth or high-latency, move the host connection to the same zone containing the associated machine catalog.)

If all Controllers in the primary zone fail:

- Web Studio cannot connect to the site.
- Connections to VDAs in the primary zone cannot be made.
- Site performance degrades until the Controllers in the primary zone become available.

For sites containing VDA versions earlier than 7.7:

- A VDA in a satellite zone accepts requests from Controllers in their local zone and the primary zone. (VDAs at minimum version 7.7 can accept Controller requests from other satellite zones.)
- A VDA in a satellite zone registers with a Controller in the primary zone or the local zone at random. (VDAs at minimum version 7.7 prefer the local zone.)

Zone preference

To use the zone preference feature, you must be using minimum StoreFront 3.7 and Citrix Gateway 11.0-65.x.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

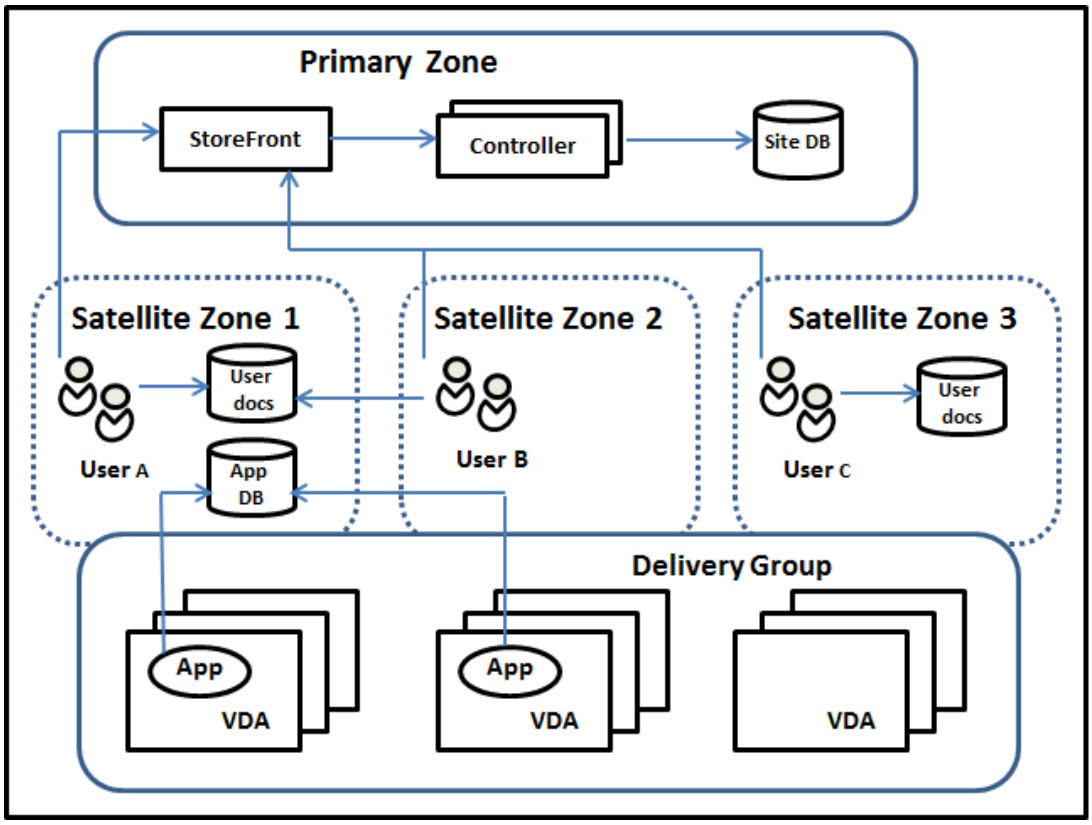
In a multi-zone site, the zone preference feature offers the administrator more flexibility to control which VDA is used to launch an application or desktop.

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.

The following graphic shows an example multi-zone configuration.



In this example, VDAs are spread among three satellite zones, but they are all in the same Delivery Group. Therefore, the broker might have a choice which VDA to use for a user launch request. This example indicates there are several locations where users can be running their Citrix Workspace app endpoints:

- User A is using a device with Citrix Workspace app in satellite zone 1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- User B is using a device in satellite zone 2.
- A user's documents can be stored in various locations.
    - Users A and B use a share based in satellite zone 1.
    - User C uses a share from satellite zone C.
    - One of the published applications uses a database located in satellite zone 1.

You associate a user or application with a zone by configuring a home zone for the user or application. The broker in the Delivery Controller™ then uses those associations to help select the zone where a session will be launched, if resources are available. You can:

- 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 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; see the "Other considerations" section. However, even in this case, the broker uses only one home zone.)

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. You can restrict the sequence; see Tailoring zone preference. 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 has a configured zone association (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 used.

- **Mandatory user home zone use:** In a Delivery Group, you can specify that a sessions launch in the user's home zone (if configured), with no failover to another zone if the home zone doesn't have available resources. This restriction is helpful when you must avoid the risk of copying large profiles or data files between zones. In other words, you would rather deny a session launch than to launch the session in a different zone.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Mandatory application home zone use:** Similarly, when you configure a home zone for an application, you can indicate that the application be launched 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 indicate that no configured user zones be considered when launching that application. For example, you might prefer that users run an application on a VDA near their device, using the user location zone preference, 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.

If the user launching an application or desktop already has a session that is suitable for the resource being launched (for example, that can use session sharing for an application, or a session that is already running the resource being launched), but that session is running on a VDA in a zone other than the preferred zone for the user/application, then the system might create a new session. This 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 zone other than the preferred zone.
3. Start a new session in the preferred zone.
4. Reconnect to a connected existing session in a zone other than the preferred zone.
5. Start a new session in a zone other than the 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the user has multiple different zone associations acquired solely through group membership, the broker chooses among the zones randomly. Once 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 Gateway must be configured to associate ranges of IP addresses with particular zones, and discovered zone identity must be passed through StoreFront to the Controller.

For more information about zone preference, see Zone preference internals.

Considerations, requirements, and best practice

- You can place the following items in a zone: Controllers, machine catalogs, host connections, users, and applications. If a catalog uses a host connection, be sure the catalog and the connection are in the same zone. (However, with a low-latency high-bandwidth connection available, they can be in different zones.)
- When you place items in a satellite zone it affects how the site interacts with them and with other objects related to them.
    - When Controllers are placed into a satellite zone, it is assumed that those machines have good (local) connectivity to hypervisors and VDAs in the same zone. Controllers in that satellite zone are then used in preference to Controllers in the primary zone for handling those hypervisors and VDA machines.
    - When a hypervisor connection is placed into a satellite zone, it is assumed that all the hypervisors managed via that hypervisor connection also reside in that satellite zone. Controllers in that satellite zone are then used in preference to Controllers in the primary zone when communicating with that hypervisor connection.
    - When a machine catalog is placed into a satellite zone, it is assumed that all the VDA machines in that catalog are in the satellite zone. Local Controllers are used in preference to Controllers in the primary zone when attempting to register with the site, after the Controller list auto-update mechanism has activated after the first registration of each VDA.
    - Citrix Gateway instances can also be associated with zones. This is done as part of the StoreFront Optimal HDX™ Routing configuration rather than, as for the other elements described here, as part of the site configuration. When a Citrix Gateway is associated with a zone, it is preferred to be used when HDX connections to VDA machines in that zone are used.
- When you create a production site and then create the first catalog and Delivery Group, all items are in the primary zone –you cannot create satellite zones until after you complete that initial

© 1997–2026 Citrix Systems, Inc. All rights reserved.

setup. (If you create an empty site, the primary zone will initially contain only a Controller. You can create satellite zones before or after creating a catalog and Delivery Group.)

- When you create the first satellite zone containing one or more items, all other items in your site remain in the primary zone.
- The primary zone is named 'Primary' by default; you can change that name. Although Web Studio indicates which zone is the primary zone, it is best practice to use an easily identifiable name for the primary zone. You can reassign the primary zone (that is, make another zone the primary zone), but it should always contain the site database and any high availability servers.
- Always keep the site database in the primary zone.
- After you create a zone, you can later move items from one zone to another. This flexibility allows you to potentially separate 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. Consider potential unintended effects before moving items between zones. Keep a catalog and the host connection it uses in the same zone, or in zones which are well connected (for example, via a low-latency and high-bandwidth network).
- For optimal performance, install Web Studio and Director only in the primary zone. You can access Web Studio and Director from a satellite zone (for example, a satellite zone containing Controllers to use as failover if the primary zone becomes inaccessible) because they are web application.
- Ideally, Citrix Gateway in a satellite zone is used for user connections coming into that zone from other zones or external locations, although you can use it for connections within the zone.
- Remember: To use the zone preference feature, you must be using minimum StoreFront 3.7 and Citrix Gateway 11.0-65.x.

Connection quality limits

The Controllers in the satellite zone perform SQL interactions directly with the site database. This imposes some limits on the quality of the link between the satellite zone and the primary zone containing the site database. The specific limits are relative to the number of VDAs and user sessions on those VDAs that are deployed in the satellite zone. So satellite zones with only a few VDAs and sessions can function with a poorer-quality connection to the database than satellite zones with large numbers of VDAs and sessions.

For more information, see Latency and SQL Blocking Query Improvements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The impact of latency on brokering performance

Although zones allow users to be on higher-latency links, providing that there is a local broker, the additional latency inevitably impacts end-user experience. For most work that users do, they experience slowness caused by round trips between Controllers in the satellite zone and the site database.

For launching applications, extra delays occur while the session brokering process identifies suitable VDAs to send session launch requests to.

Create and manage zones

A Full Administrator can perform all zone creation and management tasks. However, you can also create a custom role that allows you to create, edit, or delete a zone. 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 catalog from one zone to another, you must have edit permission for that catalog. For more information, see Delegated administration.

If you use Citrix Provisioning™: The Citrix Provisioning console is not aware of zones, so we recommend using Web Studio to create catalogs for satellite zones. Create the catalog in Web Studio, specifying the correct satellite zone. Then use the Citrix Provisioning console to provision machines in that catalog. (If you create the catalog using the Citrix Provisioning wizard, the catalog is placed in the primary zone. You must use Web Studio to move it to the satellite zone later.)

Create a zone

1. Sign in to Web Studio.
2. Select **Zones** in the left pane.
3. Select **Create Zone** in the action bar.
4. Enter a name for the zone, and a description (optional). The name must be unique within the site.
5. Select the items to place in the new zone. You can filter or search the list of items from which you can select. You can also create an empty zone; simply do not select any items.
6. Click **Save**.

As an alternative to this method, you can select one or more items in Web Studio and then select **Create Zone** in the action bar.

Change a zone name or description

1. Sign in to Web Studio.
2. Select **Zones** in the left pane.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select a zone in the middle pane and then select **Edit Zone** in the action bar.
4. Change the zone name, description, or both. If you change the name of the primary zone, make sure the zone remains easily identifiable as the primary zone.
5. Click **Save** or **Apply**.

Move items from one zone to another zone

1. Sign in to Web Studio.
2. Select **Zones** in the left pane.
3. Select a zone in the middle pane, and then select one or more items.
4. Drag the items to the destination zone or select **Move Items** in the action bar and then specify which zone to move them to.

A confirmation message lists the items you selected and asks if you are sure you want to move all of them.

Remember: When a catalog uses a host connection to a hypervisor or other service, place both the catalog and the connection in the same zone. Otherwise, performance can be affected. If you move one, move the other, too.

Delete a zone

A zone must be empty before it can be deleted. You cannot delete the primary zone.

1. Sign in to Web Studio.
2. Select **Zones** in the left pane.
3. Select a zone in the middle pane.
4. Select **Delete Zone** from the action bar. If the zone is not empty (it contains items), you are asked to choose the zone where those items will be moved.
5. Confirm the deletion.

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. Sign in to Web Studio.
2. Select **Zones** in the left pane, and then select a zone in the middle pane.
3. Select **Add Users to Zone** in the action bar.
4. In the **Add Users to Zone** dialog box, click **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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Yes = add only those users you specified who do not have a home zone; **No** = return to the user selection dialog.

5. Click **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. Sign in to Web Studio.
2. Select **Zones** in the left pane, and then select a zone in the middle pane.
3. Select **Remove Users from Zone** in the action bar.
4. In the **Add Users to Zone** dialog box, click **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 and application groups to which they belong.
5. 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, creating an Application 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 **Applications** in the left pane. Select an application and then select **Edit Application Properties** in the action bar.

On the **Zones** page of the application's properties/settings:

- If you want the application to have a home zone:
  - Select **Use the selected zone to decide** radio button and then select the zone.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 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 or user home zones are used to determine where to launch this application.

Other actions that include specifying zones

After you create at least one satellite zone, you can specify a zone when you add a host connection or create a catalog.

Usually, the primary zone is the default. When using Machine Creation Services™ to create a catalog, the zone that is configured for the host connection is automatically selected.

If the site contains no satellite zones, the primary zone is assumed and the zone selection box does not appear.

Remove broker user from the cache

August 20, 2025

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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Find if the user is assigned to an access policy: `Get-BrokerAccessPolicyRule`
- Find if the user is assigned to an application entitlement policy: `Get-BrokerAppEntitlementPol`
- Find if the user is assigned to a desktop entitlement policy: `Get-BrokerEntitlementPolicyRul`
- 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`
- 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
```

Citrix Assistant application (Preview)

September 6, 2025

Citrix Assistant app is a GUI tool designed to enable end-users to optimize their sessions across CPU, memory, networking, HDX™, and other performance factors. It offers a simple and convenient experience, often requiring just a single click to significantly improve session performance or do the troubleshooting.

Sessions can currently be optimized in the following areas:

- System Resources: CPU and memory optimization.
- Network: Network status checks and personalized recommendations.
- Applications: Display unresponsive applications and option to terminate them.
- Storage: Clean temporary files and identify files larger than 100 MB for deletion directly from the user interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Hardware diagnostics and troubleshooting:
  - Audio diagnostic and troubleshooting.
  - Camera device testing.

Installation and execution

The Citrix Assistant app is included with the Citrix Virtual Apps and Desktops ISO file. To install, download the ISO, then navigate to **Support > CitrixAssistantApp folder**. Open this folder, run `CitrixAssistant.exe`, and follow the on-screen prompts to complete the installation.

Log files

The log files for the Citrix Assistant app are stored in `USERPROFILE%\AppData\Local\Temp\citrix\AssistantApp\ctxasst.log`. Use the log file for troubleshooting.

Explore the UI

The app automatically detects your operating system's language variant and displays the app in that language.

The app features three main pages, accessible through the left pane:

- Home
- Apps
- Files

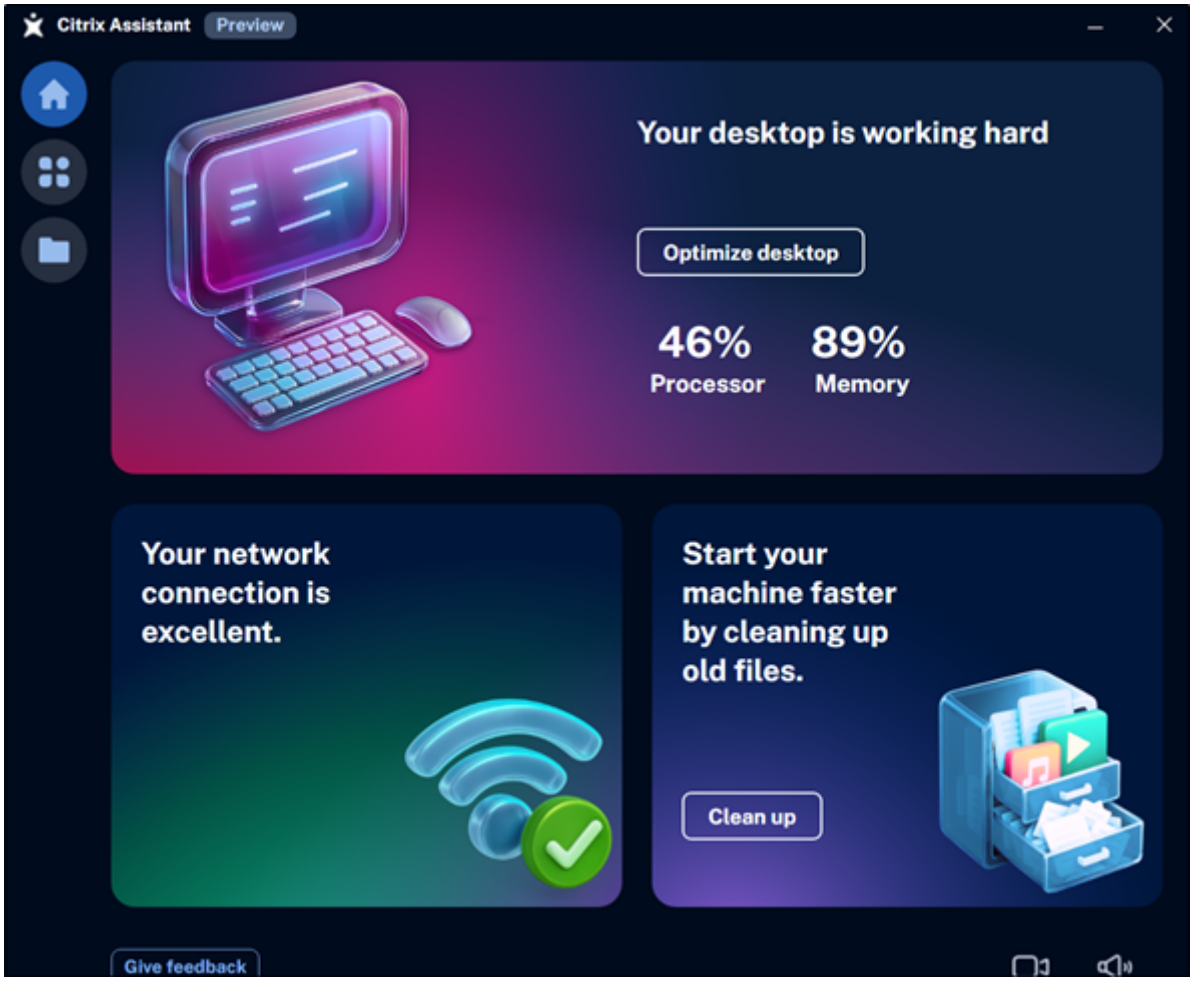
Sound and Camera settings are available in the bottom right corner.

Home page

The **Home** page provides the following functionalities:

> **Note:**
>
> Install the WEM agent on the VDA machine to enable **Optimize desktop** and **Clean up** buttons on the **Home** Page and to enable **Files** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

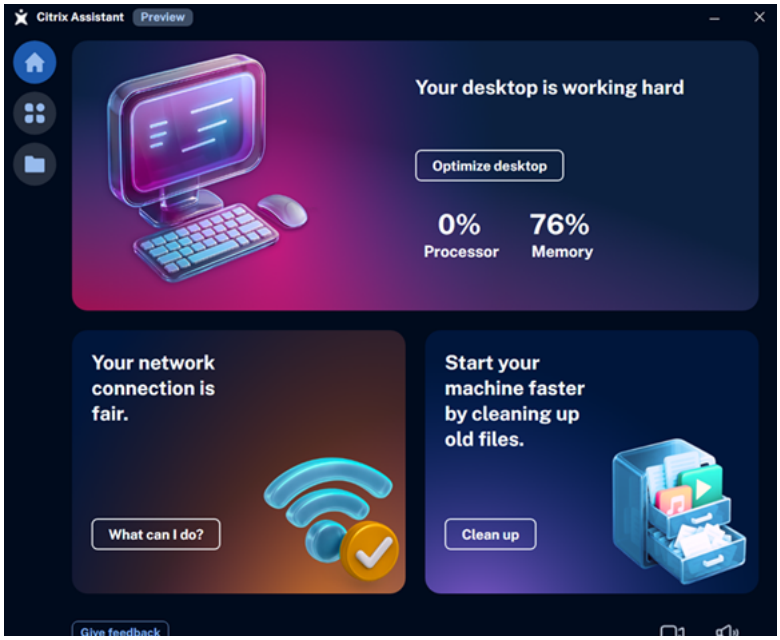


- *Optimize Desktop*: The Optimize feature enhances overall system performance by adjusting CPU priority for resource-intensive applications during periods of high CPU usage. It also reclaims memory from inactive applications to ensure efficient use of system resources. After you click **Optimize Desktop**, you might notice improved system performance.
- *Network Status*: This tile displays VDA network connection status. The network connection result is displayed, based on bandwidth and latency data. The connection status is categorized as excellent, fair, or poor. If the status is fair or poor, clicking **What can I do?** provides recommendations for improvement.

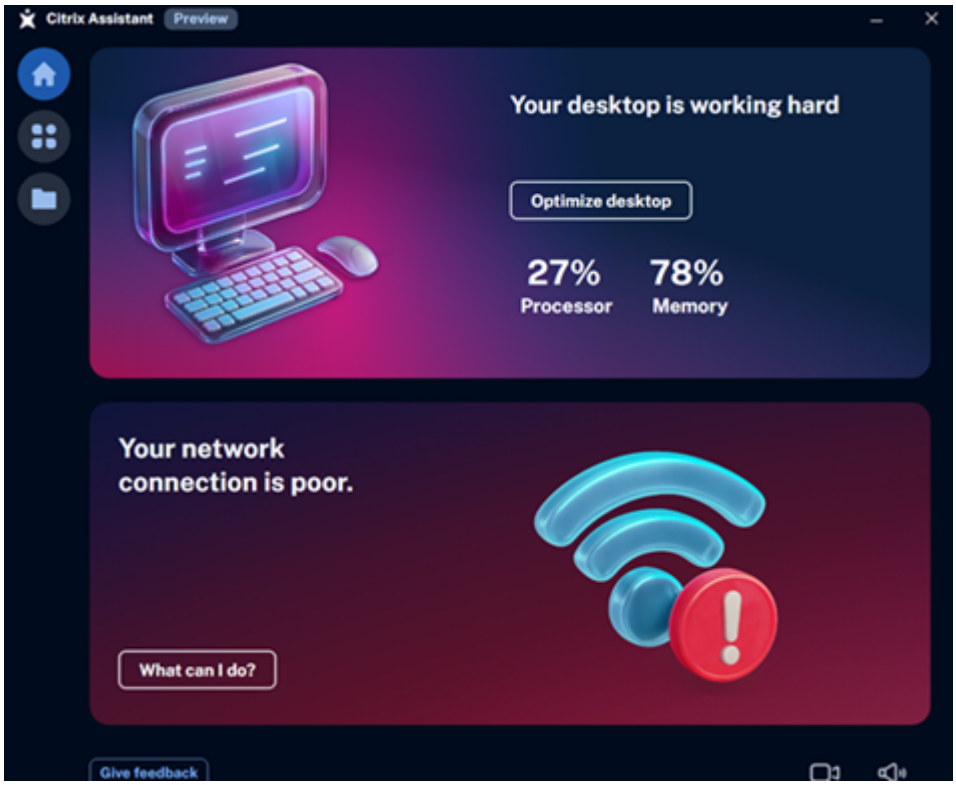
  > **Note:**
  >
  > The option to clean up files is unavailable when the connection is poor.

  Fair network connection

© 1997–2026 Citrix Systems, Inc. All rights reserved.

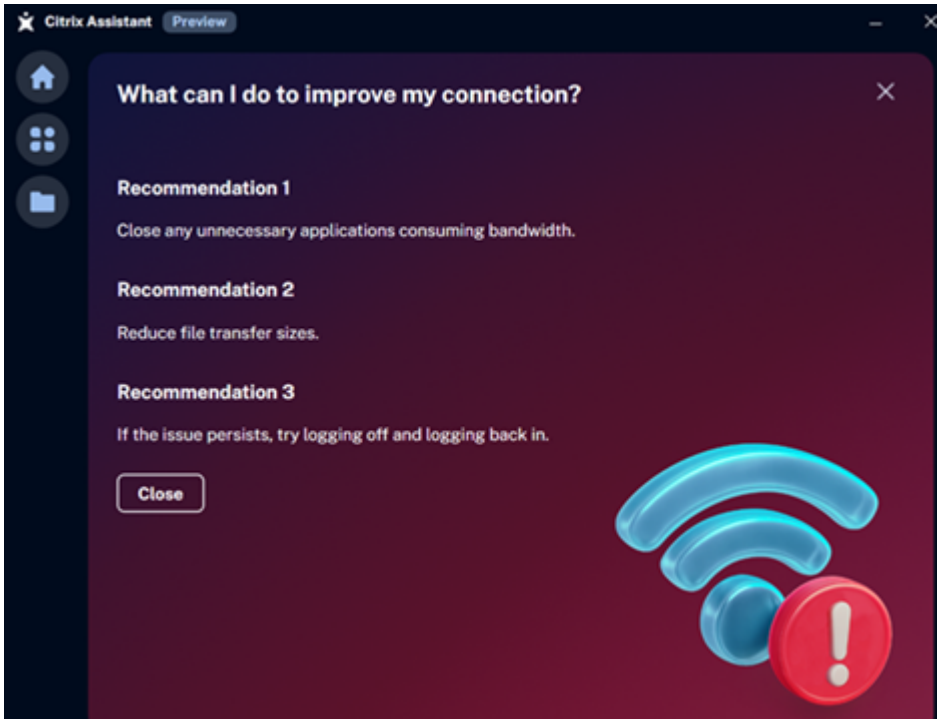


Poor network connection



Recommendation page

© 1997–2026 Citrix Systems, Inc. All rights reserved.

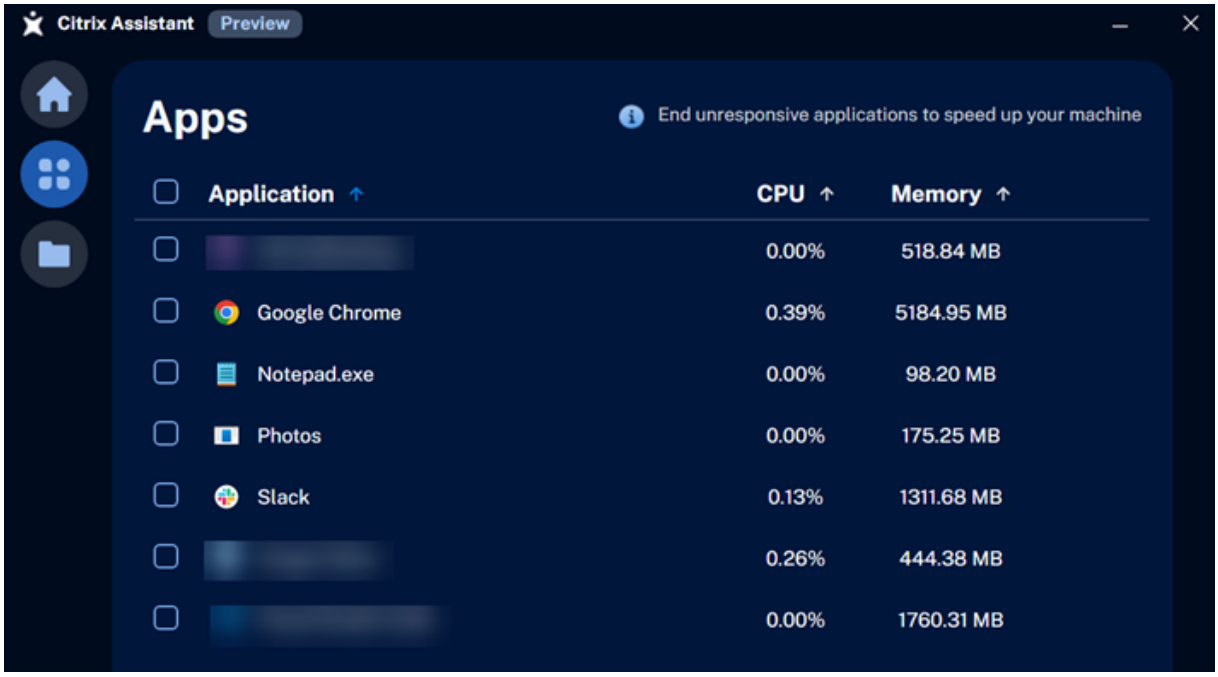


- *Clean Up*: This option provides information about your user profile and helps in cleaning up temporary or large files (larger than 100 MB). This action can significantly improve your machine's log-on time. Temporary files include crashed dump reports, application caches, and hidden files that contribute to a bulky profile. You can also access the Files page on the left pane to clean up files. For more information, see Files page.

Apps page

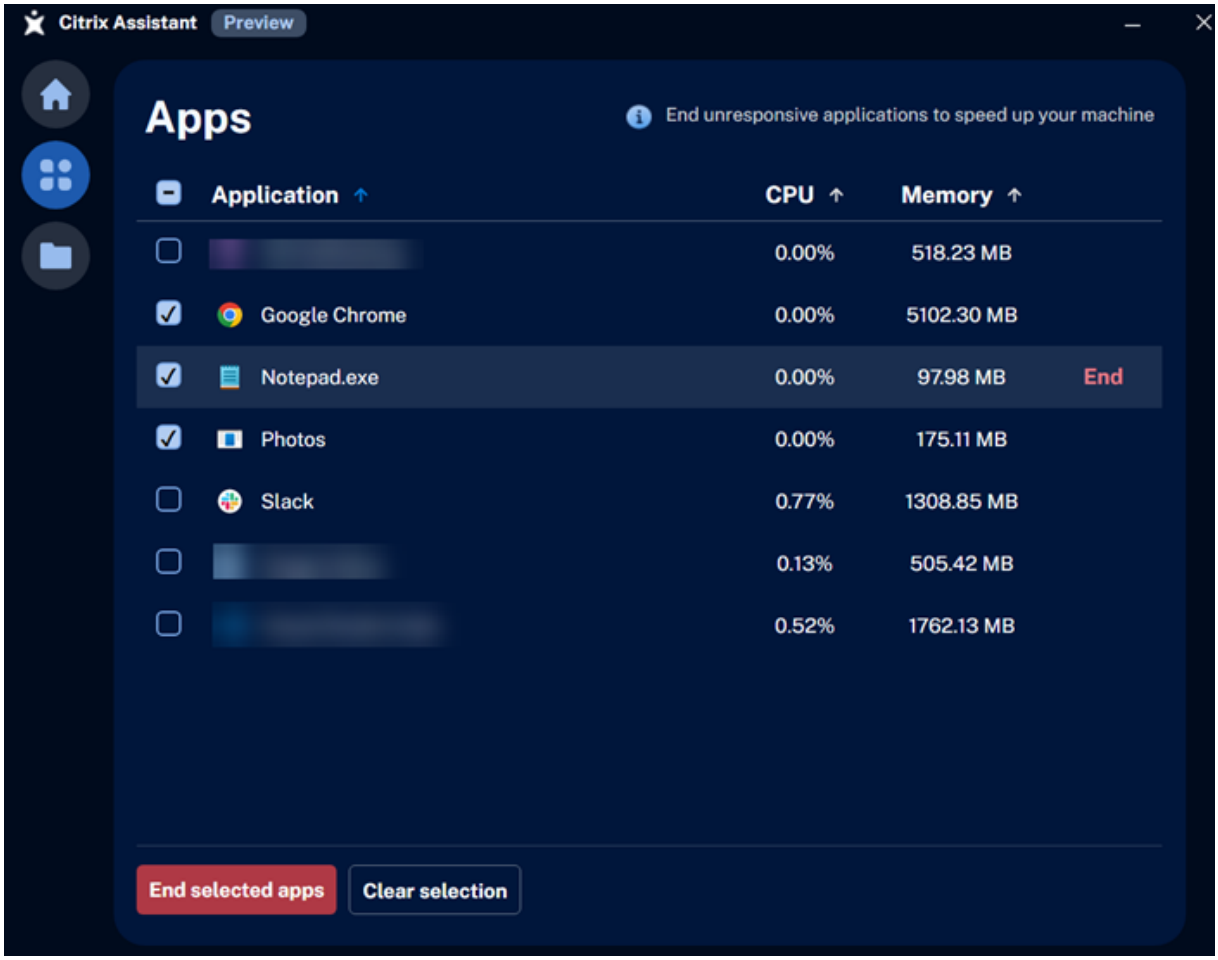
The **Apps** page displays all the unresponsive applications within the VDA session and options to terminate them. You can terminate single or multiple applications from this interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Terminate a single app: You can either hover over an app row to display the **End** button or select a checkbox and click **End selected apps**. Confirm the action when prompted.
- Terminate multiple apps: Select multiple applications at a time and click **End selected apps**. Confirm the action when prompted.

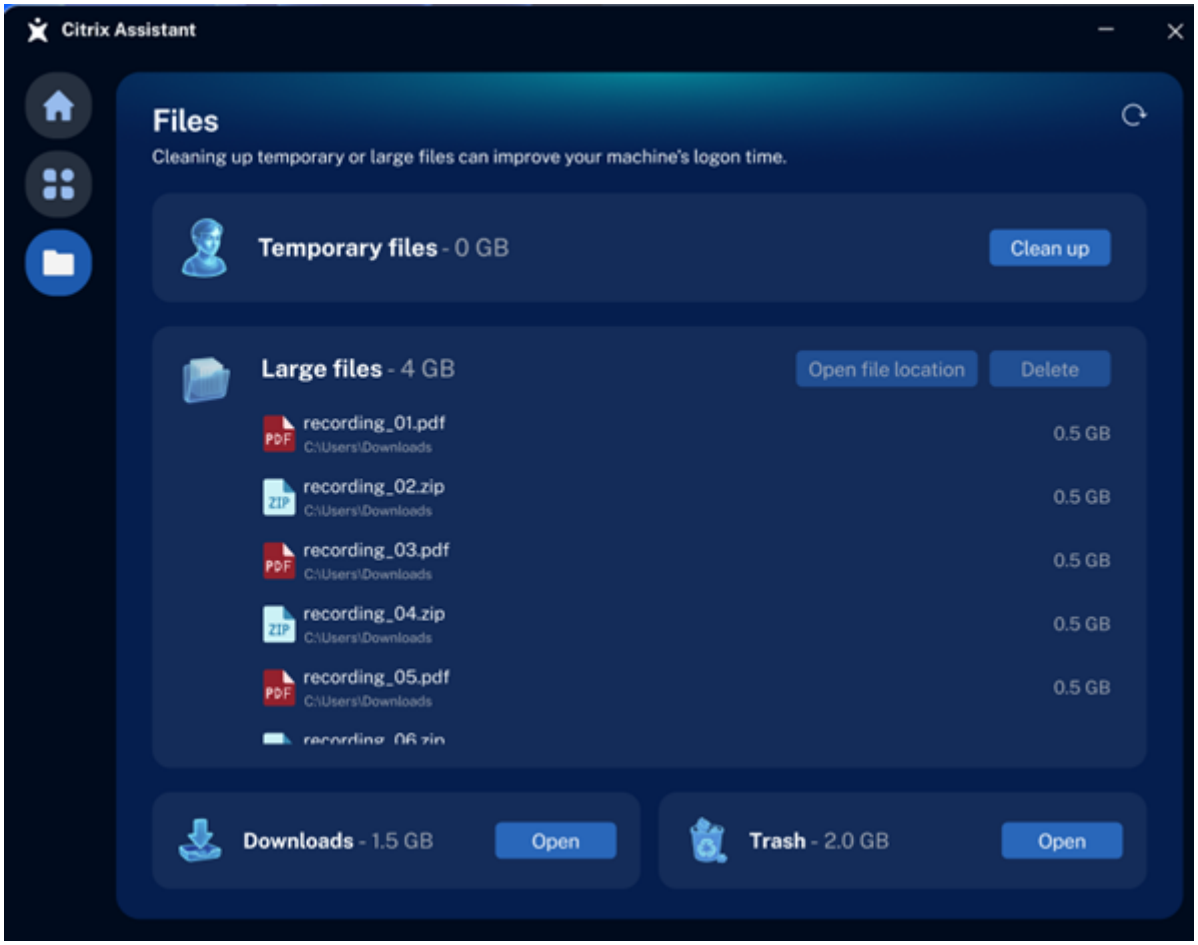
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Files page

The Files page provides information about your user profile and helps in cleaning up temporary or large files (larger than 100 MB). This action can significantly improve your machine's log-on time. Temporary files include crashed dump reports, application caches, and hidden files that contribute to a bulky profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



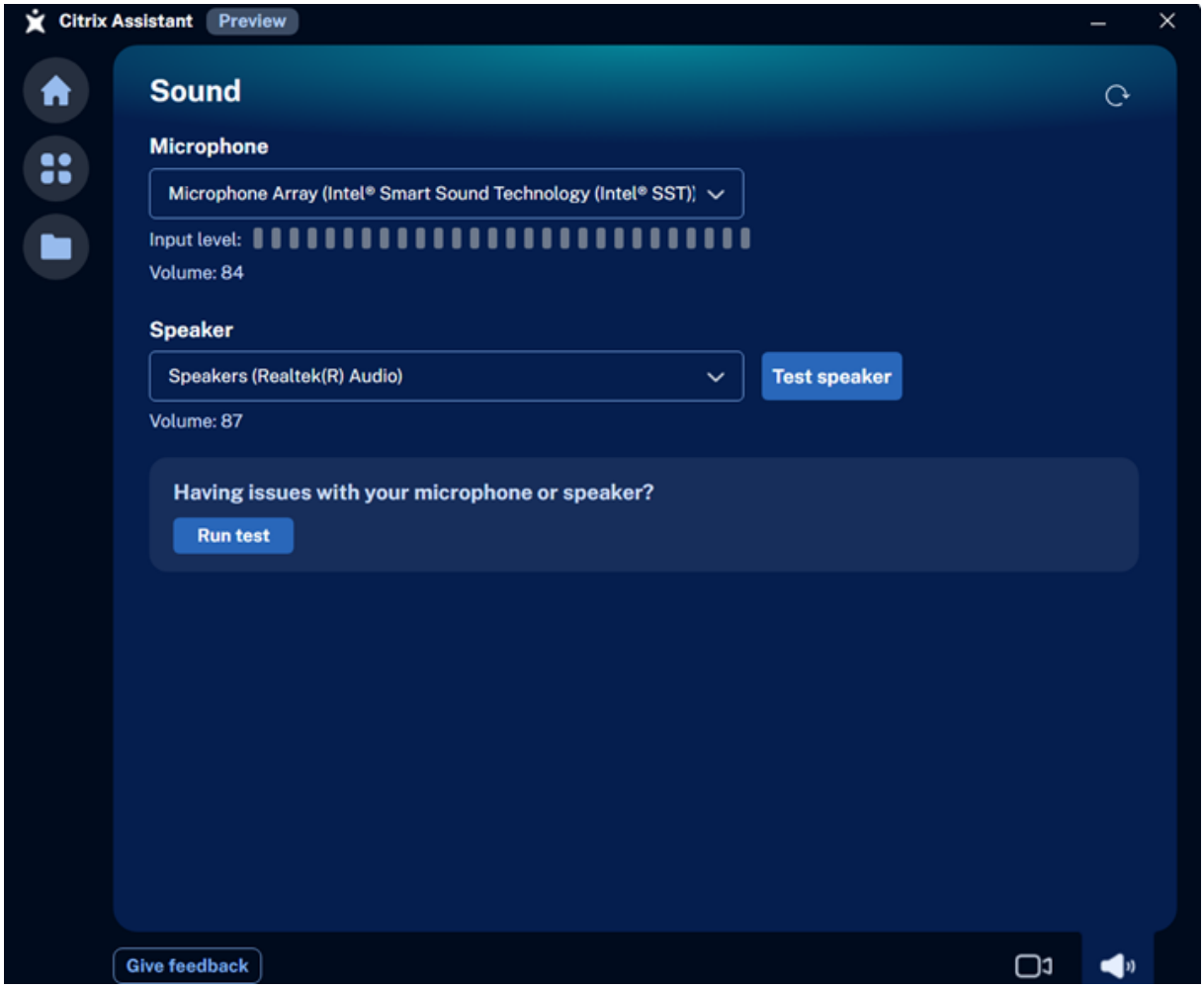
- Temporary files: Click **Clean up** to clean temporary files.
- Large files: You can either click **Delete** to remove the large files or click **Open file location** to go to their location and then decide on the appropriate action. You can use **Ctrl** key to select multiple files simultaneously.
- Downloads and Trash folder: Click **Open** to go to their location and then decide on the appropriate action.

To recalculate the data on the **Files** page, click the **Refresh** icon in the top-right corner of the app.

Sound page

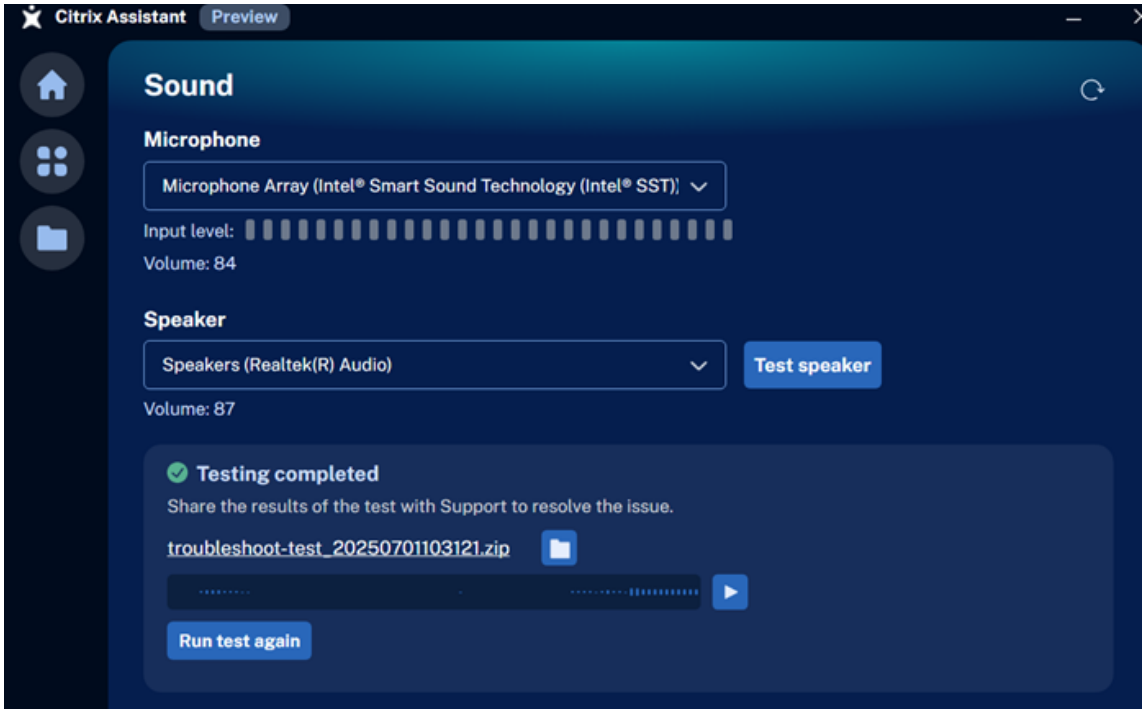
The Citrix Assistant app's sound page helps to diagnose and troubleshoot audio settings within a VDA session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- You can select a Microphone and Speaker from the drop-down list if you have multiple audio devices connected.
- Click **Test speaker** to test the selected speaker device by playing a demo audio.
- When troubleshooting audio device issues within a VDA session, click **Run test** and then the application records the sound input. This recording is then exported into a zip file. You can share the zip file with your IT or Citrix Admin team for assistance. You can also replay the audio to verify sound playback.

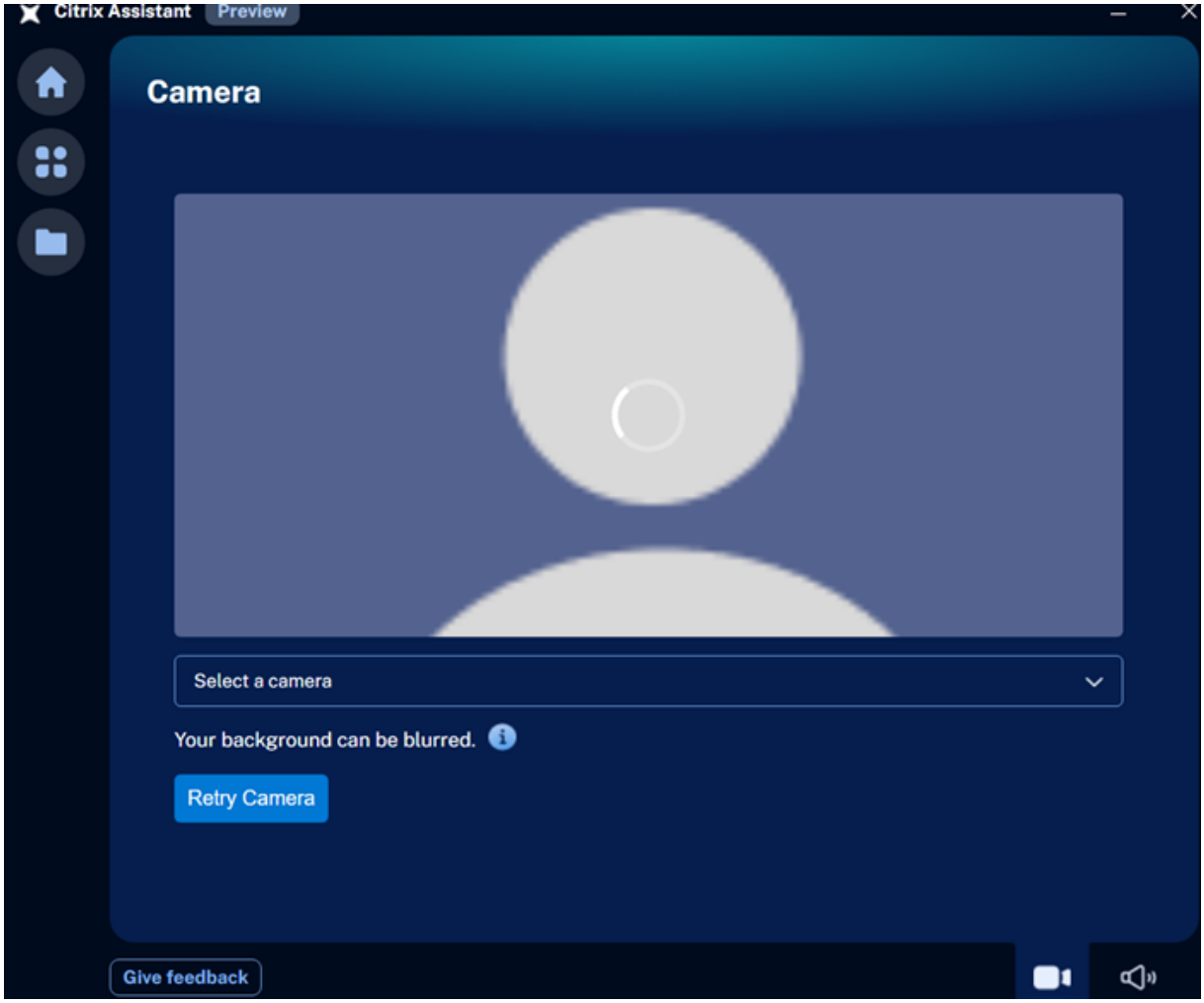
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Camera page

The Citrix Assistant app's camera page helps to configure video settings within a VDA session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- You can select a camera from the drop-down list if you have multiple cameras connected.

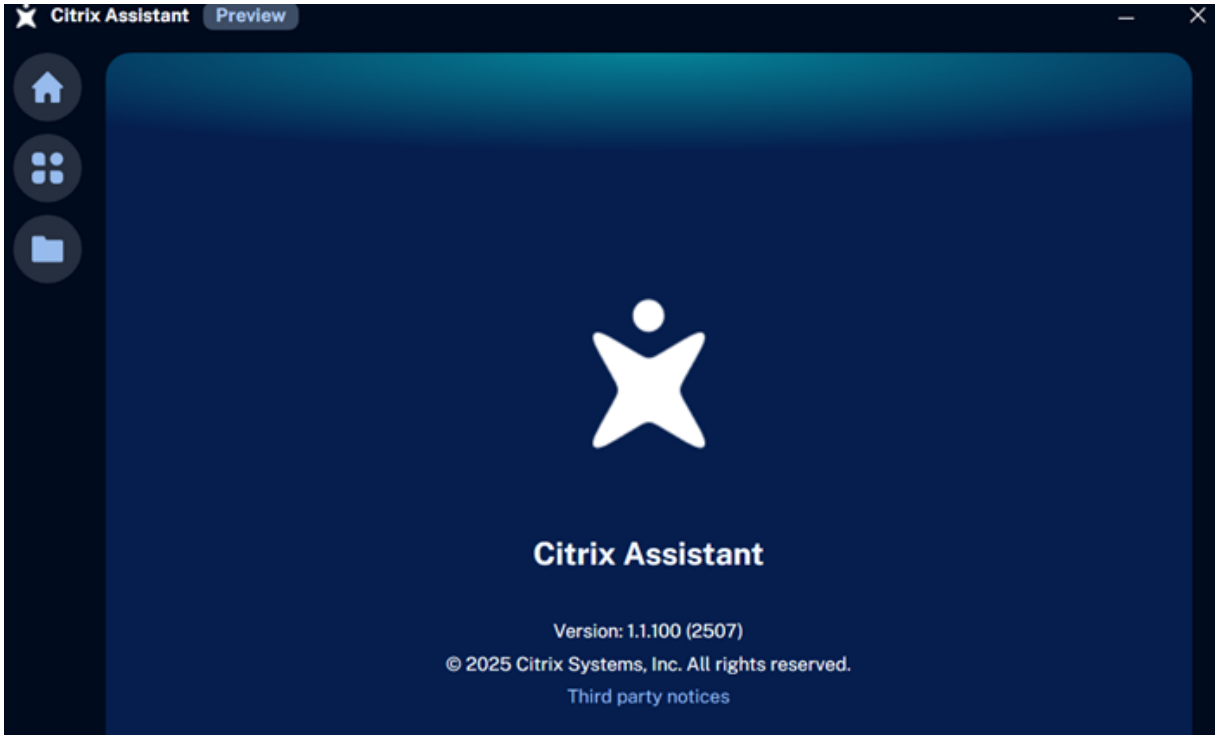
  > **Note:**
  >
  > If only **Citrix HDX Web Camera** is displayed and you have multiple camera devices connected on the CWA client, then reboot the VDA machine to see the list of all connected camera devices. Make sure to reboot only after you install the Citrix Assistant App.

- You can blur your background. To blur your background, navigate to **Citrix Workspace™ app > Preferences > Default webcam > Enable background blur**.
- To adjust your camera settings, click **Retry Camera**. However, make sure that the camera is not in use by other video conferencing tools.

About page

From the system tray, right-click the app icon to open the **About** page. The version information and the third-party license entry of the Citrix Assistant app is displayed on the **About** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Limitations

- **Optimize Desktop behavior**: The **Optimize Desktop** button currently reverts to its original state almost immediately after optimization. Future versions will provide detailed information about the optimization process and sustain the optimized state for a longer duration.
- **Camera and microphone access**: Citrix Assistant occasionally requests camera and microphone access, using the default framework notification.
- **Temporary file cleanup limitation**: The temporary files that are read-only, corrupted, or actively in use, can't be cleaned.
- **Undeletable large files**: Some large files that are read-only can't be deleted. Upcoming versions will include warning messages to inform users of this limitation.
- **Large file rendering time**: The **Large files** section might take a significant amount of time to display files. Efforts are underway to reduce the listing time for these files.

Monitor

September 13, 2025

Administrators and help desk personnel can monitor Citrix Virtual Apps and Desktops™ Sites using a variety of features and tools. Using these tools, you can monitor:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- User sessions and session use
- Logon performance
- Connections and machines, including failures
- Load evaluation
- Historical trends
- Infrastructure

Citrix Director

Director is a real-time web tool that you can use to monitor and troubleshoot, and to perform support tasks for end users.

For details, see the Director articles.

Configuration Logging

Configuration Logging allows administrators to keep track of administrative changes to a Site. Configuration Logging can help administrators diagnose and troubleshoot problems after configuration changes are made, assist change management and track configurations, and report administration activity.

You can view and generate reports about logged information from Studio. You can also view logged items in Director with the Trend View to provide notifications of configuration changes. This feature is useful for administrators who don't have access to Studio.

The Trends View gives historical data of configuration changes over a period of time so administrators can assess what changes were made to the Site, when they were made, and who made them to find the cause of an issue. This view sorts configuration information into three categories:

- Connection Failures
- Failed Single-session Machines
- Failed Multi-session Machines

For details about how to enable and configure Configuration Logging, see Configuration Logging. The Director articles describe how to view logged information from that tool.

Event logs

Services within Citrix Virtual Apps and Desktops log events that occur. Event logs are used to monitor and troubleshoot operations.

For details, see Event logs. Individual feature articles might also contain event information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration logging

May 5, 2025

Configuration logging is a feature that captures site configuration changes and administrative activities to the database. The feature is enabled by default. 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 administration activity.

You set configuration logging preferences, display configuration logs, and generate HTML and CSV reports from Citrix Studio. You can filter configuration log displays by date ranges and full text search results. Mandatory logging, when enabled, prevents configuration changes from being made unless they can be logged. With appropriate permission, you can delete entries from the configuration log. You cannot use the configuration logging feature to edit log content.

Configuration logging uses a PowerShell SDK and the Configuration Logging Service. The Configuration Logging Service runs on every Controller in the site. If one Controller fails, the service on another Controller automatically handles logging requests.

By default, the configuration logging feature is enabled, and uses the database that is created when you create the site (the site configuration database). You can specify a different location for the database. The configuration logging Database supports the same high availability features as the site configuration Database.

Access to configuration logging is controlled through delegated administration, with the Edit Logging Preferences and View Configuration Logs permissions.

Configuration logs are localized when they are created. For example, a log created in English is read in English, regardless of the locale of the reader.

What is logged

Configuration changes and administrative activities initiated from Studio, Director, and PowerShell scripts are logged. 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix policies through Studio

Examples of logged administrative changes include:

- Power management of a virtual machine or a user desktop
- Studio or Director sending a message to a user

The following operations are not logged:

- Autonomic 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, direct access of the database, or from sources other than Studio, Director, or PowerShell.
- When the deployment is initialized, configuration logging becomes available when the first Configuration Logging Service instance registers with the Configuration Service. Therefore, the early stages of configuration are not logged (for example, when the database schema is obtained and applied, when a hypervisor is initialized).

Manage configuration logging

By default, configuration logging uses the database that is created when you create a site (also known as the site configuration database). Citrix recommends that you use a separate location for the configuration logging database (and the monitoring database) for the following reasons:

- The backup strategy for the configuration logging database is likely to differ from the backup strategy for the site configuration database.
- The volume of data collected for configuration logging (and the Monitoring Service) might adversely affect the space available to the site configuration database.
- It splits the single point of failure for the three databases.

Product editions that do not support configuration logging do not have a Logging node in Studio.

Enable and disable configuration logging and mandatory logging

By default, configuration logging is enabled, and mandatory logging is disabled.

1. Sign in to Web Studio and select **Logging** in the left pane.
2. Select **Preferences** in the action bar. The configuration logging dialog box contains database information and indicates whether configuration logging and mandatory logging are enabled or disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select the desired action:

   To enable configuration logging, select **Enable**. This is the default setting. If the database cannot be written to, the logging information is discarded, but the operation continues.

   To disable configuration logging, select **Disable**. If logging was previously enabled, existing logs remain readable with the PowerShell SDK.

   To enable mandatory logging, select **Prevent changes to the site configuration when the database is not available**. No configuration change or administrative activity that is normally logged is allowed unless it can be written in the configuration logging database. You can enable mandatory logging only when configuration logging is enabled (when **Enable** is selected). If the Configuration Logging Service fails, and high availability is not in use, mandatory logging is assumed. In such cases, operations that would normally be logged are not performed.

   To disable mandatory logging, select **Allow changes when to the site configuration when the database is not available**. Configuration changes and administrative activities are allowed, even if the configuration logging database cannot be accessed. This is the default setting.

Change the configuration logging database location

You cannot change the database location when mandatory logging is enabled, because the location change includes a brief disconnect interval that cannot be logged.

1. Create a database server, using a supported SQL Server version.
2. Sign in to Web Studio and select **Logging** in the left pane.
3. Select **Preferences** in the action bar.
4. In the Logging Preferences dialog box, select **Change logging database**.
5. In the Change Logging Database dialog box, specify the location of the server containing the new database server. See Database address formats for valid formats.
6. To allow Studio to create the database, click **OK**. When prompted, click **OK**, and the database is created automatically. Studio attempts to access the database using the current Studio user's credentials. If that fails, you are prompted for the database user's credentials. Studio then uploads the database schema to the database. (The credentials are retained only during database creation.)
7. To create the database manually, click **Generate database script**. The generated script includes instructions for manually creating the database. Ensure that the database is empty and that at least one user has permission to access and change the database before uploading the schema.

The configuration logging data in the previous database is not imported to the new database. Logs cannot be aggregated from both databases when retrieving logs. The first log entry in the new configuration logging database indicates that a database change occurred, but it does not identify the previous database.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View configuration log content

To view configuration log content, select **Logging** in the left pane, and then select the **Events** tab.

By default, event logs are listed by administrator names. You can perform the following tasks as needed:

- **View log details.** A high-level operation results in one or more service and SDK calls, which are low level operations. When you select a high-level operation in the upper pane, the lower pane displays the low-level operations.
- **Sort the display.** Sort the display by clicking a column header.
- **Filter logs.** Refine the display by setting filter conditions such as day intervals or custom periods or by entering complete or partial Main Task names in the Search box. To return to the standard display after using search, clear the text in the Search box.
- **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:

- 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 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's included.

- When using a script that calls PowerShell cmdlets, if you create a low-level operation without specifying a parent high-level operation, configuration logging creates a surrogate high-level operation.

Generate reports

You can generate CSV and HTML reports containing configuration log data.

- The CSV report contains all the logging data from a specified time interval. The hierarchical data in the database is flattened into a single CSV table. No aspect of the data has precedence in the file. No formatting is used and no human readability is assumed. The file (named MyReport) contains the data in a universally consumable format. CSV files are often used for archiving data or as a data source for a reporting or data manipulation tool such as Microsoft Excel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The HTML report provides a human-readable form of the logging data for a specified time interval. It provides a structured, navigable view for reviewing changes. An HTML report comprises two files, named Summary and Details. Summary lists high level operations: when each operation occurred, by whom, and the outcome. Clicking a **Details** link next to each operation takes you to the low level operations in the Details file, which provides additional information.

To generate a configuration log report, select **Logging** in the Studio navigation pane, and then select **Create custom report** in the action bar.

- Select the date range for the report.
- Select the report format: CSV, HTML, or both.
- Browse to the location where you want to save the report.

Delete configuration log content

To delete the configuration log, you must have certain delegated administration and SQL Server database permissions.

- **Delegated administration:** You must have a delegated administration role that allows the deployment configuration to be read. The Full administrator role has this permission. A custom role must have Read Only or Manage selected in the Other permissions category.

  To create a backup of the configuration logging data before deleting it, the custom role must also have Read Only or Manage selected in the Logging Permissions category.

- **SQL Server database:** You must have a SQL server login with permission to delete records from the database. There are two ways to do this:

  - Use a SQL Server database login with a sysadmin server role, which allows you to perform any activity on the database server. Alternatively, the `serveradmin` or `setupadmin` server roles allow you to perform deletion operations.
  - If your deployment requires more security, use a non-sysadmin database login mapped to a database user who has permission to delete records from the database.

    1. In SQL Server Management Studio, create a SQL Server login with a server role other than 'sysadmin.'
    2. Map the login to a user in the database. SQL Server automatically creates a user in the database with the same name as the login.
    3. In Database role membership, specify at least one of the role members for the database user: `ConfigurationLoggingSchema_ROLE` or `dbowner`.

  For more information, see the SQL Server Management Studio documentation.

To delete the configuration logs:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Sign in to Web Studio and select **Logging** in the left pane.
2. Select **Delete logs** in the action bar.
3. You are asked if you want to create a backup of the logs before they are deleted. If you choose to create a backup, browse to the location where the backup archive is saved. The backup is created as a CSV file.

After the configuration logs are cleared, the log deletion is the first activity posted to the empty log. That entry provides details about who deleted the logs, and when.

View API and PowerShell logs

To monitor API requests made during your current session, click the **APIs** tab. API logs are cleared after you sign out of Web Studio.

To view PowerShell commands corresponding to UI actions you've taken during the day, click the **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
```

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-LogHighLevelOperation
 -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 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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[String, String]”). The properties whose names match the keys in the map are removed.

Event logs

May 5, 2025

The following articles list and describe events that can be logged by services within Citrix Virtual Apps and Desktops.

This information is not comprehensive. Readers should check individual feature articles for additional event information.

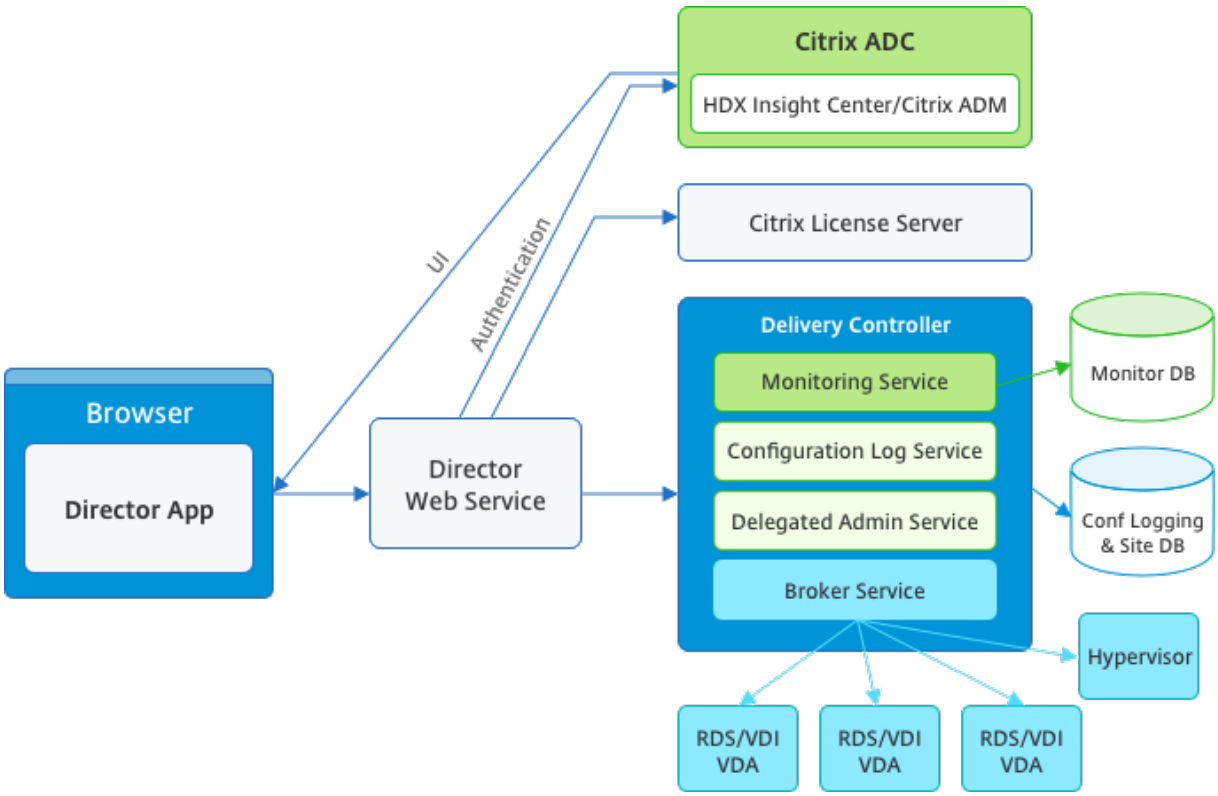
- Citrix Broker Service events
- Citrix FMA Service SDK events
- Citrix Configuration Service events
- Citrix Delegated Administration Service events

Director

September 6, 2025

Director is a monitoring and troubleshooting console for Citrix Virtual Apps and Desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Director can access:

- Real-time data from the Broker Agent using a unified console integrated with Analytics, Performance Manager, and Network Inspector. The following analytics are powered by Citrix ADM to identify bottlenecks due to the network in your Citrix Virtual Apps™ or Desktops environment:
  - Performance management for health and capacity assurance
  - Historical trending and network analysis
- Historical data stored in the Monitor database to access the Configuration Logging database.
- ICA® data from the Citrix Gateway using Citrix ADM.
  - Gain visibility into the end-user experience for virtual applications, desktops, and users for Citrix Virtual Apps or Desktops.
  - Correlate network data with application data and real-time metrics for effective troubleshooting.
  - Integrate with Citrix Virtual Desktop 7 Director monitoring tool.

Director uses a troubleshooting dashboard that provides real-time and historical health monitoring of the Citrix Virtual Apps or Desktops Site. This feature allows you to see failures in real time, providing a better idea of what the end users are experiencing.

For more information regarding the compatibility of Director features with Delivery Controller (DC), VDA and any other dependent components, see Feature compatibility matrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> With the disclosure of the Meltdown and Spectre speculative execution side-channel vulnerabilities, Citrix recommends that you install relevant mitigation patches. These patches might impact SQL Server performance. For more information, see the Microsoft support article, Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities. Citrix recommends that you test the scale and plan your workloads before rolling out the patches in your production environments.

Director is installed by default as a website on the Delivery Controller. For prerequisites and other details, see the System requirements documentation for this release. For specific information on the installation and configuration of Director, see Install and configure Director.

Log on to Director

The Director website is at https or `http://<Server FQDN>/Director`.

If one of the Sites in a multi-site deployment is down, the logon takes a little longer while it attempts to connect to the Site that is down.

Use Director with PIV smart card authentication

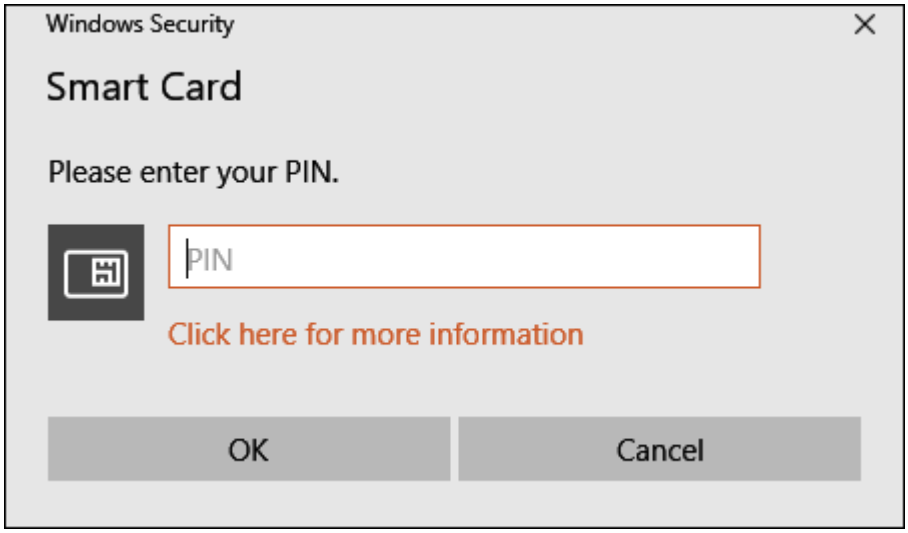
Director now supports Personal Identity Verification (PIV) based smart card authentication to log on. This feature is useful for organizations and government agencies that use smart card based authentication for access control.
Smart card authentication requires specific configuration on the Director server and in the Active Directory. The configuration steps are detailed in Configure PIV smart card authentication.

> **Note:**
>
> Smart card authentication is supported only for users from the same Active Directory domain.

After performing the required configuration, you can log on to Director using a smart card:

1. Insert your smart card into the smart card reader.
2. Open a browser and go to the Director URL, `https://<directorfqdn>/Director`.
3. Select a valid user certificate from the displayed list.
4. Enter your smart card token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



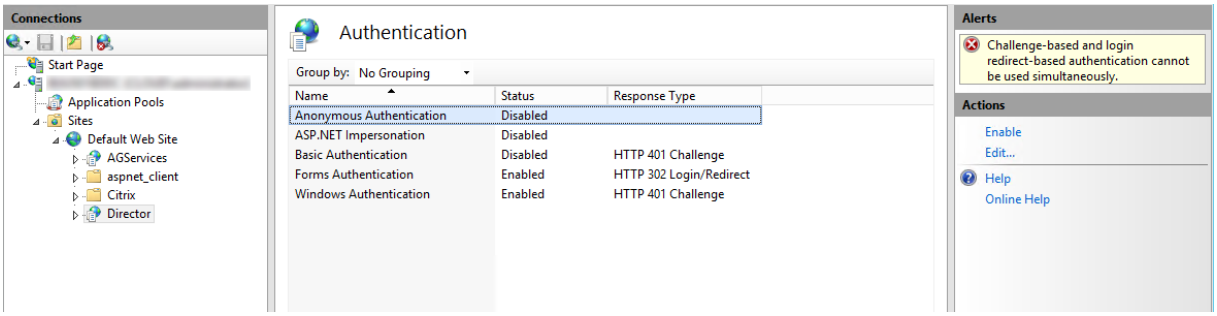
5. After you are authenticated, you can access Director without keying extra credentials on the Director logon page.

Use Director with Integrated Windows Authentication

With Integrated Windows Authentication(IWA), domain-joined users gain direct access to Director without rekeying their credentials on the Director logon page. The prerequisites for working with Integrated Windows Authentication and Director are:

- Enable Integrated Windows Authentication on the IIS website that hosts Director. When you install Director, Anonymous and Forms Authentications are enabled. To support Integrated Windows Authentication and Director, disable Anonymous Authentication and enable Windows Authentication. Forms Authentication must remain set to Enabled for authentication of non-domain users.

    1. Start IIS manager.
    2. Go to **Sites** > **Default Web Site** > **Director**.
    3. Select **Authentication**.
    4. Right-click **Anonymous Authentication**, and select **Disable**.
    5. Right-click **Windows Authentication**, and select **Enable**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configure Active Directory delegation permission for the Director machine. Configuration is only required if Director and the Delivery Controller™ are installed on separate machines.

  1. On the Active Directory machine, open the Active Directory Management Console.
  2. In the Active Directory Management Console navigate to **Domain Name** > **Computers.** Select the Director machine.
  3. Right-click and select **Properties**.
  4. In Properties, select the **Delegation** tab.
  5. Select the option, **Trust this computer for delegation to any service (Kerberos only)**.

- The browser that is used to access Director must support Integrated Windows Authentication. Additional configuration steps might be required in Firefox and Chrome. For more information, refer to the browser documentation.
- The Monitoring Service must be running Microsoft .NET Framework 4.5.1 or a later supported version listed in the System Requirements for Director. For more information, see System Requirements.

When a user logs off Director or if the session times out, the logon page is displayed. From the logon page, the user can set the Authentication type to **Automatic logon** or **User credentials**.

Interface views

Director provides different views of the interface tailored to particular administrators. Product permissions determine what is displayed and the commands available.

For example, help desk administrators see an interface tailored to help desk tasks. Director allows help desk administrators to search for the user reporting an issue and display activity associated with that user. For example, status of the user's applications and processes. They can resolve issues quickly by performing actions such as ending an unresponsive application or process, shadowing operations on the user's machine, restarting the machine, or resetting the user profile.

In contrast, full administrators see and manage the entire Site and can perform commands for multiple users and machines. The Dashboard provides an overview of the key aspects of a deployment, such as the status of sessions, user logons, and the Site infrastructure. Information is updated every minute. If issues occur, details appear automatically about the number and type of failures that have occurred.

For more information about the various roles and their permissions in Director, see Delegated Administration and Director

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Usage data collection by Pendo

The Director Service starts using Pendo to collect usage data after Director is installed. Statistics regarding the usage of the Trends pages and OData API call analytics are collected. Analytics collection complies with the Citrix Privacy Policy. Data collection is enabled by default when you install Director.

To opt out of the Pendo data collection, edit the registry key on the machine where Director is installed. If the registry key doesn't exist, create and set it to the desired value. Refresh the Director instance after changing the registry key value.

Caution: Using the Registry Editor 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 the Registry Editor can be solved. Use the Registry Editor at your own risk. Citrix recommends that you back up Windows Registry before changing it.

Location: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Name: DisableGoogleAnalytics

> **Note:**
>
> Previously, Director Service used Google Analytics to collect the data. The same registry key is now used for Pendo.

Value: 0 = enabled(default), 1 = disabled

You can use the following PowerShell cmdlet to disable data collection by Pendo:

```
1 New-Item HKLM:\SOFTWARE\Citrix -Name Director
2
3 New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
     DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

New features guide

Director has an in-product guide that uses Pendo to give an insight into the new features released in the current version of Director. The quick overview coupled with appropriate in-product messages helps you understand what's new in the product.

To opt out of this feature, edit the registry key, as described below on the machine where Director is installed. If the registry key doesn't exist, create and set it to the desired value. Refresh the Director instance after changing the registry key value.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Caution:**
>
> Using the Registry Editor 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 the Registry Editor can be solved. Use the Registry Editor at your own risk. Citrix recommends that you back up Windows Registry before changing it.

Location: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Name: DisableGuidedHelp

Value: 0 = enabled(default), 1 = disabled

You can use the following PowerShell cmdlet to disable the in-product guide:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

Reference articles

- Reduce MTTR from Citrix Director
- Citrix Director - Manage and configure alerts and notifications with PowerShell
- Citrix Virtual Apps and Desktops developer documentation

What's new in related products

- Citrix DaaS
- StoreFront
- Secure Private Access
- Citrix Enterprise Browser
- Citrix Workspace
- Provisioning

Install and configure

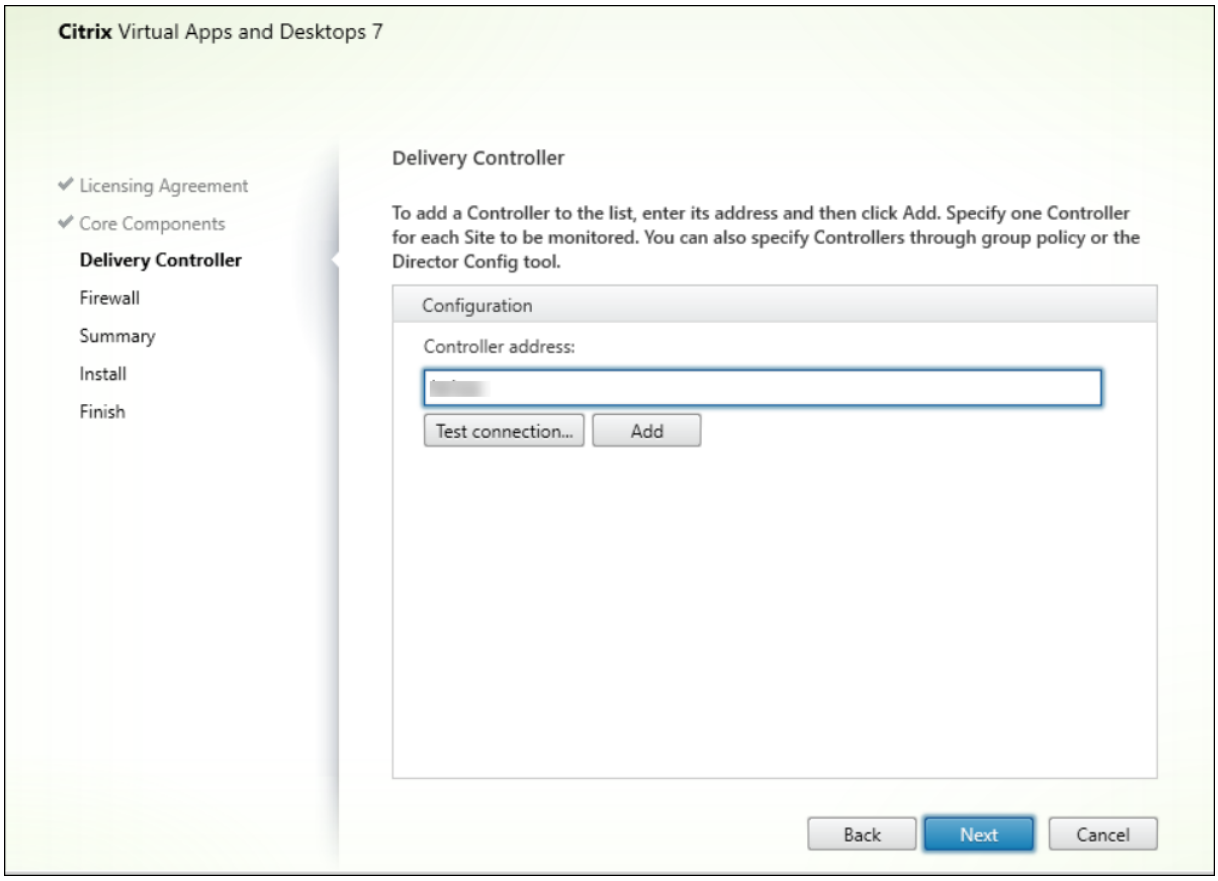
September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Install Director

Install Director using the full product ISO Installer for Citrix Virtual Apps and Desktops, which checks for prerequisites, installs any missing components, sets up the Director website, and performs basic configuration. For prerequisites and other details, see the System requirements documentation for this release. This release of Director is not compatible with Virtual Apps deployments earlier than 6.5 or Virtual Desktops deployments earlier than 7.
The default configuration provided by the ISO installer handles typical deployments. If Director was not included during installation, use the ISO installer to add Director. To add any additional components, rerun the ISO installer and select the components to install. For information on using the ISO installer, see Install core components in the installation documentation. Citrix recommends that you install using the full product ISO installer only, not the .MSI file.

When Director is installed on the Controller, it is automatically configured with localhost as the server address, and Director communicates with the local Controller by default. To install Director on a dedicated server that is remote from a Controller, you are prompted to enter the FQDN or IP address of a Controller.



> **Note:**
>
> Click **Add** to add the Controller to be monitored.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director communicates with that specified Controller by default. Specify only one Controller address for each site that you monitor. Director automatically discovers all other Controllers in the same site and falls back to those other Controllers if the Controller you specified fails.

> **Note:**
>
> Director does not load balance among Controllers.

To secure the communications between the browser and the Web server, Citrix® recommends that you implement TLS on the IIS website hosting Director. Refer to the Microsoft IIS documentation for instructions. Director configuration is not required to enable TLS.

Deploy and configure Director

When Director is used in an environment containing more than one site, be sure to synchronize the system clocks on all the servers where Controllers, Director, and other core components are installed. Otherwise, the sites might not display correctly in Director.

> **Important:**
>
> To protect the security of user names and passwords sent using plain text through the network, allow Director connections using only HTTPS, and not HTTP. Certain tools are able to read plain text user names and passwords in HTTP (unencrypted) network packets, which can create a potential security risk for users.

Configure permissions

To log on to Director, administrators with permissions for Director must be Active Directory domain users and must have the following rights:

- Read rights in all Active Directory forests to be searched (see Advanced configuration).
- Configured Delegated Administrator roles (see delegated administration and Director).
- To shadow users, administrators must be configured using a Microsoft group policy for Windows Remote Assistance. In addition:
  - When installing VDAs, ensure that the Windows Remote Assistance feature is enabled on all user devices (selected by default).
  - When you install Director on a server, ensure that Windows Remote Assistance is installed (selected by default). However, it is disabled on the server by default. The feature does not need to be enabled for Director to provide assistance to end users. Citrix recommends leaving the feature disabled to improve security on the server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To enable administrators to initiate Windows Remote Assistance, grant them the required permissions by using the appropriate Microsoft Group Policy settings for Remote Assistance. For information, see CTX127388: How to Enable Remote Assistance for Desktop Director.

Citrix uberAgent® integration with Director

Citrix uberAgent is now included by default with the Citrix Virtual Apps and Desktops™ installation, providing enhanced monitoring capabilities and seamless integration with Citrix Director. Administrators can exclude it from installation by deselecting it on the **Optional Software** screen during Virtual Delivery Agent setup.

For more information on installing uberAgent as part of the Citrix Virtual Apps and Desktops installation, see the uberAgent documentation.

Key feature:

Local application usage monitoring: With Citrix uberAgent, you can monitor the usage of applications launched within virtual desktop sessions (also known as local applications) and through the Director integration, the data is available directly on the Director dashboard (available with a Platinum license).

Configuring Citrix uberAgent integration with Director

After installing Citrix uberAgent, configure the following policies in Citrix Web Studio™ to fully integrate and use uberAgent with Director:

- **Enable uberAgent Data Collection Policy**: When enabled, uberAgent provides insights into application usage and performance, system health, network metrics, and security analysis. This policy is disabled by default.
- **Enhance Director with uberAgent Data Policy**: This policy enables the integration of Director with uberAgent. It allows Director to process data provided by uberAgent to enhance monitoring capabilities, including monitoring of local application usage. This policy is enabled by default.

Once configured, the data becomes available in the Application Usage Monitoring section of Citrix Director.

> **Note:**
>
> It takes at least one day for uberAgent data on local application usage to be aggregated and displayed in Director..

© 1997–2026 Citrix Systems, Inc. All rights reserved.

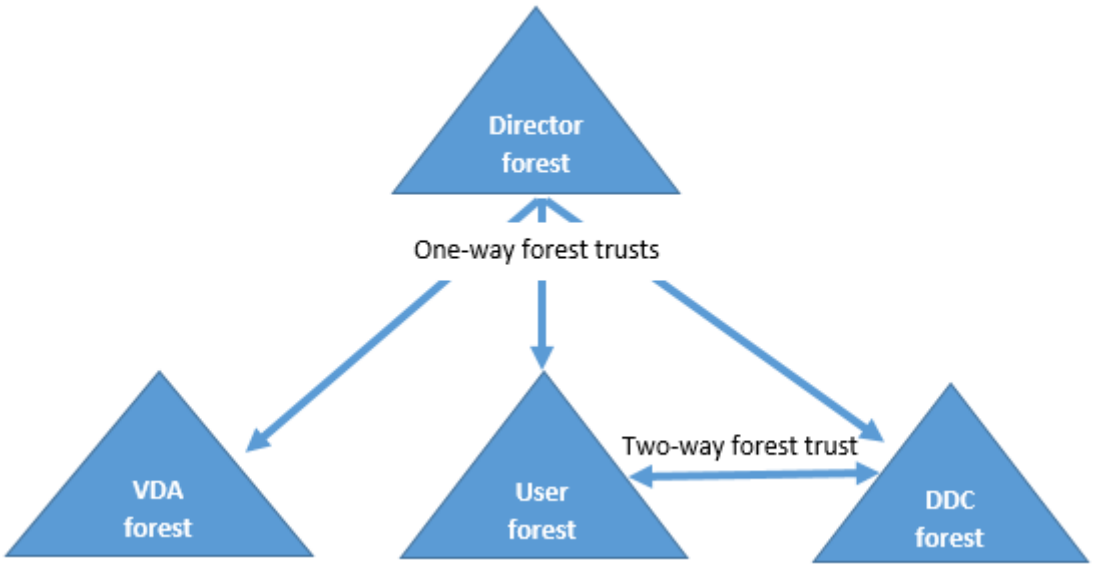
Advanced configuration

September 6, 2025

Director can support multi-forest environments spanning a forest configuration where users, Delivery Controllers (DCs), VDAs, and Directors are located in different forests. This requires proper setup of trust relationships among the forests and configuration settings.

Recommended configuration in a multi-forest environment

The recommended configuration requires creation of outgoing and incoming forest trust relationships among the forests with domain-wide authentication.



The trust relationship from the Director enables you to troubleshoot issues in user sessions, VDAs, and Delivery Controllers located in different forests.

Advanced configuration required for Director to support multiple forests is controlled through settings defined in Internet Information Services (IIS) Manager.

> **Important:**
>
> When you change a setting in IIS, the Director service automatically restarts and logs off users.

To configure advanced settings using IIS:

1. Open the Internet Information Services (IIS) Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Double-click a setting to edit it.
5. Click **Add** to add a new setting.

Director uses Active Directory to search for users and to look up more user and machine information. By default, Director searches the domain or forest in which:

- The administrator's account is a member.
- The Director web server is a member (if different).

Director attempts to perform searches at the forest level using the Active Directory global catalog. If you do not have permissions to search at the forest level, only the domain is searched.

Searching or looking up data from another Active Directory domain or forest requires that you explicitly set the domains or forests to be searched. Configure the following Applications setting to the Director website in the IIS Manager:

```
Connector.ActiveDirectory.Domains = (user),(server)
```

The value attributes user and server represent the domains of the Director user (the administrator) and Director server, respectively.

To enable searches from an extra domain or forest, add the name of the domain to the list, as shown in this example:

```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

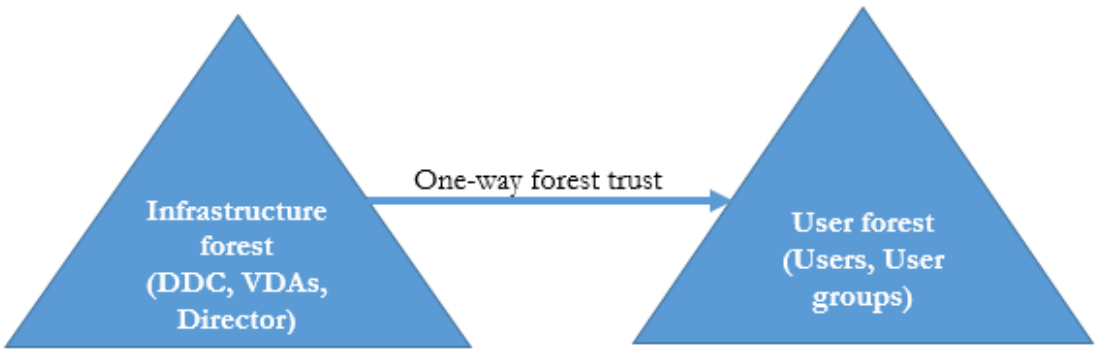
For each domain in the list, Director attempts to perform searches at the forest level. If you do not have permissions to search at the forest level, only the domain is searched.

Domain local group configuration

Most Citrix Service Providers (CSPs) have similar environment set-ups consisting of the VDAs, DCs, and Director in the Infrastructure forest. The users or user-group records belong to the Customer forest. A one-way outgoing trust exists from the Infrastructure forest to the Customer forest.

CSP administrators typically create a domain local group in the Infrastructure forest and add the users or user groups in the Customer forest to this domain local group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Director can support a multi-forest set-up like this and monitor the sessions of users configured using domain local groups.

1. Add the following Applications settings to the Director website in IIS Manager:

```
Connector.ActiveDirectory.DomainLocalGroupSearch= true

DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
```

   <domain1><domain2> are names of the forests in which the domain local group exists.

2. Assign the domain local group to delivery groups in Web Studio.
3. Restart IIS and log on to Director again for the changes to take effect. Now, Director can monitor and show the sessions of these users.

Add sites to Director

If Director is already installed, configure it to work with multiple sites. To configure, use the IIS Manager Console on each Director server to update the list of server addresses in the application settings.

Add an address of a Controller from each site to the following setting:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAController and SiteBController are the addresses of Delivery Controllers from two different sites.

Disable the visibility of running applications in the Activity Manager

By default, the Activity Manager in Director displays a list of all running applications for a user's session. This information is viewed by all administrators that have access to the Activity Manager feature

© 1997–2026 Citrix Systems, Inc. All rights reserved.

in Director. For Delegated Administrator roles, this includes Full Administrator, delivery group Administrator, and Help Desk Administrator.

To protect the privacy of users and the applications they are running, you can disable the **Applications** tab to list running applications.

> **Warning:**
>
> 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 the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. On the VDA, modify the registry key at HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDis
   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.
2. On the server with Director installed, modify the setting that controls the visibility of running applications. By default, the value is "true"which allows visibility of running applications in the Applications tab. Change the value to "false"which disables visibility. This option affects only the Activity Manager in Director, not the VDA.
   Modify the value of the following setting:
   UI.TaskManager.EnableApplications = false

> **Important:**
>
> To disable the view of running applications, make both changes to ensure that the data is not displayed in the Activity Manager.

Configure PIV smart card authentication

September 6, 2025

This article lists the configuration required on the Director Server and in the Active Directory to enable the smart card authentication feature.

> **Note:**
>
> Smart card authentication is supported only for users from the same Active Directory domain.

Director server configuration

Perform the following configuration steps on the Director server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

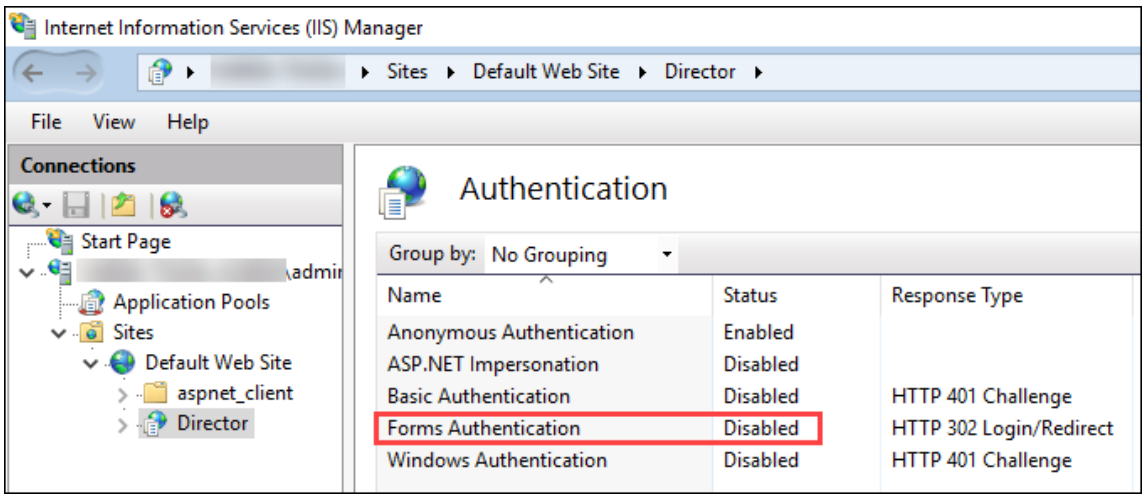
1. Install and enable the Client Certificate Mapping Authentication. Follow the **Client Certificate Mapping authentication using Active Directory** instructions in the Microsoft document, Client Certificate Mapping Authentication.
2. Disable Forms Authentication on the Director site.

   Start IIS Manager.

   Go to **Sites** > **Default Web Site** > **Director**.

   Select **Authentication**.

   Right-click **Forms Authentication**, and select **Disable.**



3. Configure the Director URL for the more secure https protocol (instead of HTTP) for client certificate authentication.

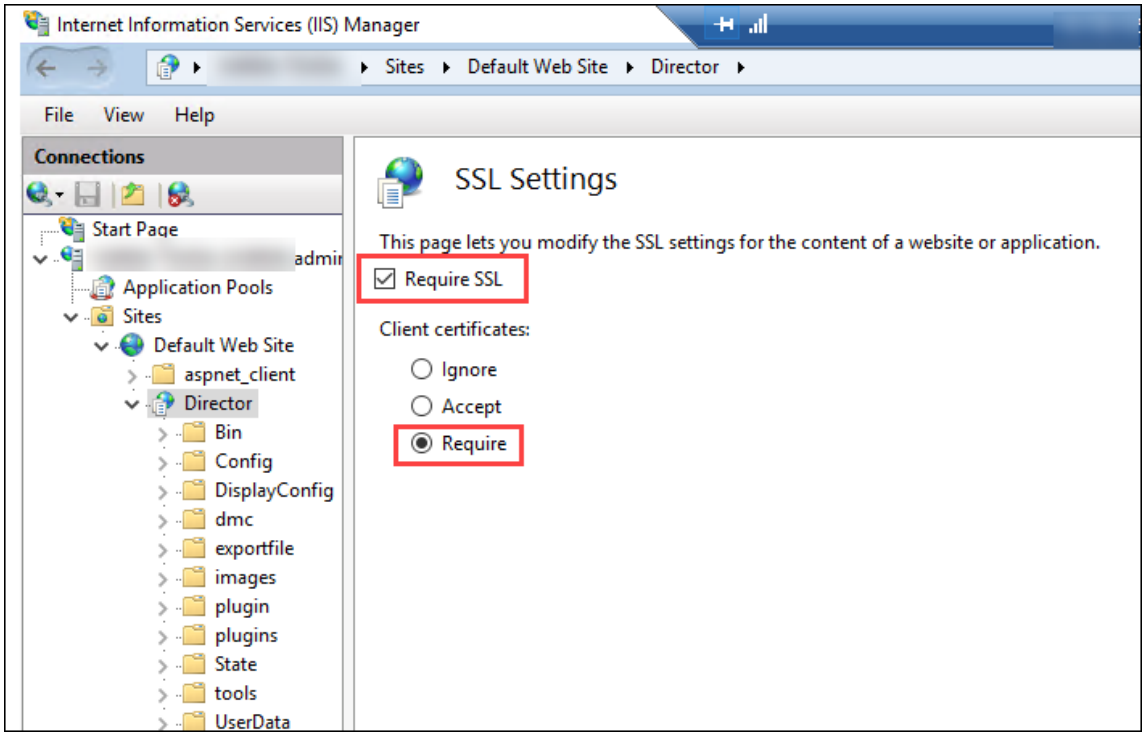
   a) Start IIS Manager.

   b) Go to **Sites** > **Default Web Site** > **Director**.

   c) Select **SSL Settings.**

   d) Select **Require SSL** and **Client certificates** > **Require.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Update web.config. Open the web.config file (available in c:\inetpub\wwwroot\Director) using a text editor.

Under the <system.webServer> parent element, add the following snippet as the first child element:

```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

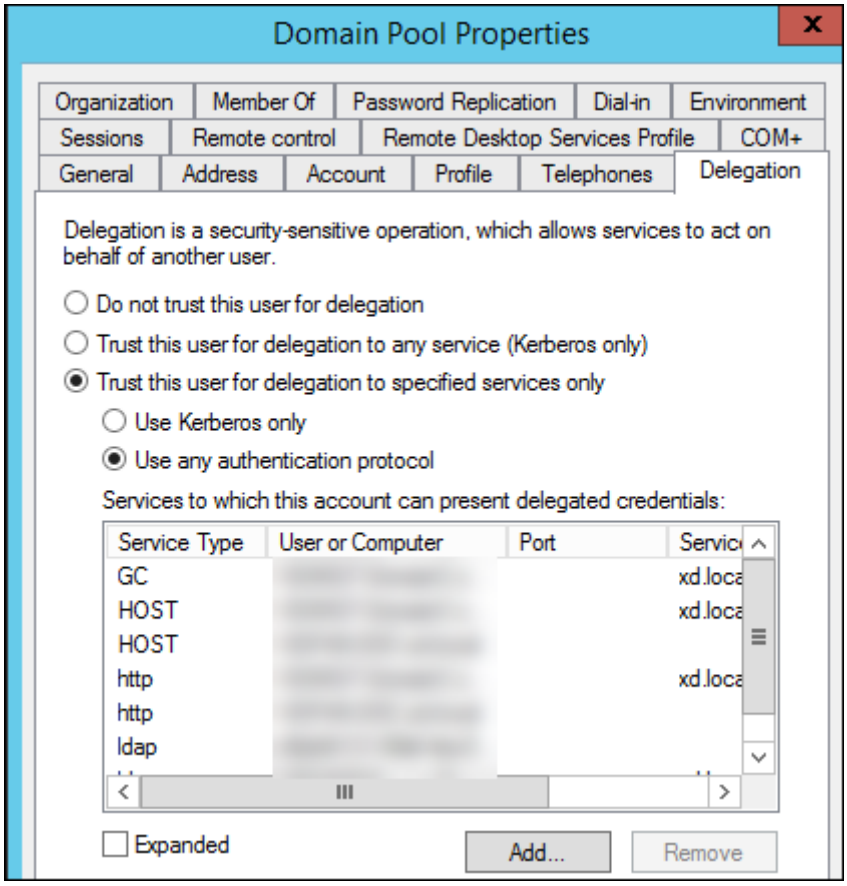
Active Directory configuration

By default the Director application runs with the **Application Pool** identity property. Smart card authentication requires delegation for which the Director application identity must have Trusted Computing Base (TCB) privileges on the service host.

Citrix recommends that you create a separate service account for Application Pool identity. Create the service account and assign TCB privileges as per the instructions in the Microsoft MSDN article, Protocol Transition with Constrained Delegation Technical Supplement.

Assign the newly created service account to the Director application pool. The following figure shows the properties dialog of a sample service account, Domain Pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



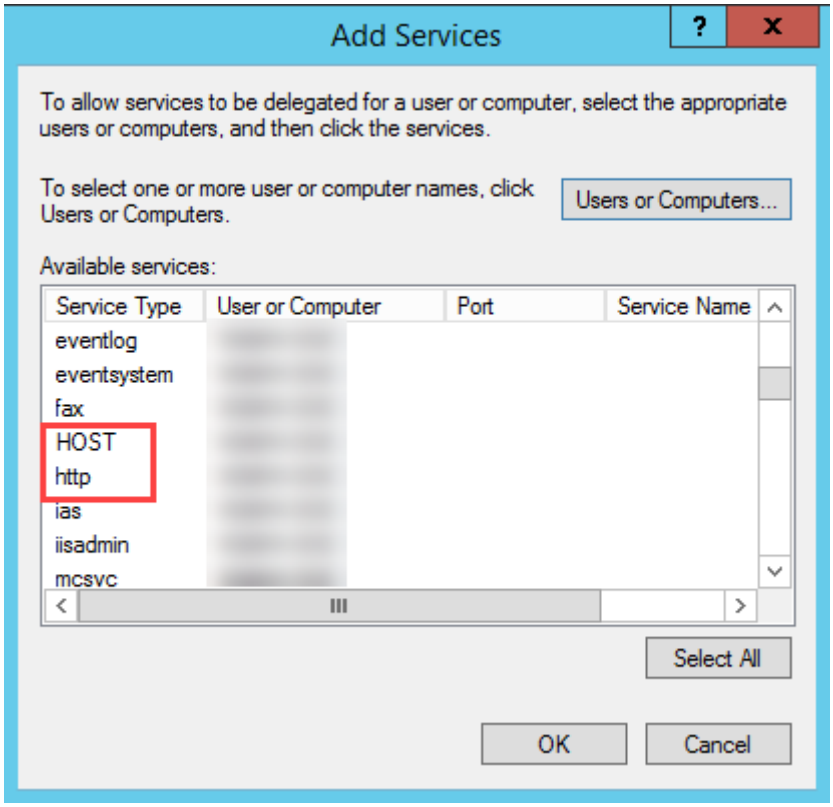
Configure the following services for this account:

- Delivery Controller™: HOST, HTTP
- Director: HOST, HTTP
- Active Directory: GC, LDAP

To configure,

1. In the user account properties dialog, click **Add.**
2. In the **Add Services** dialog, click Users or Computers.
3. Select the Delivery Controller host name.
4. From the **Available services** list, select HOST and HTTP **Service Type**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Similarly, add Service Types for **Director** and **Active Directory** hosts.

Create Service Principal Name records

You must create a service account for each Director server and load-balanced Virtual IPs (VIP) used to access a pool of Director servers. You must create service principal name (SPN) records to configure a delegation to the newly created service account.

- Use the following command to create an SPN record for a Director server:

```
setspn -a http/<directorServer>.<domain_fqdn> <domain>\<
   DirectorAppPoolServiceAcct>
```

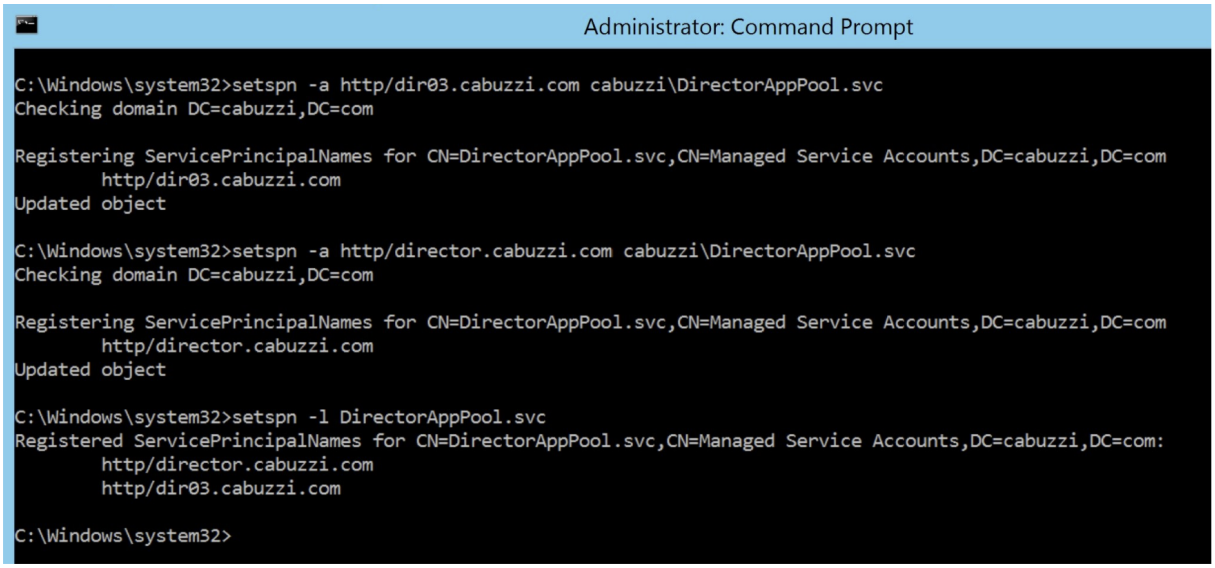
- Use the following command to create an SPN record for a load-balanced VIP:

```
setspn -S http/<DirectorFQDN> <domain>\<
   DirectorAppPoolServiceAcct>
```

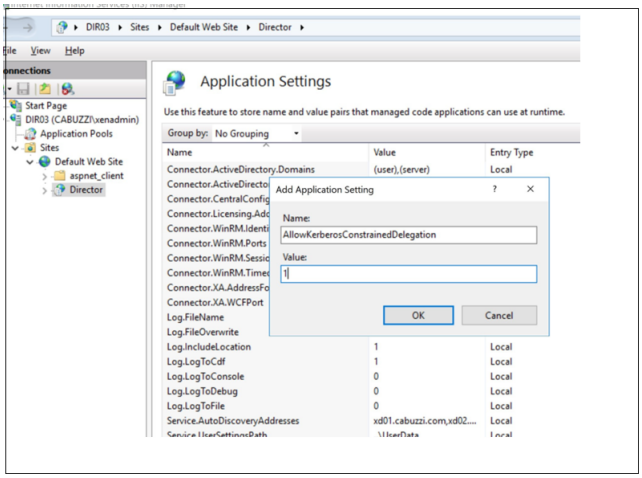
- Use the following command to view or test the created SPNs:

```
setspn –l <DirectorAppPoolServiceAcct>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

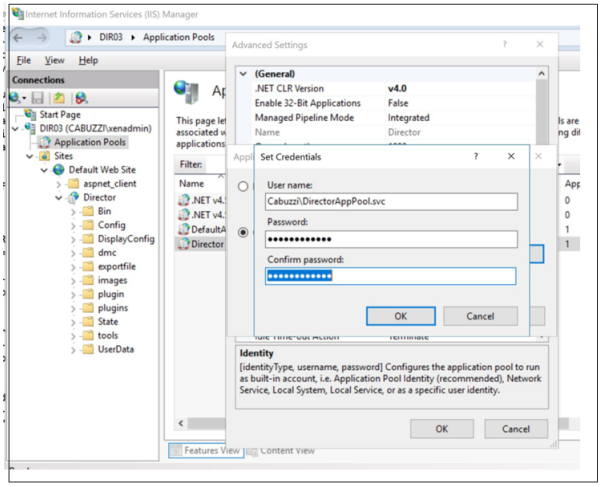


- Select the Director virtual directory in the left pane and double click **Application Settings**. Inside the Application Settings window, click **Add** and ensure **AllowKerberosConstrainedDelegation** is set to 1.



- Select **Application Pools** in the left-hand pane, then right-click the Director application pool and select **Advanced Settings**.
- Select **Identity**, click the ellipses ("…") to enter the service account domain\logon and password credentials. Close the IIS console.

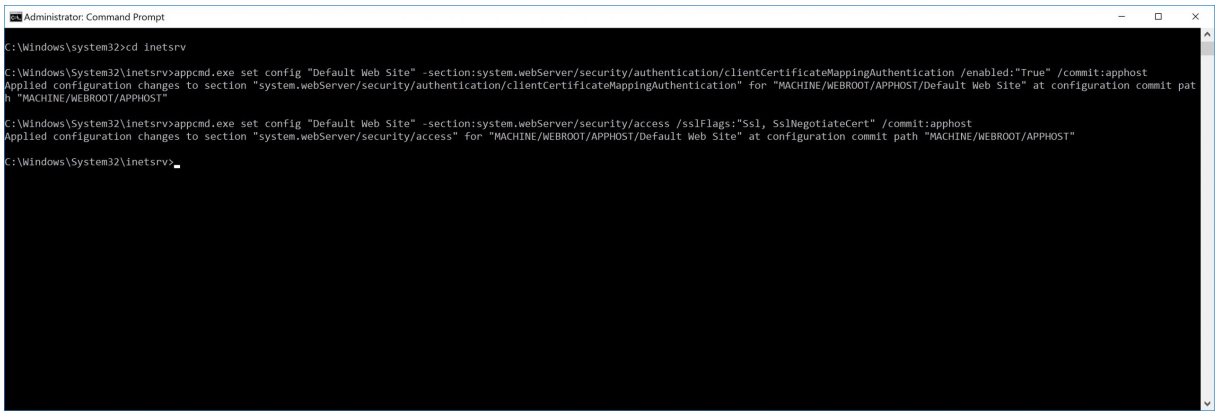
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- From an elevated command prompt, change the directory to C:\Windows\System32\inetsrv and enter the following commands:

```
appcmd.exe set config "Default Web Site" -section:system.webServer/security/authentication/clientCertificateMappingAuthentication /enabled:"True" /commit:apphost
```

```
appcmd.exe set config "Default Web Site" -section:system.webServer/security/access /sslFlags:"Ssl, SslNegotiateCert" /commit:apphost
```



Firefox browser configuration

To use the Firefox browser, install the PIV driver available at OpenSC 0.17.0. For installation and configuration instructions, see Installing OpenSC PKCS#11 Module in Firefox, Step by Step.
For information on the usage of the smart card authentication feature in Director, see the Use Director with PIV based smart card authentication section in the Director article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure network analysis

September 6, 2025

> **Note:**
>
> The availability of this feature depends on your organization's license and your administrator permissions.

Director integrates with Citrix ADM to provide network analysis and performance management:

- Network analysis uses HDX™ Insight reports from Citrix ADM to provide an application and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment.
- Performance management provides historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

After you enable this feature in Director, HDX Insight reports provide Director with additional information:

- The Network tab in the Trends page shows latency and bandwidth effects for applications, desktops, and users across your entire deployment.
- The User Details page shows latency and bandwidth information specific to a particular user session.

Limitations:

- In the Trends view, HDX connection logon data isn't collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.

To enable network analysis, you must install and configure Citrix ADM in Director. Director requires Citrix ADM Version 11.1 Build 49.16 or later. MAS is a virtual appliance that run on the XenServer. Using network analysis, Director communicates and gathers the information that is related to your deployment.

For more information, see the Citrix ADM documentation.

> **Note:**
>
> Citrix NetScaler Insight Center has reached its End of Maintenance date as of 15 May 2018. See the Citrix Product Matrix. Integrate Director with Citrix ADM for network analysis. To migrate your NetScaler Insight Center to Citrix ADM, see Migrate from NetScaler Insight Center to Citrix ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. On the server where Director is installed, locate the DirectorConfig command line tool in C:\inetpub\wwwroot\Director\tools, and run it with parameter /configNetScaler from a command prompt.
2. When prompted, enter the Citrix ADM machine name (FQDN or IP address), the user name, password, HTTPS connection type (preferred over HTTP), and choose Citrix ADM integration.
3. To verify the changes, log off and log back on.

> **Note:**
>
> For security reasons, it is recommended to create a custom role for ADM integration with Director with sufficient permission to access HDX Insight only.
>
> For more information, see Configure access policies.

Delegated administration and Director

September 6, 2025

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.

For information about creating delegated administrators, see the main delegated administration article.

Administrative permissions determine the Director 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.

The built-in roles and permissions also determine how administrators use Director:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Administrator Role	Permissions in Director
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, power management and session management, enabling maintenance mode, and exporting trends data.
Read Only Administrator	Can access all views and see all objects in specified scopes and 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. 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 Director and cannot view data.

Configure custom roles for Director administrators

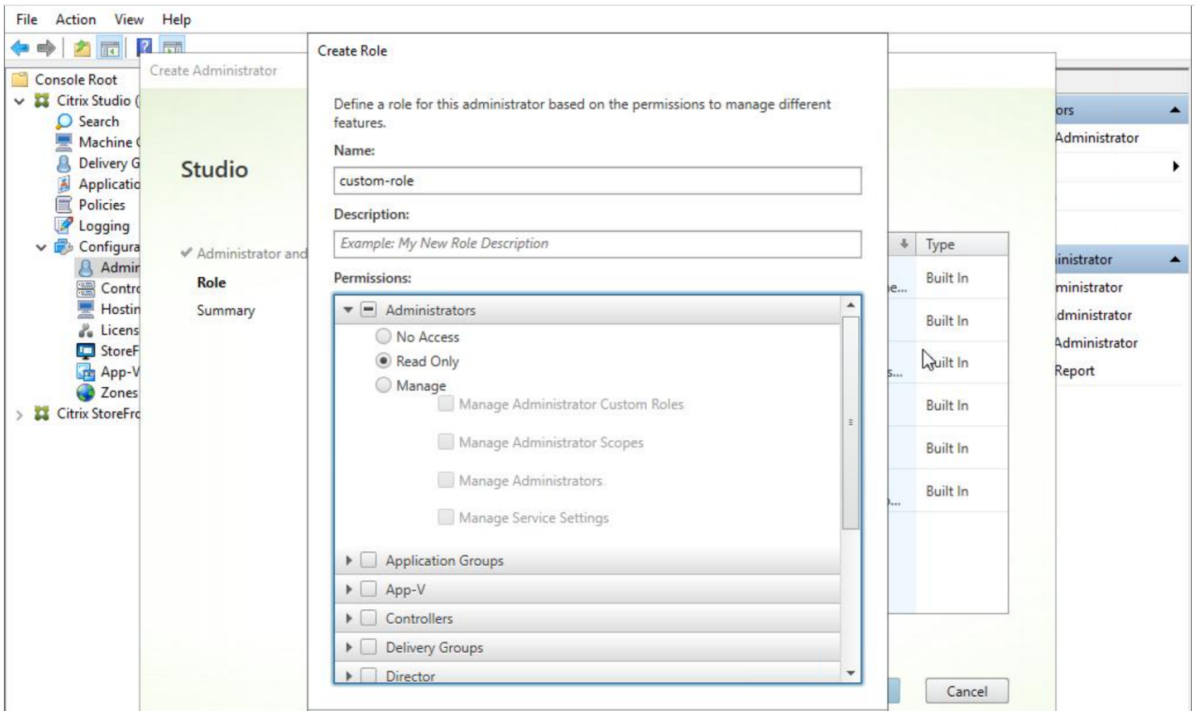
In Studio, you can also configure Director-specific, custom roles to more closely match the requirements of your organization and delegate permissions more flexibly. For example, you can restrict the built-in Help Desk administrator role so that this administrator cannot log off sessions.

If you create a custom role with Director permissions, you must also give that role other generic per-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

missions:

- Delivery Controller™ permission to log on to Director - at least read only access in Administrator node
- Permissions to delivery groups to view the data related to those delivery groups in Director - at least read only access



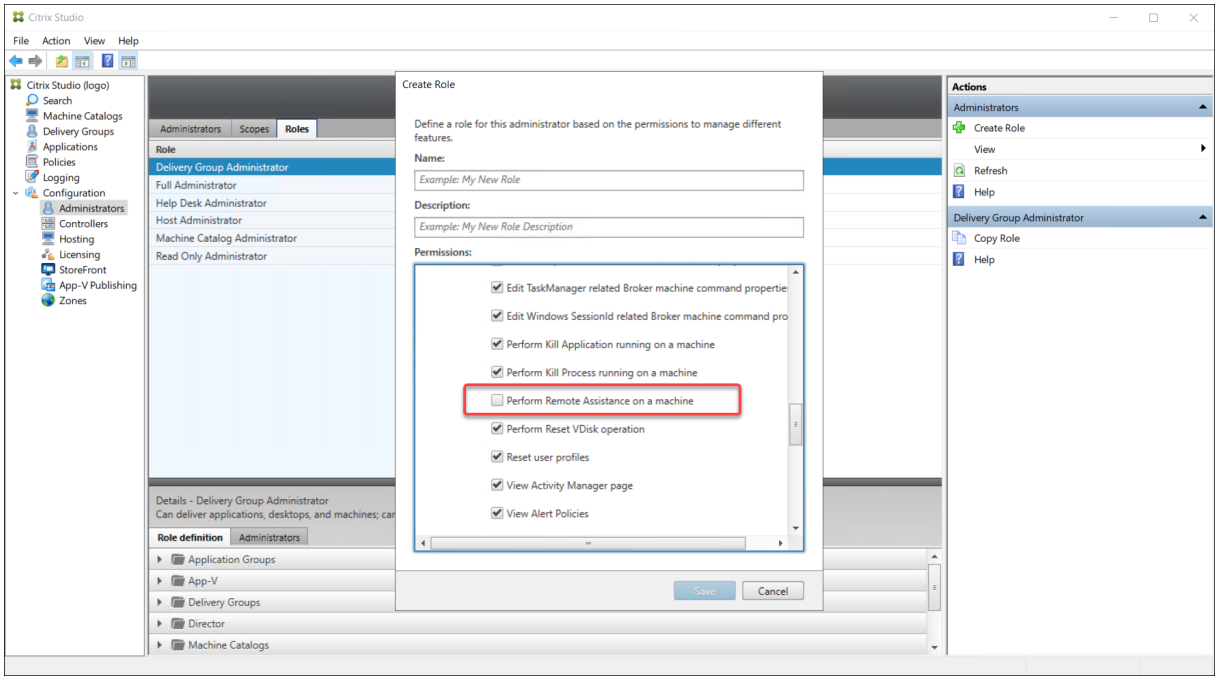
Alternatively, you can create a custom role by copying an existing role and include extra permissions for different views. For example, you can copy the Help Desk role and include permissions to view the Dashboard or Filters pages.

Select the Director permissions for the custom role, which include:

- Perform Kill Application running on a machine
- Perform Kill Process running on a machine
- Perform Remote Assistance on a machine
- Reset user profiles
- View Client Details page
- View Dashboard page
- View Filters page
- View Machine Details page
- View Trends page
- View User Details page

In this example, Shadowing (Perform Remote Assistance on a machine) is turned off.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A permission can have dependencies on other permissions to become applicable on the UI. For example, selecting the **Perform Kill Application running on a machine** permission enables the **End Application** functionality only in those panels to which the role has permission. You can select the following panel permissions:

- View Filters page
- View User Details page
- View Machine Details page
- View Client Details page

In addition, from the list of permissions for other components, consider these permissions from delivery groups:

- Enable/disable maintenance mode of a machine using delivery group membership.
- Perform power operations on Windows Desktop machines using delivery group membership.
- Perform session management on machines using delivery group membership.

Secure Director deployment

September 6, 2025

This article highlights areas that might have an impact on system security when deploying and configuring Director.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director communications

In a production environment, use the HTTPS protocols to secure the data passing between Director and your servers. HTTPS uses Transport Layer Security (TLS) protocols to provide strong data encryption.

> **Note:**
>
> - Citrix® strongly recommends that you restrict access to Director console within the intranet network.
> - Citrix strongly recommends that you do not enable unsecured connections to Director in a production environment.
> - Use TLS 1.2 or higher. Do not use legacy TLS or SSL.

To secure communications between users' web browsers and Director, refer to Enable TLS on Web Studio and Director

To secure communications between Director and Citrix Virtual Apps and Desktops servers (for monitoring and reports), refer to Securing On-Premises Monitor OData API Access.

To secure communications between Director and Citrix ADC (for Citrix Insight), when you Configure network analysis, choose a connection type of HTTPS.

Configure Microsoft Internet Information Services (IIS)

You can configure Director with a restricted IIS configuration.

Application Pool recycling limits

Director uses an application pool called **Director**. You can set the following Application Pool recycling limits on the application pool:

- Virtual Memory Limit: 4,294,967,295
- Private Memory Limit: The size of the physical memory of the StoreFront™ server
- Request Limit: 4,000,000,000

File name extensions

During installation, Director configures request filtering to only allow the following extensions:

- .
- .aspx

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- .css
- .eot
- .html
- .ico
- .js
- .png
- .svc
- .svg
- .png
- .json
- .woff
- .woff2
- .ttf

HTTP Verbs

During installation, Director configures request filtering to only allow the following verbs:

- GET
- POST
- HEAD

IIS features

Director does not require the following IIS components:

- ISAPI extensions
- CGI programs
- FastCGI programs

You can remove these components.

.NET trust level

Director requires **.NET Trust Level** to be set to **Full Trust**. Do not set the .NET trust level to any other value.

Configure user rights

When Director is installed, its application pool is granted the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Log on as a service** logon right
- **Adjust memory quotas for a process**, **Generate security audits**, and **Replace a process level token** privileges

The rights and privileges mentioned are normal installation behavior when application pools are created.

You do not need to change these user rights. These privileges are not used by Director and are automatically disabled.

Director security separation

You can deploy any web applications in the same web domain (domain name and port) as Director. However, any security risks in those web applications can potentially reduce the security of your Director deployment. Where a greater degree of security separation is required, Citrix recommends that you deploy Director in a separate web domain.

Configuring on-premises sites with Citrix Analytics for Performance™

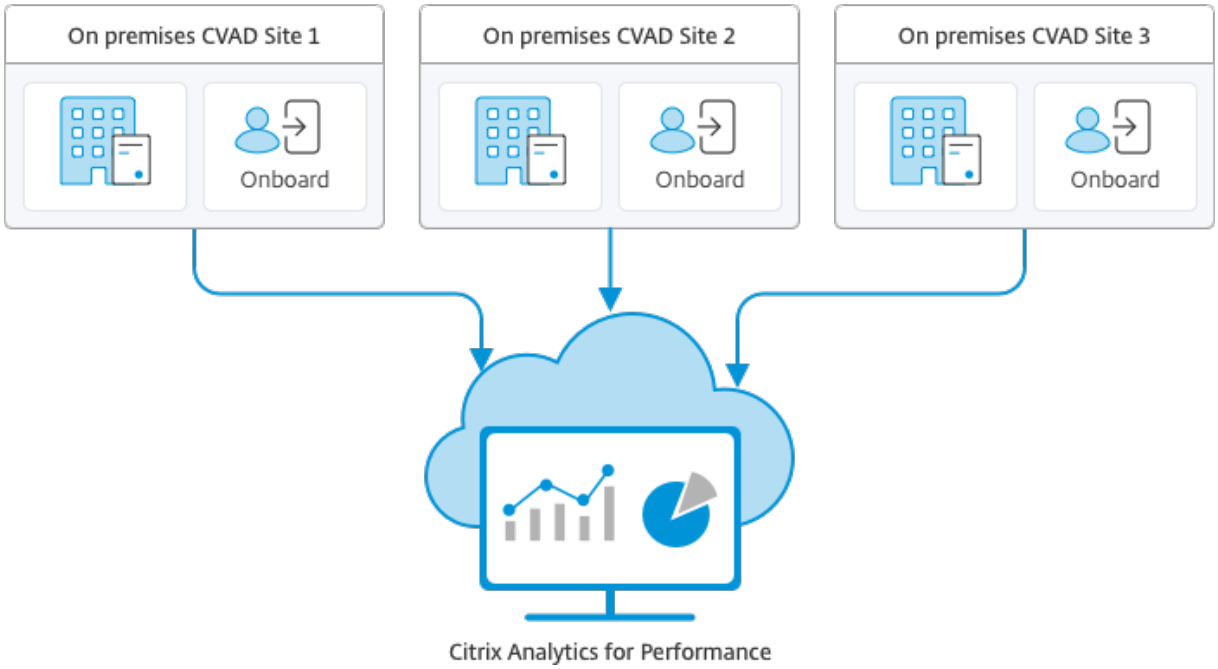
September 6, 2025

Citrix Analytics for Performance (Performance Analytics) is the comprehensive performance monitoring solution from the Citrix Analytics Cloud Service. Performance analytics provides advanced insights and analytics built on performance metrics. Performance Analytics helps you monitor and view the usage and performance metrics of one or more Citrix Virtual Apps and Desktops™ sites in your organization.

For more information about Performance Analytics, see the Performance Analytics article.

You can send performance data from your site to Citrix Analytics for Performance on Citrix Cloud™ to leverage its advanced performance analytics capabilities. To view and use Performance Analytics, you must first configure your on-premises sites with Citrix Analytics for Performance from the **Analytics** tab in **Director**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Performance Analytics accesses data in a secure manner and no data is transferred from Citrix Cloud to the on-premises environment.

Prerequisites

To configure Citrix Analytics for Performance from Director, no new components need to be installed. Ensure that the following requirements are met:

- Your Delivery Controller and Director are on version 1912 CU2 or later. For more information, see Feature compatibility matrix.

> **Note:**
>
> - Configuring your on-premises site with Citrix Analytics for Performance from Director might fail if the Delivery Controller is running a Microsoft .NET Framework version earlier than 4.8. As a workaround, upgrade the .NET Framework in your Delivery Controller to version 4.8. LCM-9255.
> - When you configure your on-premises site running Citrix Virtual Apps and Desktops version 2012 with Citrix Analytics for Performance from Director, the configuration might fail after a couple of hours or after a restart of the Citrix Monitor Service in the Delivery Controller. The Analytics tab displays a Not Connected status in this case. As a workaround, create an Encryption folder in the registry on the Delivery Controller, Location: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor, Folder Name: Encryption. Ensure that the CitrixMonitor account has Full Control Access on the Encryption

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> folder. Restart the Citrix Monitor Service.DIR-14324.

- Access to the **Analytics** tab to perform this configuration is available for full administrators only.
- For Performance Analytics to access performance metrics, outbound internet access is available on all Delivery Controllers and the machines on which Director is installed. Specifically, ensure accessibility to the following URLs:
  - Citrix Key Registration: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/`

  In case, Delivery Controllers and Director machines are within an intranet and outbound internet access is via a proxy server, ensure the following:
- The proxy server must allow the preceding list of URLs.
- Add the following configuration in the Director web.config and citrix.monitor.exe.config files. Ensure that you add this configuration within the **configuration** tags:

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</system.net>
```

  - The Director web.config is located at `C:\inetpub\wwwroot\Director\web.config` on the machine where Director is installed.
  - The citrix.monitor.exe.config is located at `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` on the machine where the Delivery Controller is installed.

  This setting is provided by Microsoft on IIS. For more information, see `https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`.

  The **defaultproxy** field in the config file controls the outbound access of Director and Monitor Service. Configuration and communication with Performance Analytics requires the **defaultproxy** field to be set to **true**. It is possible that the policies in effect set this field to false. In this case, you must manually set the field to true. Take a backup of the config files before you make the changes. Restart the Monitoring service on the Delivery Controller™ for the changes to be affected.
- You have an active Citrix Cloud entitlement for Citrix Analytics for Performance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

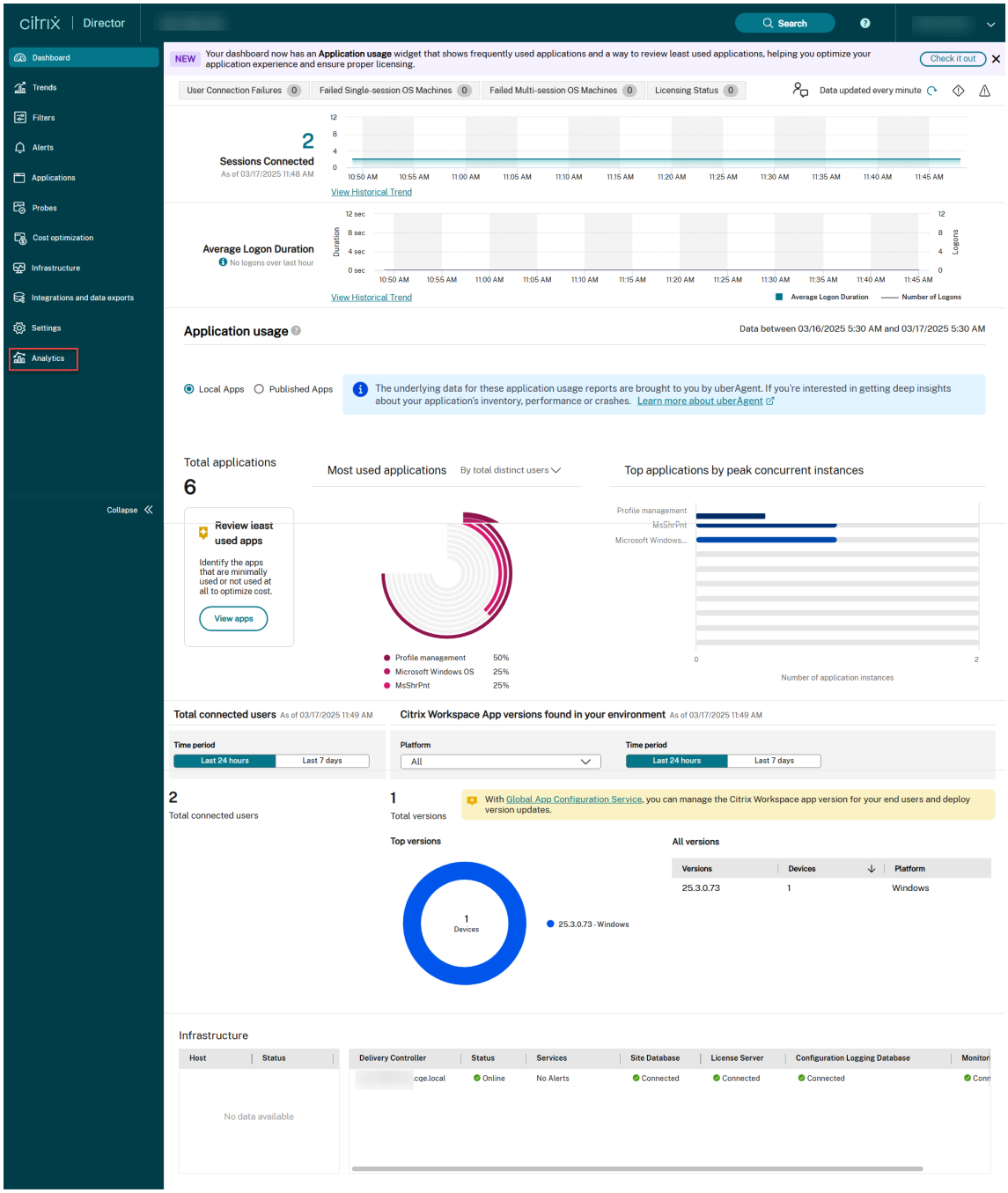
- Your Citrix Cloud account is an Administrator account with rights to the Product Registration Experience. For more information about administrator permissions, see Modify Administrator Permissions.

Configuration steps

After you have verified the prerequisites, do the following:

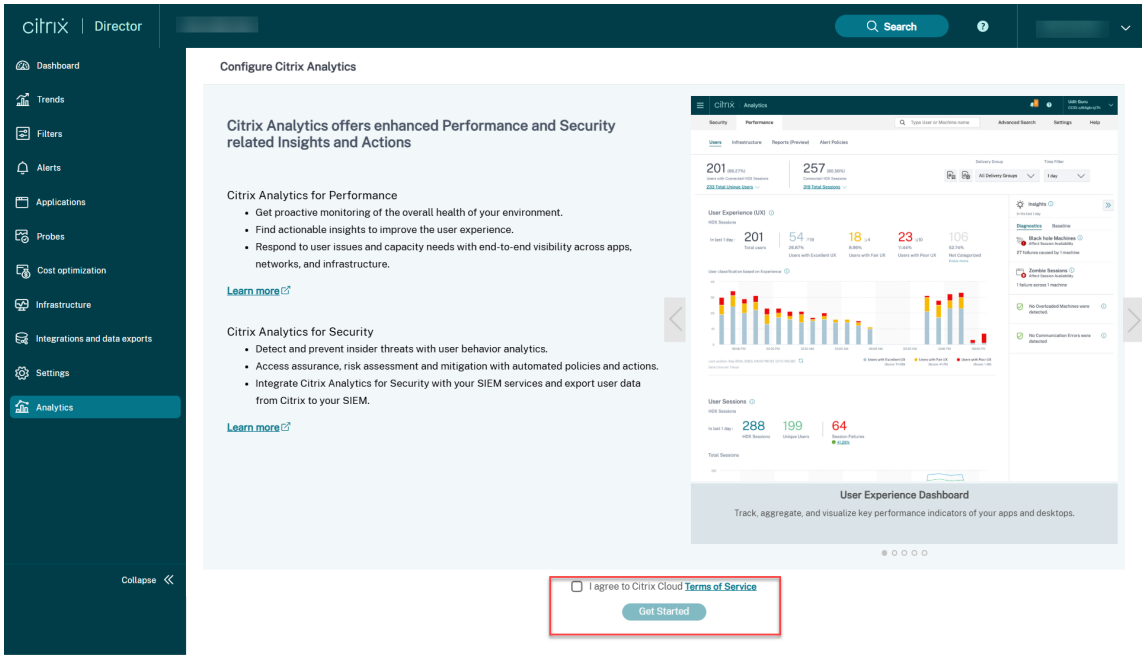
1. Sign in to Director as a full administrator and select the site which you want to configure with Performance Analytics. The Director Dashoard page appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

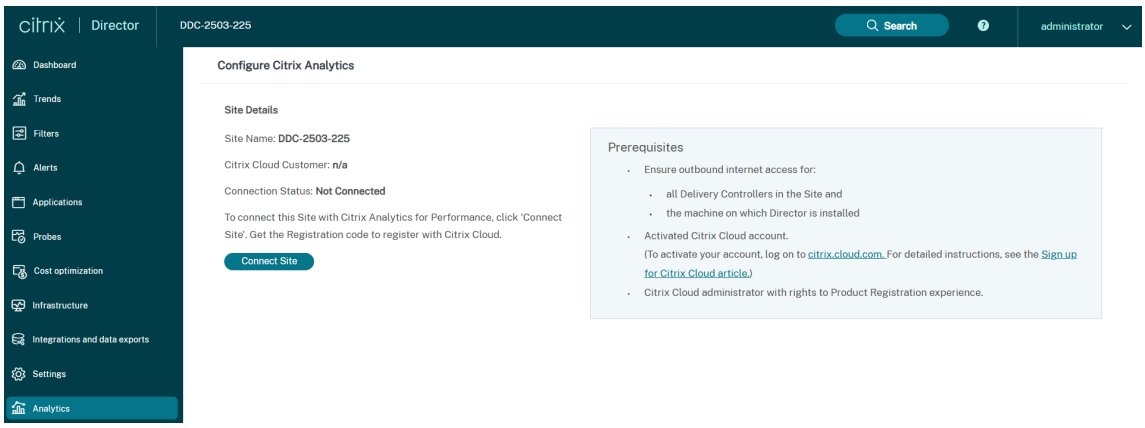


2. Click the **Analytics** tab. The **Configure Citrix Analytics** page appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



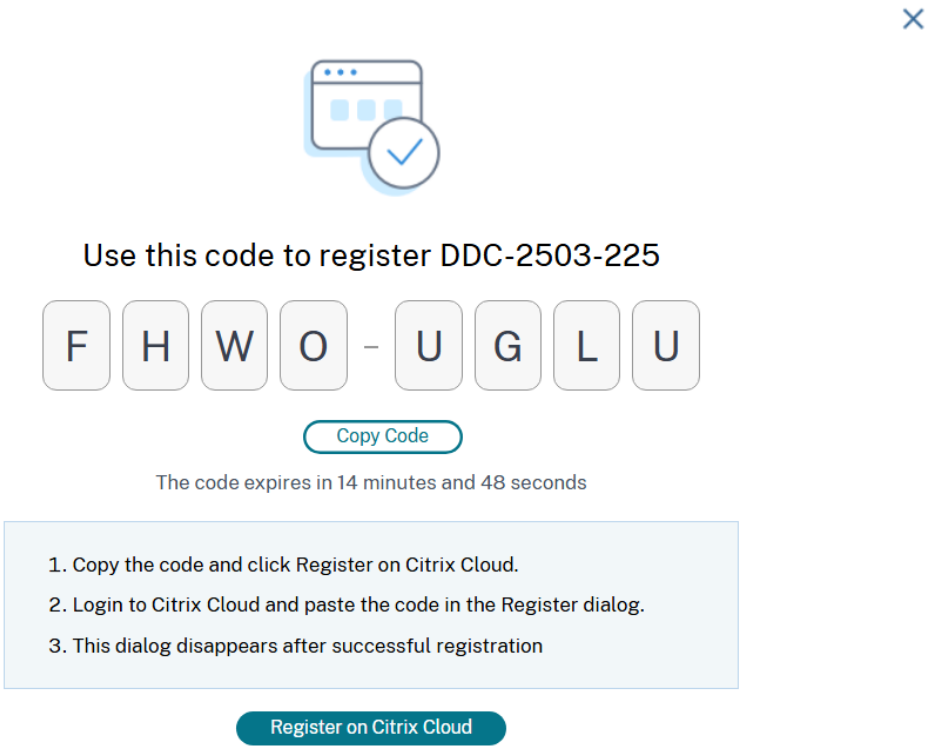
3. Review the steps, select the terms of service, and then click **Get Started**. The **Site Details** page appears.



4. Review the prerequisites and ensure that they are met. Review the site details.
5. Click **Connect Site** to start the configuration process.

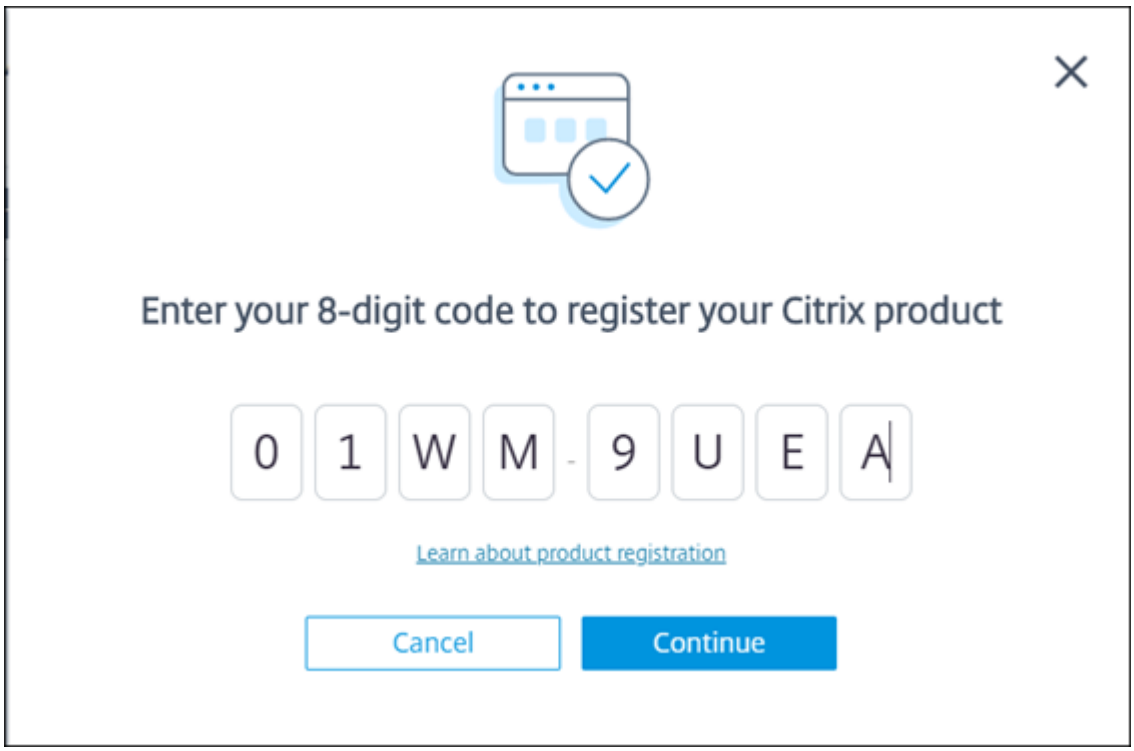
   A unique 8-digit registration code is generated to be used to register this site with Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



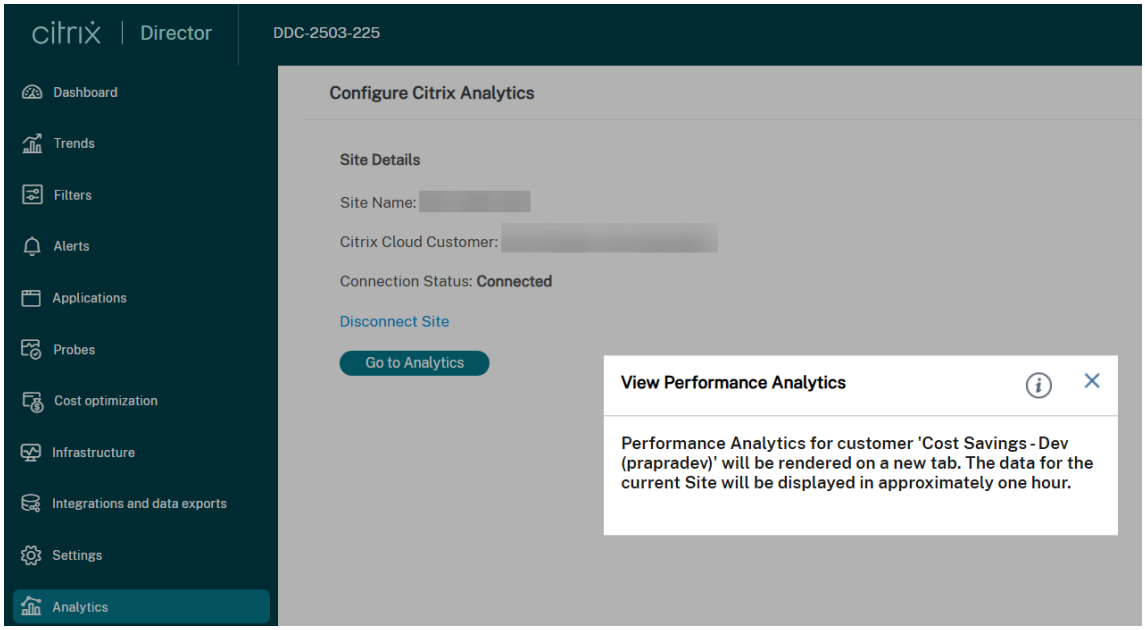
6. Click **Copy Code** to copy the code and then click **Register on Citrix Cloud**. You are redirected to the registration URL in Citrix Cloud.
7. Sign in with your Citrix Cloud credentials and select your customer.
8. Paste the copied registration code in the Product Registrations page in Citrix Cloud. Click **Continue** to register. Review the registration details and click **Register**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



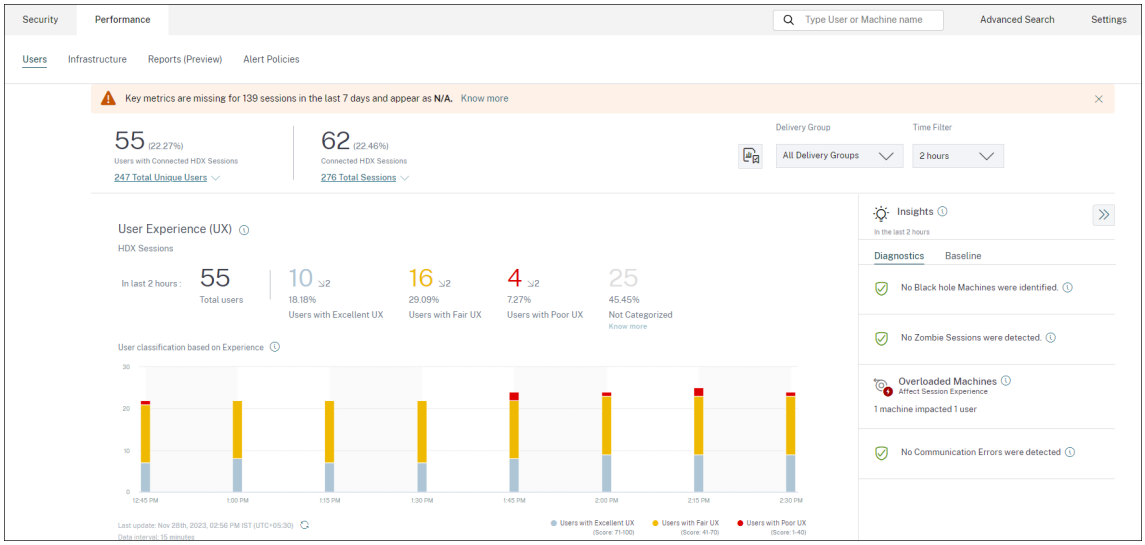
Your on-premises site registers with Citrix Cloud.

9. From **Director**, click **Go to Analytics** on the **Analytics** tab.



Performance Analytics opens on a new tab on your browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If your Citrix Cloud session has expired, you might be redirected to the Citrix.com or My Citrix account logon page.

10. To register multiple sites with Performance Analytics, repeat the preceding configuration steps for each site from Director. Metrics for all configured sites are displayed on the Performance Analytics dashboard.

    In case you have more than one Director instance running per site, configure from any one Director instance. All other Director instances connected to the site are updated at the next refresh after the configuration process.

11. To disconnect your site from Citrix Cloud, click **Disconnect Site**. This option deletes the existing configuration.

    > **Notes:**
    >
    > The first time you configure a site, events from the site might take some time (approximately an hour) to be processed; causing a delay in the display of metrics on the Performance Analytics dashboard. Thereafter, events refresh at regular intervals.
    >
    > Upon disconnect, data transmission from the old account continues for some time until the events from the new account are transmitted. For approximately one hour after data transmission stops, analytics related to the old account remain displayed on the Performance Analytics Dashboard.
    >
    > Upon expiry of entitlement to the Citrix Analytics service, it takes up to a day to stop sending the site metrics to Performance Analytics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Independent release of Director for LTSR deployments

September 13, 2025

The independent release of Director for LTSR deployments now provides an option to access the latest Director features for enhanced troubleshooting and monitoring in Citrix® environments to compatible LTSR environments. This feature allows you to use the latest Director version on your 2402 LTSR deployments. Also, provides access to features released after the LTSR announcement without impacting the application delivery infrastructure.

The standalone installer includes the latest .msi for Monitor service, Director service, and the Monitor Snap-in. Using these new .msi files, you can upgrade your 2402 LTSR CU1 with current release features.

For information on the Director features that are part of current releases after the 2402 LTSR release, see the following:

- Citrix Virtual Apps and Desktops 2407 release
- Citrix Virtual Apps and Desktops 2411 release

To learn more about specific features on Director with the minimum version of VDA, see Director Version Matrix.

Benefits

- **Access to new features**: Get access to Director features released after the 2402 LTSR announcement, including those in Citrix Virtual Apps and Desktops™ 2407 and 2411 Cumulative Release (CR).
- **Targeted upgrades:** Upgrade only the Director and Monitoring Service components without impacting the rest of your LTSR infrastructure.
- **LTSR compatibility**: Maintain your LTSR environment while benefiting from the latest Director enhancements.
- **Rollback option:** You have the flexibility to roll back to the previous Director version if needed.

Key consideration

The upgraded Director component is LTSR compatible, but is not covered by LTSR core component support. However, the rest of your LTSR infrastructure retains its existing support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

1. Download the `Director2411.zip` file from the Citrix downloads page.
2. Unzip the installer file, and can find the following installers:
   - DesktopDirector.msi
   - Monitor_PowerShellSnapIn.msi
   - Monitor_Service_x64.msi
3. Ensure you are using a Citrix Virtual Apps and Desktops 2402 LTSR or 2402 LTSR CU1 site.

High-level overview

To upgrade a Citrix Virtual Apps and Desktops 2402 LTSR CU1 site with the latest features of the Current Release, follow these steps:

1. **Backup your database**: Before upgrading, ensure you back up the Monitoring database. This procedure is crucial as the upgrade process also updates the database.
2. **Upgrade your site**: Proceed with upgrading your site to incorporate the new features of the current release.
3. **Rollback option**: If you decide not to continue with the upgraded site, you can revert to your previous site using the rollback steps.

Upgrade steps

1. Take a back up of the Monitoring database.
2. Download the `Director2411.zip` file from the Citrix downloads page.
3. Unzip the installer file, and can find the following installers:
   - DesktopDirector.msi
   - Monitor_PowerShellSnapIn.msi
   - Monitor_Service_x64.msi
4. Navigate to the location of the .msi files.
5. Install the Monitor service using the command line:

```
msiexec /i Monitor_service_x64 REINSTALLMODE=amus /l*v <logfile
    path and name>
```

6. Follow the onscreen instructions and complete the wizard.
7. Install Director service using the command line:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
msiexec /i DesktopDirector /l*v <logfile path and name>
```

8. Follow the onscreen instructions and complete the wizard.
9. Run the following command using the command line.

```
DirectorConfig.exe /UPGRADE
```

10. Install Monitor Snap-in using the command line

```
msiexec /i Monitor_PowershellSnapin_x64.msi
```

11. Once all the .msi installation is complete, navigate to the Monitor service in Program Files and run the command:

```
Citrix.Monitor.exe /upgrade /enablefeatures
```

12. Open Citrix Site Manager and select the **Automatic Site Upgrade** option and complete the upgrade workflow.
13. Sign in to the Director to verify the new features are available.

Rollback steps

1. Make sure to take the backup of the Monitoring database.
2. Download and run the database rollback script named dbollback.zip.
3. Uninstall the following from the Control Panel:
   - Select **Citrix Monitor Service PowerShell Snap-in- x64** and click **Uninstall**.
   - Select **Citrix Monitor Service - x64** and click **Uninstall**.
   - Select **Citrix Director** and click **Uninstall**.
4. Restore the monitoring database from the backup that you have taken already. For more information, see the knowledge-sharing article CTX135207.
5. Reinstall the Delivery Controller and Director using the Citrix Virtual Apps and Desktops installer. For more information, see install core components

   Or,

You can also reinstall the components using the following command:

```
XenDesktopServerSetup.exe /components controller,director /
   configure_firewall /quiet
```

1. Once the installation is complete, select the **Open Citrix Site Manager** checkbox.
2. Perform a site upgrade if suggested in the Citrix Site Manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support and compliance

Support

- The Cumulative Release (CR) versions of Director are LTSR compatible, but not LTSR compliant.
- Once upgraded, all support tickets, and bug fixes required are added to the following Cumulative Release (CR) for Director.
- The CR with the changes or fixes are made available in the following Cumulative Updates (CU).

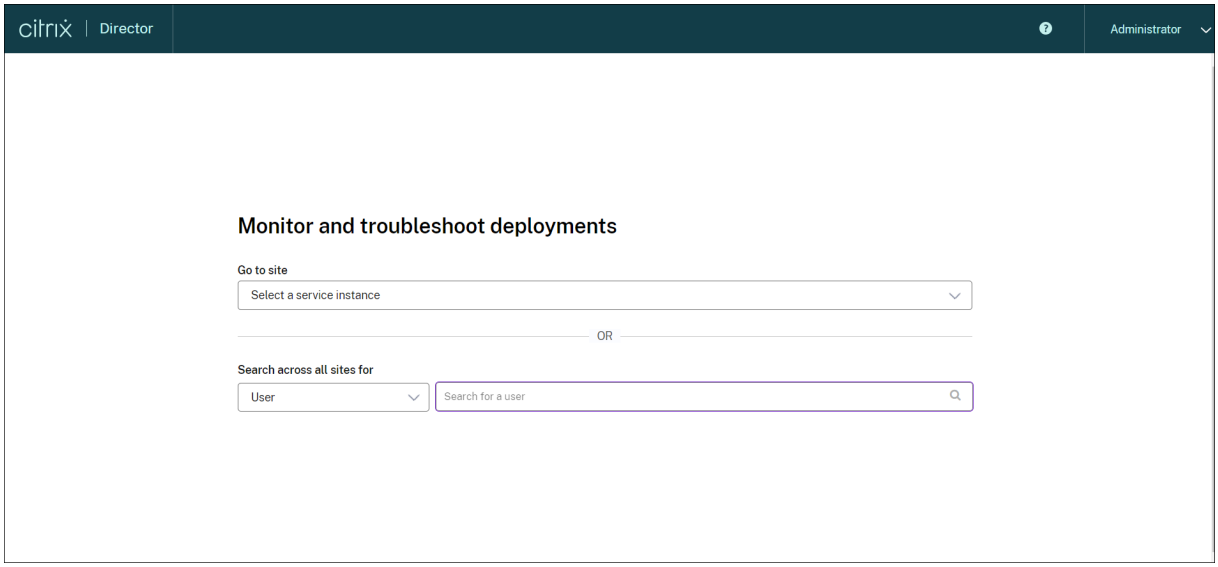
508/WCAG 2.1

- For customers with the 508/wcag 2.1 compliance mandate, it is recommended to continue to use the LTSR version of all core components.

Site Analytics

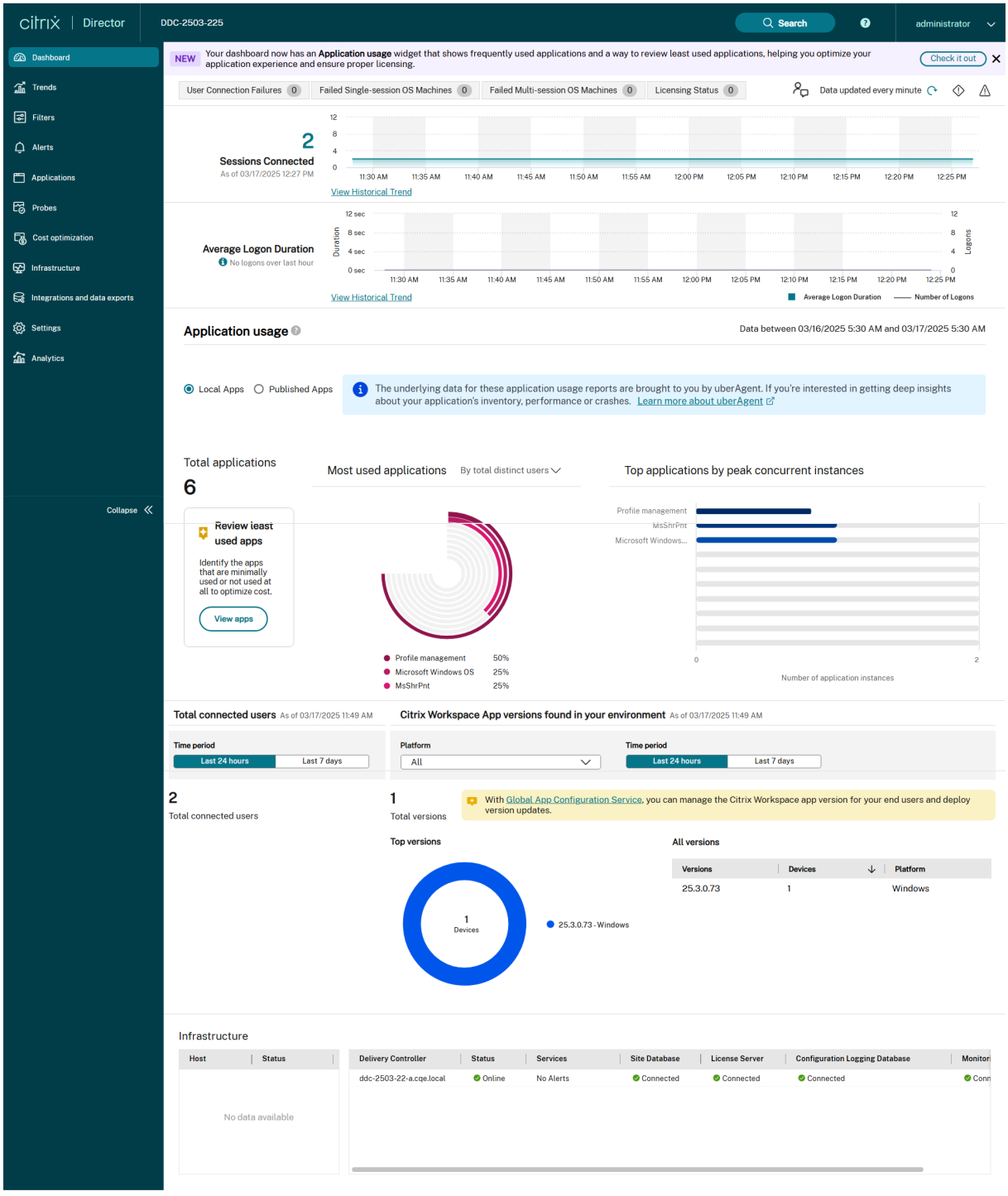
September 6, 2025

Using Director, you can monitor the health your deployments. You can troubleshoot performance issues by searching for a user, endpoint, or machine across all onboarded sites.



With full administrator permission, when you open Director, the Dashboard provides a centralized location to monitor the health and usage of a site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If there are 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.

> **Note:**
>
> Depending on your organization's license and your Administrator privileges, some options or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> features might not be available.

Panels on the Director Dashboard

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 broken out by delivery groups. 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 broken out by 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.

Licensing Status

License Server alerts display alerts sent by the License Server and the actions required to resolve the alerts. Requires License Server Version 11.12.1 or later. Delivery Controller alerts display the details of the licensing state as seen by the Controller and are sent by the Controller. Requires Controller for XenApp 7.6 or XenDesktop 7.6 or later. You can set the threshold for alerts in Studio. Licensing status displayed in **Delivery Controllers** > **Details** > **Product Editions** > **PLT** indicates **Premium** and not **Platinum**.

Grace State

Director displays one of the following grace states. This information is fetched from the Delivery Controller.

1. **Not Active:** Not in any type of License caching mode. Normal licensing limits apply.
2. **Emergency Grace:** Comes into effect when the license server is unreachable or the license information cannot be fetched while brokering a connection. Users are not affected. Errors shown in Director cannot be dismissed until the license server is reachable.
3. **Grace Expired:** Emergency License caching mode has expired.

For more information, see License overdraft and License burst mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sessions Connected

Connected sessions across all delivery groups for the last 60 minutes.

Average Logon Duration

Logon data for the last 60 minutes. The large number on the left is the average logon duration across the hour. Logon data for VDAs earlier than XenDesktop 7.0 is not included in this average. For more information, see Diagnose user logon issues.

Infrastructure

Lists your site's infrastructure - hosts and Controllers. For infrastructure from XenServer or VMware, you can view performance alerts. For example, you can configure XenCenter to generate performance alerts when CPU, network I/O, or disk I/O usage go over a specified threshold on a managed server or virtual machine. By default, the alert repeat interval is 60 minutes, but you can configure this as well. For details, see the XenCenter Performance Alerts section in the XenServer product documentation.

> **Note:**
>
> If no icon appears for a particular metric, this indicates that this metric is not supported by the type of host you are using. 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 following sections):

- Control user machine power
- Prevent connections to machines

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.

Monitor 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.

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 and 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, where 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. Filter the sessions 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 disconnect. For more information, see Troubleshoot applications.
View data over a longer period of time	On the Trends view, select the **Sessions** tab to drill down to more specific usage data for connected and disconnected sessions over a longer period of time (that is, session totals from earlier than the last 60 minutes). To view this information, click **View historical trends**.

> **Note:**
>
> If the user device is running a legacy Virtual Delivery Agent (VDA), such as a VDA earlier than version 7, or a Linux VDA, Director cannot display complete information about the session. Instead,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> it displays a message that the information is not available.

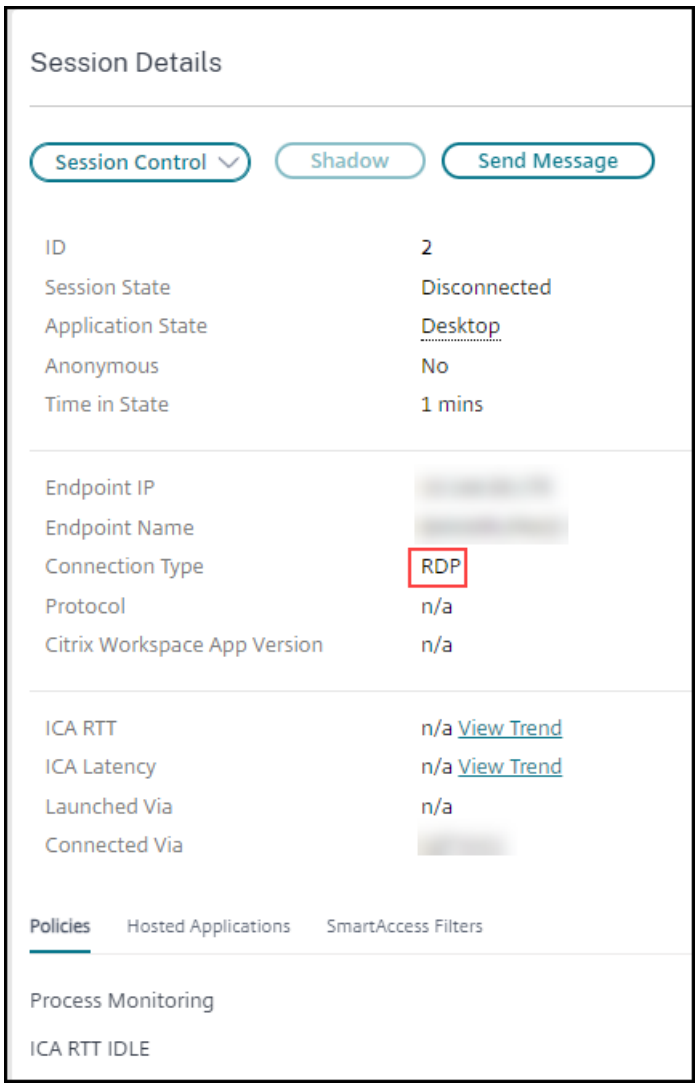
Desktop Assignment Rules limitation:
Web Studio allows assignment of multiple Desktop Assignment Rules (DAR) for different users or user groups to a single VDA in the delivery group. StoreFront™ displays the assigned desktop with the corresponding **Display Name** as per the DAR for the logged in user. However, Director 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 Director.
You can map the assigned desktop displayed in StoreFront to the delivery group name displayed in Director using 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
```

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.



- For **HDX™** Connection type,
  - The Protocol is displayed as **UDP**, if EDT is used for the HDX connection.
  - 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 cannot be established using EDT, it falls back to the TCP protocol.

For more information about adaptive transport configuration, see Adaptive Transport.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 contain trends represented as graphs and tables. CSV format reports contain tabular data that can be processed to generate views or can be archived.

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 name and format of the report.

Director generates the report based on the filter criteria 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 Director 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.

You can change the default limit by configuring the Director Application Settings in Internet Information Services (IIS).

Report format	Default number of records supported	Fields in Director Application Settings	Max number of records supported
PDF	500	UI.ExportPdfDrilldownLimit	5000
Excel	100,000	UI.ExportExcelDrilldownLimit	1,000,000
CSV	100,000 (10,000,000 in **Sessions** tab)	UI.ExportCsvDrilldownLimit	10,000,000

To change the limit of the number of records you can export:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the IIS Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Edit or add a setting for the fields UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownLimit, or UI.ExportCsvDrilldownLimit as required.

Adding these field values in Application Settings overrides the default values.

> **Warning:**
>
> Setting field values greater than the max number of records supported can impact the performance of Export and is not supported.

Error Handling

This section gives you information on dealing with errors that you might encounter during Export operation.

- **Director has timed out**

This error can occur due to network issues or high resource usage on the Director server or with the Monitor Service.

The default timeout duration is 100 seconds. To increase the timeout duration of the Director Service, set the value of **Connector.DataServiceContext.Timeout field in** Director Application Settings in Internet Information Services (IIS):

1. Open the IIS Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Edit the value **Connector.DataServiceContext.Timeout**.

- **Monitor has timed out**

This error can occur due to network issues or high resource usage with the Monitor Service or on the SQL server.

To increase the timeout duration of the Monitor Service, run the following PowerShell commands on the Delivery Controller:

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **Max concurrent Export or Preview operations ongoing**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director supports one instance of Export or Preview. If you get the **Max concurrent Export or Preview operations ongoing** error, try the next Export operation again later.

It is possible to increase the number of concurrent Export or Preview operations, however this can impact the performance of Director and is not supported:

1. Open the IIS Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Edit the value **UI.ConcurrentExportLimit**.

- **Insufficient disk space in Director**

Each Export operation requires a maximum of 2 GB hard disk space in the Windows Temp folder. Retry Export after clearing space or adding more hard disk space on the Director server.

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 Director, 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 is not 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 example, select machines that appear in Director as "failed to start,"and use this command to restart them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Command	Function
Force Restart	Restarts the VM without first performing 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 performing 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.

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 as soon as all users are logged off. For users who do not log off, send a message informing them that machines will be shut down at a certain time, and 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 indicating that the desktop is unavailable. No new connections can be made until you disable maintenance mode.

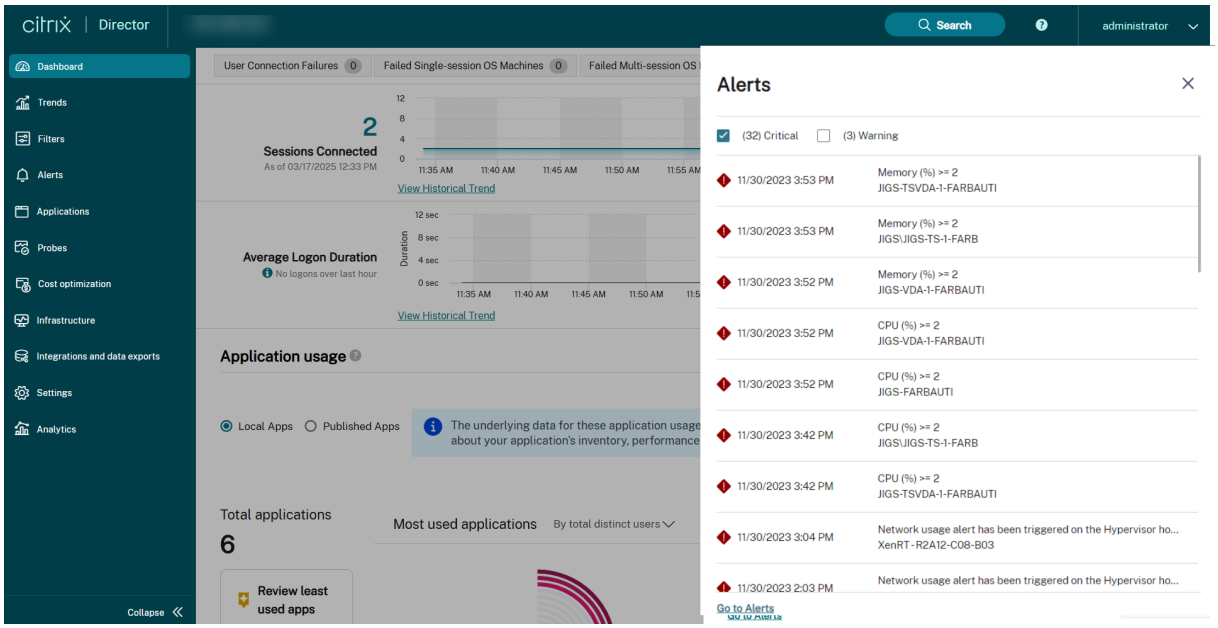
Application Analytics

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 probe results, number of instances per application, and faults and errors associated with the published applications. For more information, see the Application Analytics section in **Troubleshooting Applications**.

Alerts and notifications

September 6, 2025

Alerts are displayed in Director on the dashboard and other high-level views with warning and critical alert symbols. Alerts are available for **Premium** licensed sites. Alerts update automatically every minute; you can also update alerts on demand.



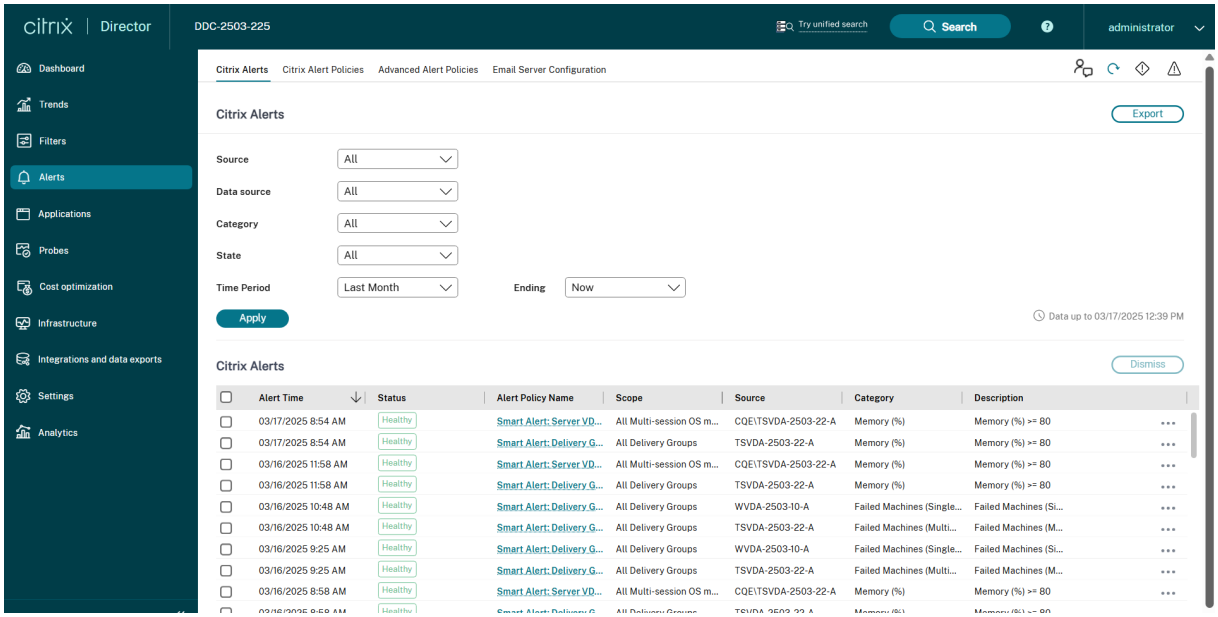
A warning alert (amber triangle) indicates that the warning threshold of a condition has been reached or exceeded.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Director 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.



Citrix® alerts

Citrix alerts are alerts monitored in Director that originate from Citrix components. You can configure Citrix alerts within Director 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.

> **Note:**
>
> Ensure that your firewall, proxy, or Microsoft Exchange Server do not block the email alerts.

Smart alert policies

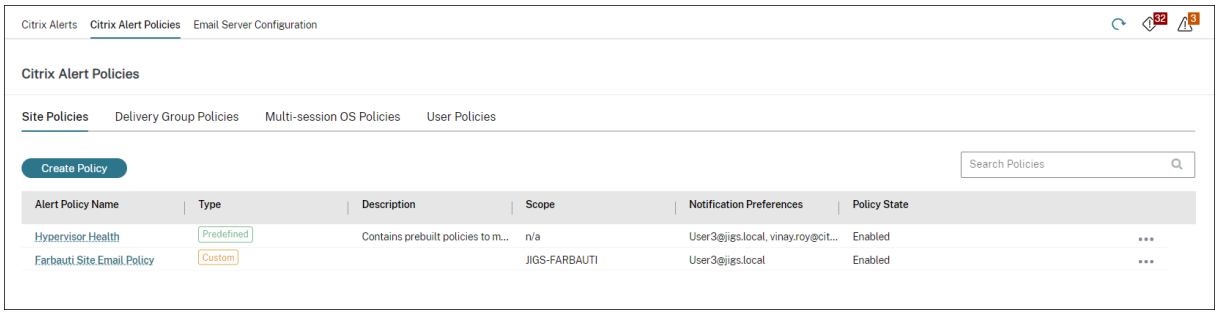
A set of built-in alert policies with predefined threshold values is available for Delivery Groups and Multi-session OS VDA scope. This feature requires Delivery Controller(s) version 7.18 or later. You can modify the threshold parameters of the built-in alert policies in **Alerts** > **Citrix Alerts Policy**.
These policies are created when there is at least one alert target -a Delivery Group or a Multi-session OS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA defined in your site. Additionally, these built-in alerts are automatically added to a new delivery group or a Multi-session OS VDA.

In case you upgrade Director and your site, the alert policies from your previous Director instance are carried over. 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.



Advanced alert policies

The Proactive Notification and Alerting feature of the Director 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.

You can create an Advanced alert policy from the **Alerts** > **Advanced alert policy** > **Create Policy** section.

You can select the one of the following Data source:

- Machines
- Provisioning Service
- StoreFront™
- Delivery Controller™

© 1997–2026 Citrix Systems, Inc. All rights reserved.

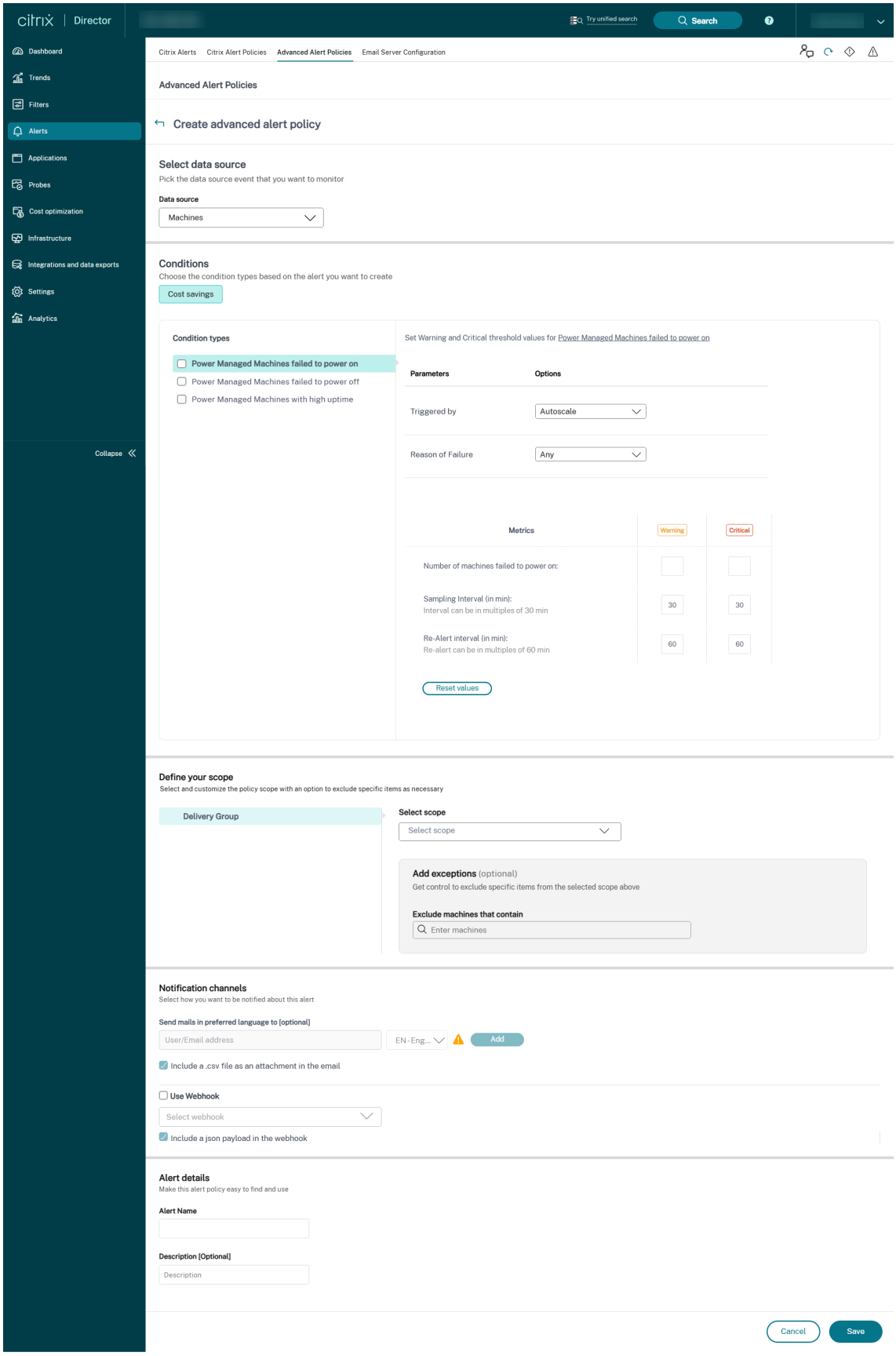
Alerts for cost savings

You can create alerts for cost savings which help you optimize costs. Currently, you can create alerts for machines.

To create alerts on Machines, do the following:

1. Click the **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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select the following condition types as required:
    - Power Managed Machines failed to power on
    - Power Managed Machines failed to power off
    - Power Managed Machines with high uptime
5. Select the specific parameters and the corresponding options for each of the selected conditions.
6. 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 a minimum of 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
7. Schedule re-alert intervals for the selected alerts as needed.
8. Define the scope of the alert.
9. Set the notification channels. This can be email or Webhook.
    a) 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

    For more information, see Enhancements on alert content.
10. Enter the **Alert details** such as **Alert Name** and **Description** (optional).
11. Click **Save**. The alert is created.

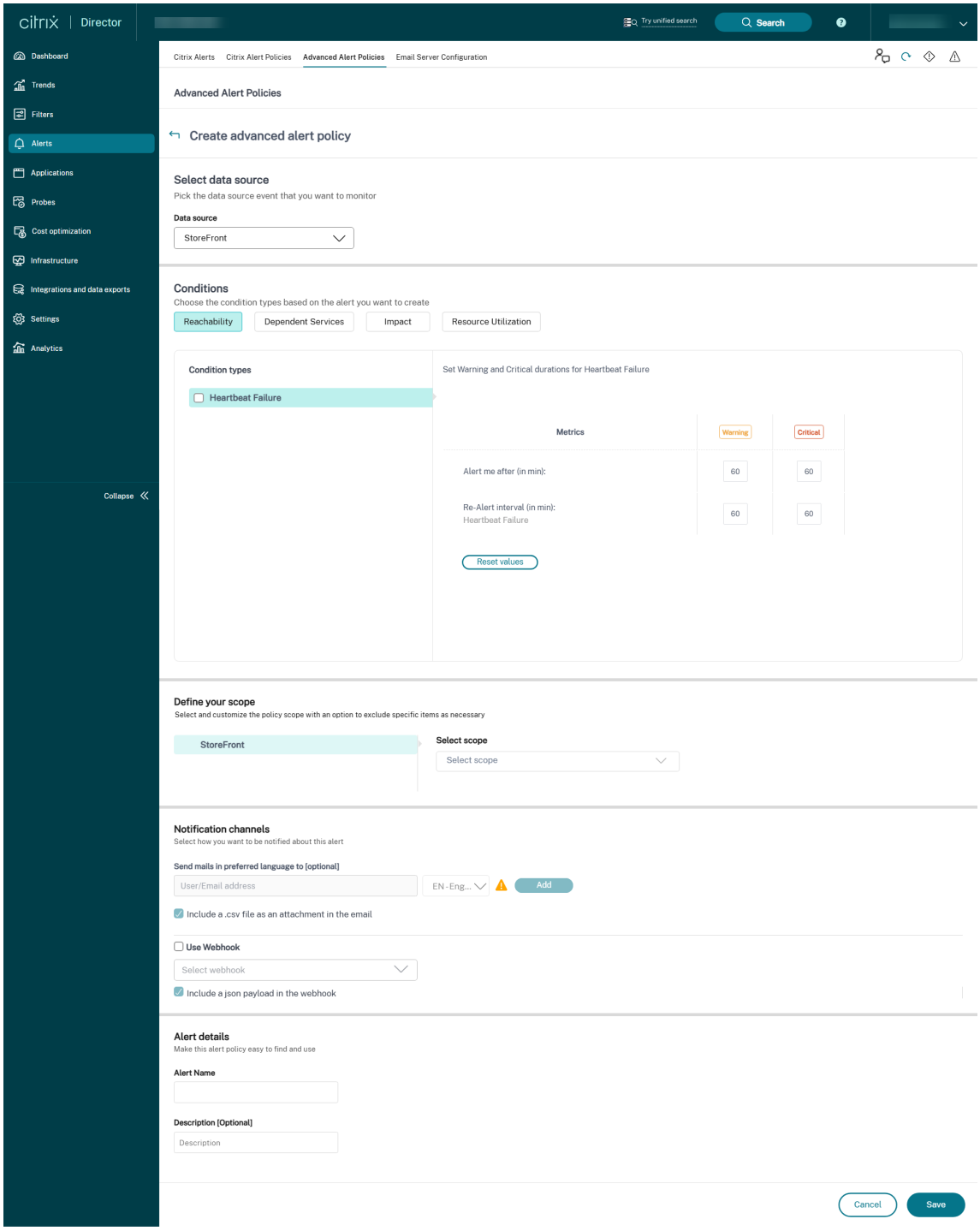
Alerts for infrastructure monitoring

You can create alerts to monitor the health of the following supported Citrix Virtual Apps and Desktops™ components:

- Provisioning Service

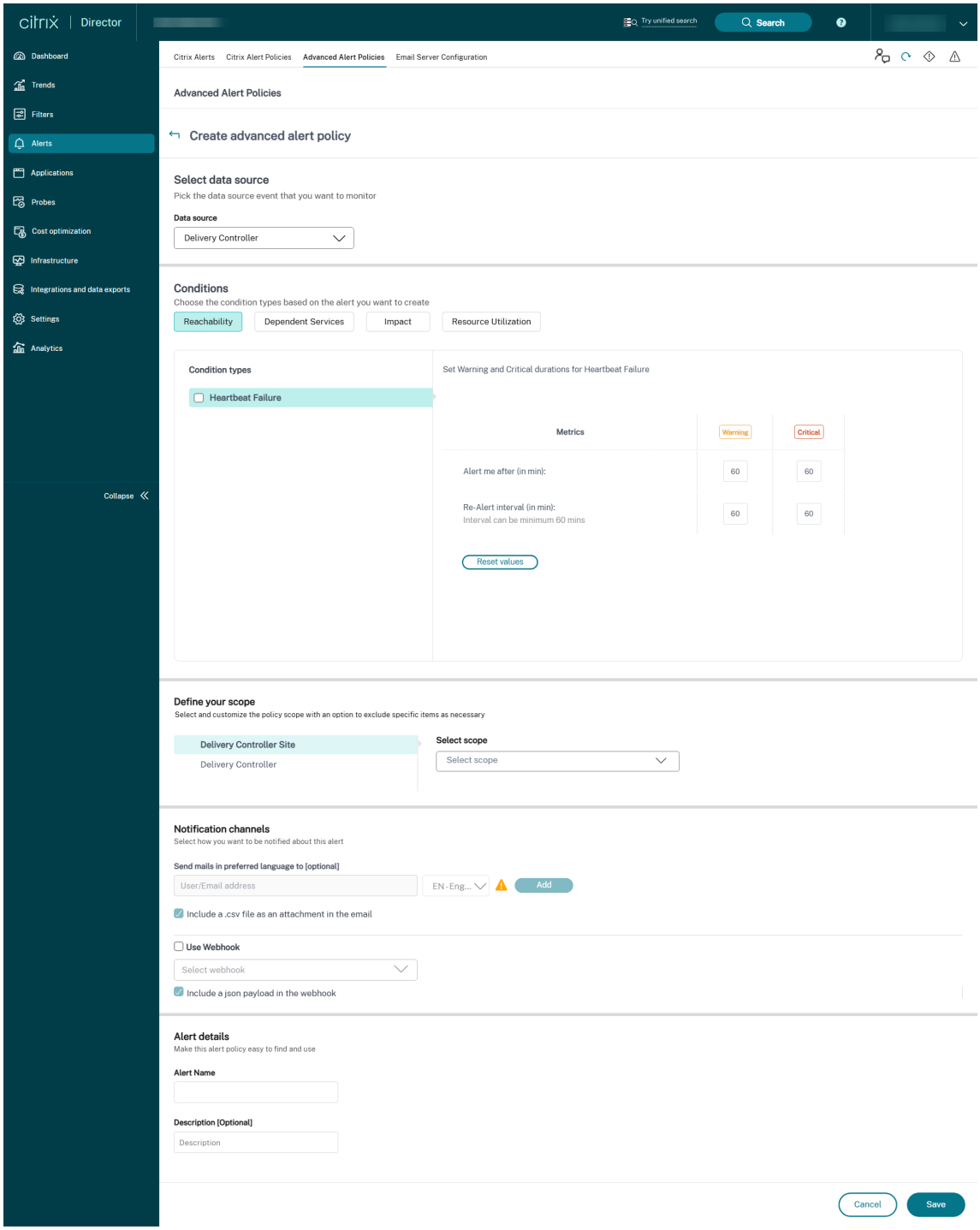
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- StoreFront



- Delivery Controller

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once the Infrastructure monitoring setup is completed, you can use the health data available in Director 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. For Provisioning Service and Delivery Controller, you can select the scope of alerts as either site level or individual server level. For example, in the case of Provisioning Service, if you select "All Provisioning Service,"you will receive only a single alert for the entire site, even if the site has two servers. This is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

considered a site-level alert. 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.

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 Service health metrics
- StoreFront health metrics
- Delivery Controller 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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
# Add Target UID's
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

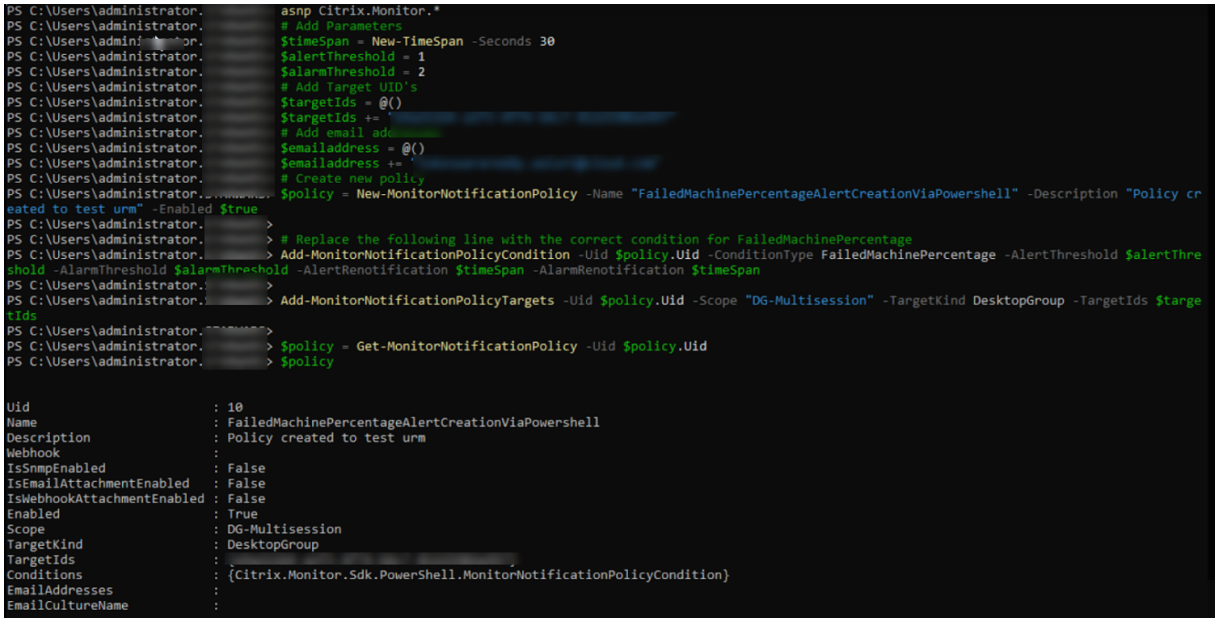
```
$targetIds = @()
$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"
# Add email addresses
$emailaddress = @()
$emailaddress += "loki@abc.com"
# Create new policy
$policy = New-MonitorNotificationPolicy -Name "
    FailedMachinePercentageAlertCreationViaPowershell" -Description "
    Policy created 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
```



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
```

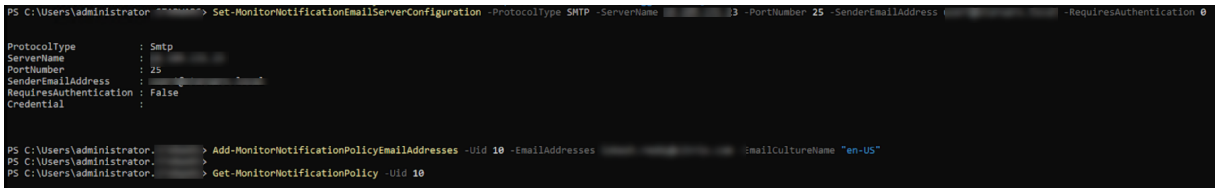
To add email to policy

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid -
    EmailAddresses $emailaddress -EmailCultureName "en-US"
```

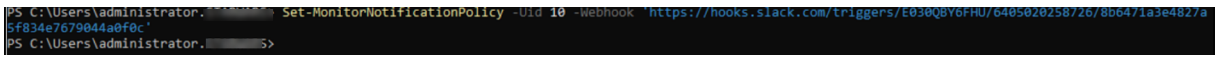
Sample script to add email:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
    $emailaddress -EmailCultureName "en-US"
```



To add Webhook URL to policy

```
Set-MonitorNotificationPolicy  – Uid $polcy.Uid  – Webhook 'URL'
```

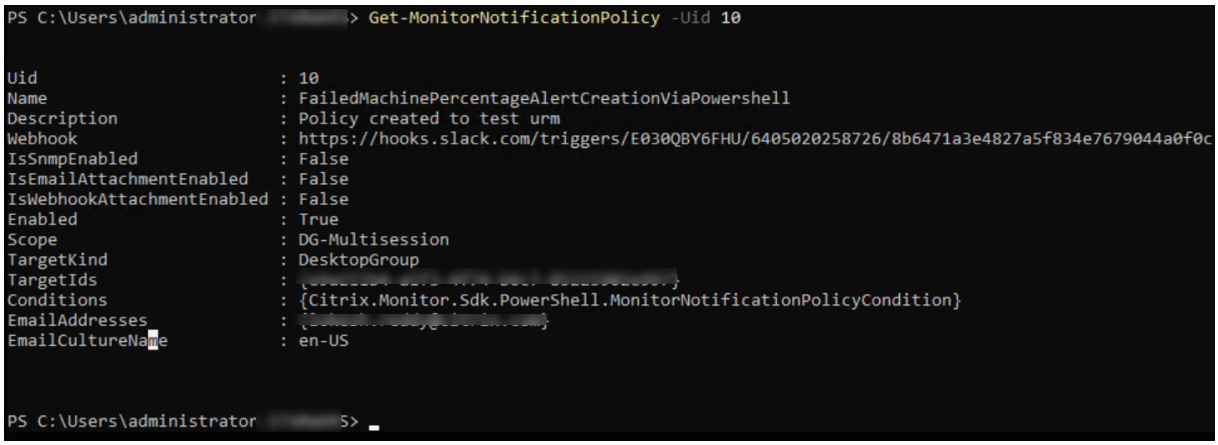


Sample scipt to add webhook URL:

```
Set-MonitorNotificationPolicy  – Uid 10   – Webhook  'https://hooks.slack
    .com/triggers/E030QBY6FHU/6405020258726/8
    b6471a3e4827a5f834e7679022a1f1c'
```

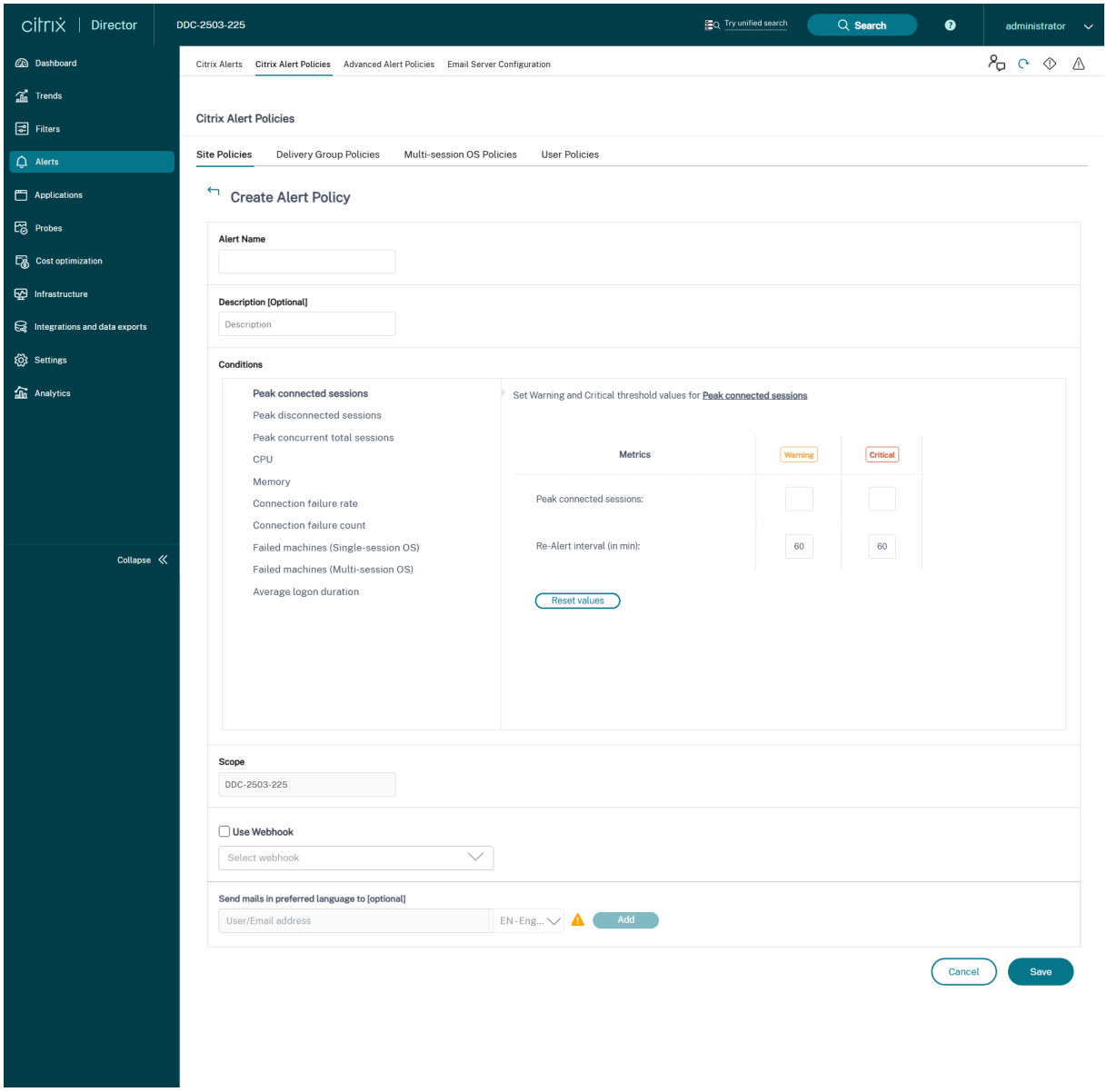
Get Created Policy details

```
Get-MonitorNotificationPolicy -Uid 10
```



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create alert policies



To create an alert policy, for example, to generate an alert when a specific set of session count criteria is 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 must be notified by email when the alert is triggered. You have to specify an email server on the **Email Server Configuration** tab to set email Notification preferences in Alerts Policies.

    a) You can also receive the alert content in a .CSV attachment or through the json payload. For this, select the following checkboxes:

    - **Include a json payload as an attachment in the webhook**
    - **Include a csv file as an attachment in the email**

> **Note:**
>
> To receive alert content through .CSV attachment and json payload options are available only for a few alerts currently. For more information, see Enhancements on alert content

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 Director 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

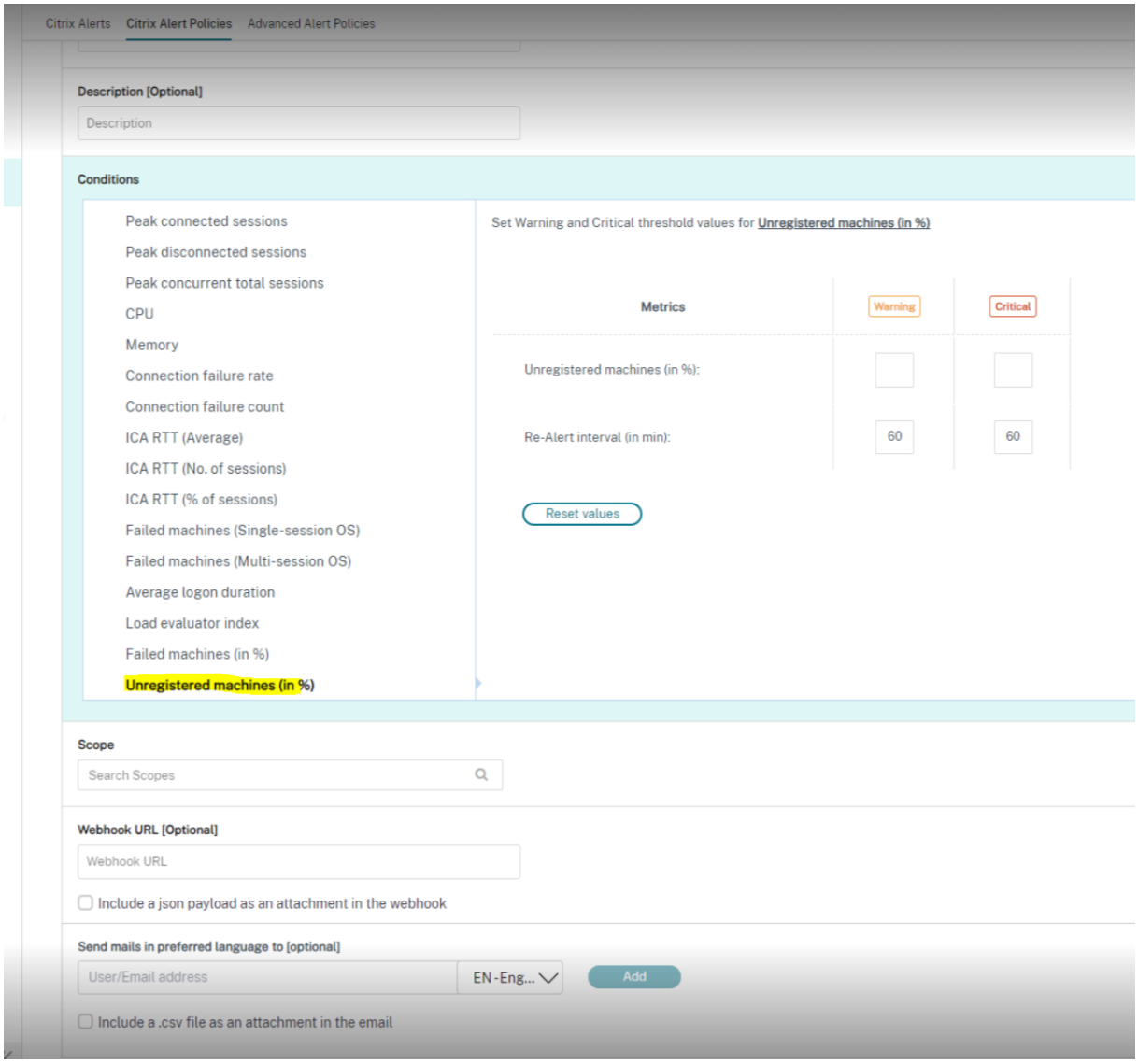
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Failed power on actions
- Failed power off actions
- Unregistered machines (%)

To use this feature, navigate to the alert and select the following checkboxes:

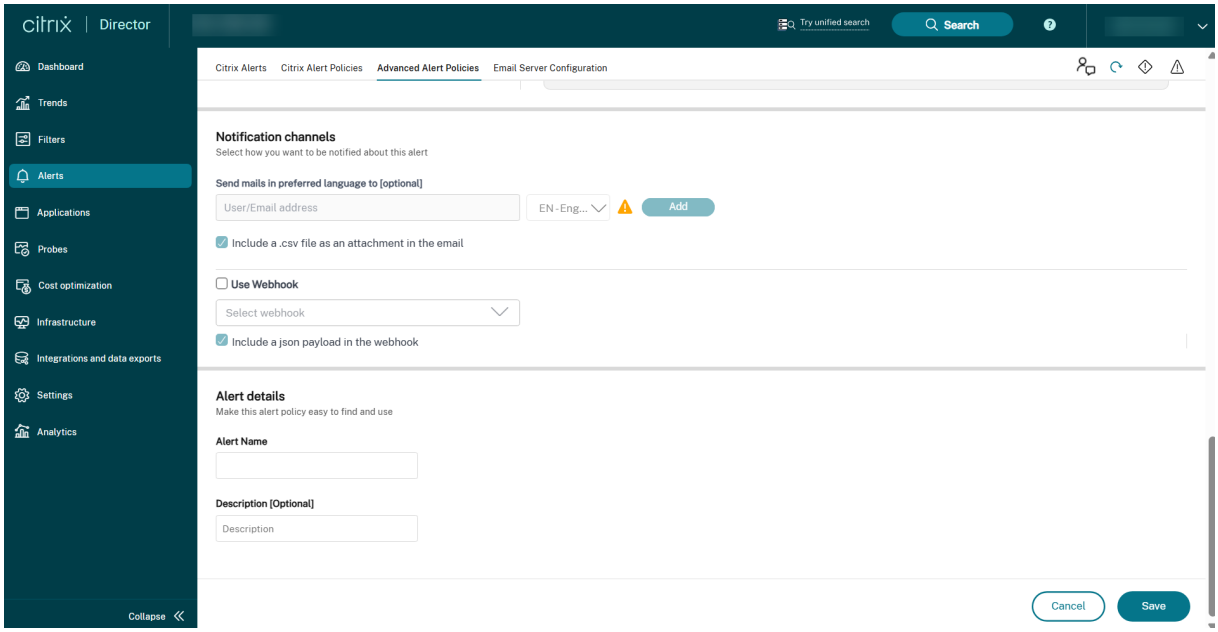
- **Include a json payload as an attachment in the webhook**
- **Include a csv file as an attachment in the email**

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>\",\"Condition
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      \":\"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,
    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\":\"<IPV4
    Address of the Machine>\",\"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>\" }
 ] }
 "
 }
```

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 (
    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 }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
,{
\"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 Director 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 Director 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 Director Session Trends view in Director 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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 additional CPU resources in the future.

> **Note:**
>
> The **Enable resource monitoring** policy setting 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 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 additional memory in the future.

> **Note:**
>
> The **Enable resource monitoring** policy setting 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 Director 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 Director 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 Citrix ADM documentation.
- If Citrix ADM is not available, check the Director 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.

- Check Citrix ADM for the number of sessions with high ICA RTT. For more information, see Citrix ADM documentation.
- If Citrix ADM is not available, work with 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 - 400ms for 10 or more sessions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Citrix ADM documentation.
- If Citrix ADM is not available, work with 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 Director Dashboard and Filters views.

- Run Citrix Scout diagnostics to determine the root cause.

  Smart policy conditions:

  - **Scope:** Delivery Group, Multi-session OS 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 Director Dashboard and Filters views.

- Run Citrix Scout diagnostics to determine the root cause.

  Smart policy conditions:

  - **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Failures can occur for various reasons as shown in the Director 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 the 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 Director 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 alerts under **Citrix Alerts**. You can filter it by **Unregistered Machines (in %)** category and for the required state and time.

You can also receive alert details in a CSV attachment if there is an email or through a JSON payload if there is a webhook.

> **Note:**
>
> The critical value must be greater than the warning value.

Policy conditions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 if there is an email or through a JSON payload if there is a webhook.

Average Logon Duration

Average logon duration for logons that occurred over the last hour.

- Check the Director Dashboard to get up-to-date metrics regarding the logon duration. Many 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Director 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 a new alerts policy with a webhook URL:

```
$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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{
 "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\>,

"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or
    dismissed\>,

"Site" : \<Site name\> }
```

Bulk alert dismissal

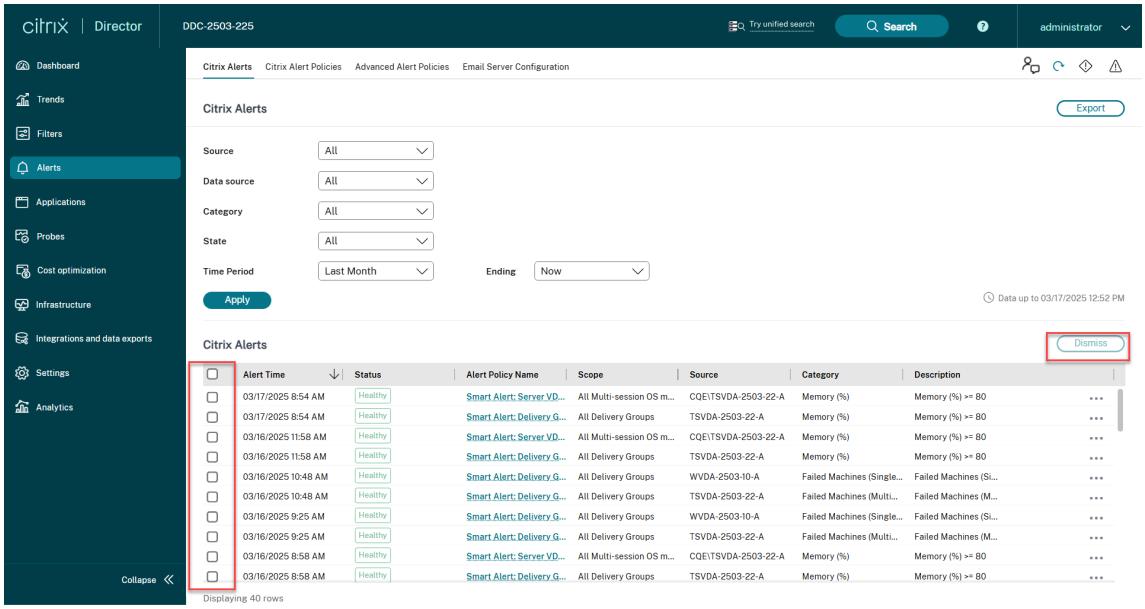
This feature optimizes the alert management process for administrators, providing flexibility and reducing alert fatigue. Administrators can bulk dismiss alerts based on time, type, or category, simplifying alert management during maintenance or when dealing with hypervisors and other environments.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 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:

To create a webhook without authorization header:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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 "profile_slack" -Description "webhook
    profile for slack" -Url $url -Headers $headers -PayloadFormat
    $payloads
```

To create a webhook with authorization header:

```
$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>")

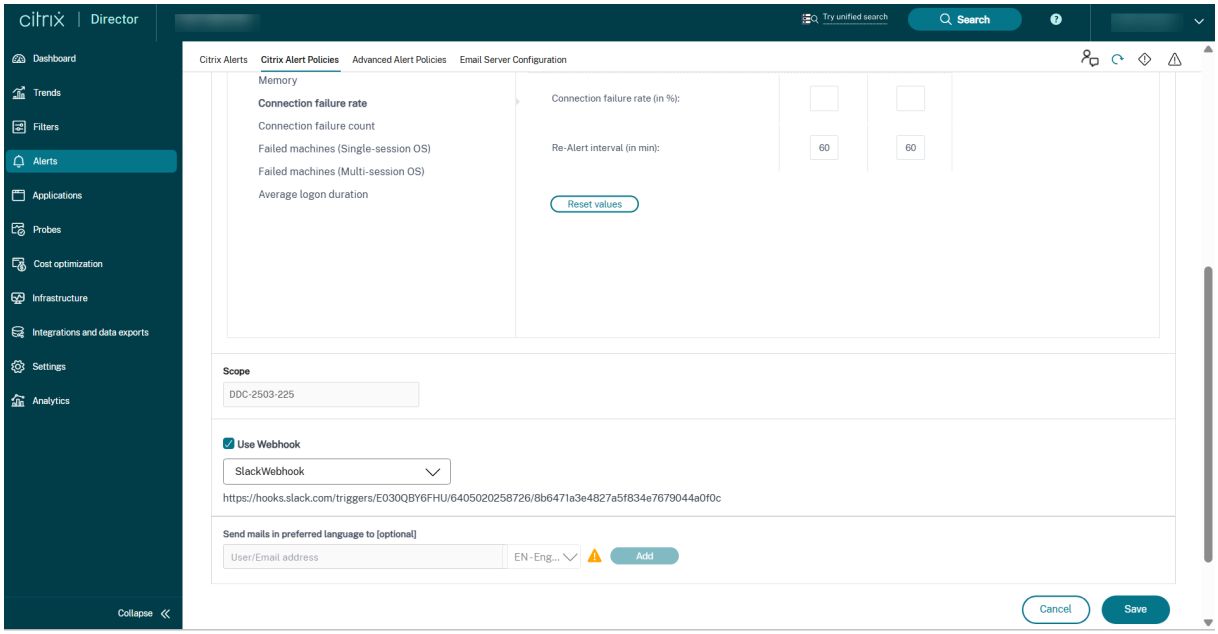
$payloads = '{
  "text": "$PAYLOAD"  }
 '

$url = "<Fill this field with the required URL>"

Add-MonitorWebhookProfile -Name "profile_azure" -Description "webhook
    profile for azure function with Authentication" -Url $url -Headers
    $headers -PayloadFormat $payloads
```

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
```

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
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>")

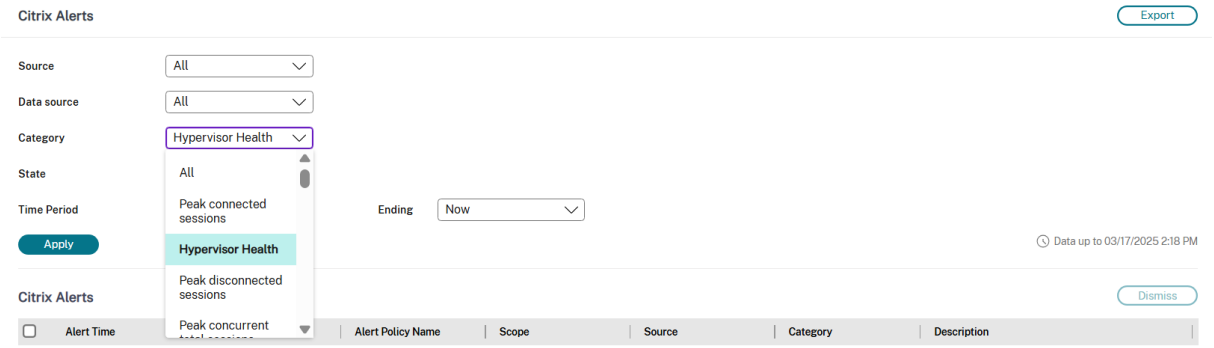
$payloads = '{
  "text": "$PAYLOAD"  }
 '
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
10
11 $url ="<Fill this field with the required URL>"
12
13 Test-MonitorWebhookProfile -Url $url -Headers $headers -PayloadFormat
      $payloads
```

Hypervisor Alerts Monitoring

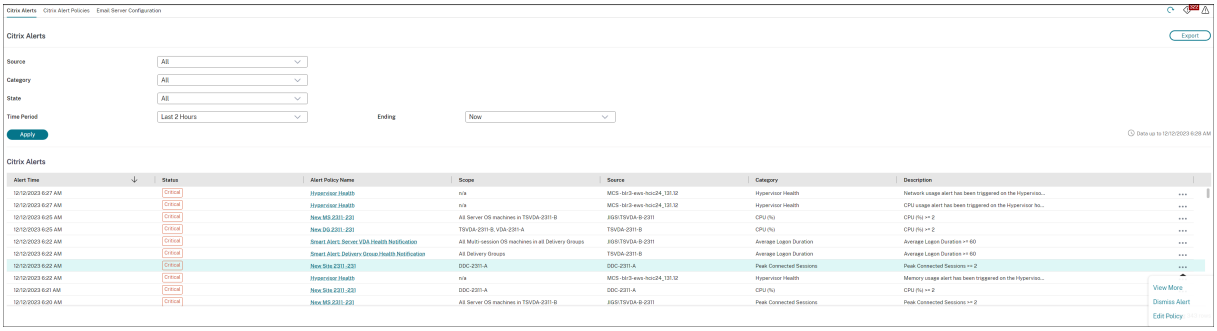
Director displays alerts to monitor hypervisor health. Alerts from XenServer® and VMware vSphere help monitor hypervisor parameters and states. The connection status to the hypervisor is also monitored to provide an alert if the cluster or pool of hosts is rebooted or unavailable.



To receive hypervisor alerts, ensure that a hosting connection is created in Web Studio. For more information, see Connections and resources. Only these connections are monitored for 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



This feature requires Delivery Controller version 7 1811 or later. If you are using an older version of Director with sites 7 1811 or later, only the hypervisor alert count is displayed. To view the alerts, you must upgrade Director.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following table describes the various parameters and states of Hypervisor alerts.

Alert	Supported Hypervisors	Triggered by	Condition	Configuration
CPU usage	XenServer, VMware vSphere	Hypervisor	CPU usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Memory usage	XenServer, VMware vSphere	Hypervisor	Memory usage alert threshold is reached or exceeded	Alert thresholds must be configured in the Hypervisor.
Network usage	XenServer, 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	XenServer, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> For more information about configuring alerts, see Citrix XenCenter Alerts or check the VMware vCenter Alerts documentation.

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 Director. However, modifying email preferences and dismissing an alert can be done in Director. You can disable the alert if your role does not involve infrastructure monitoring.

> **Important:**
>
> - Alerts triggered by the Hypervisor are fetched and displayed in Director. However, changes in the life cycle/state of the Hypervisor alerts are not reflected in Director.
> - Alerts that are healthy or dismissed or disabled in the Hypervisor console continues to appear in Director and have to be dismissed explicitly.
> - Alerts that are dismissed in Director are not dismissed automatically in the Hypervisor console.

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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application usage monitoring

September 13, 2025

Citrix Director helps you to monitor the usage of following:

- Applications launched within virtual desktop sessions (also known as local applications)
- Applications launched from the Citrix Workspace™ app session directly (also know 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 contains curated charts. These charts help the IT admins or application admins to gain insight into which applications are heavily used and the extent of their usage.

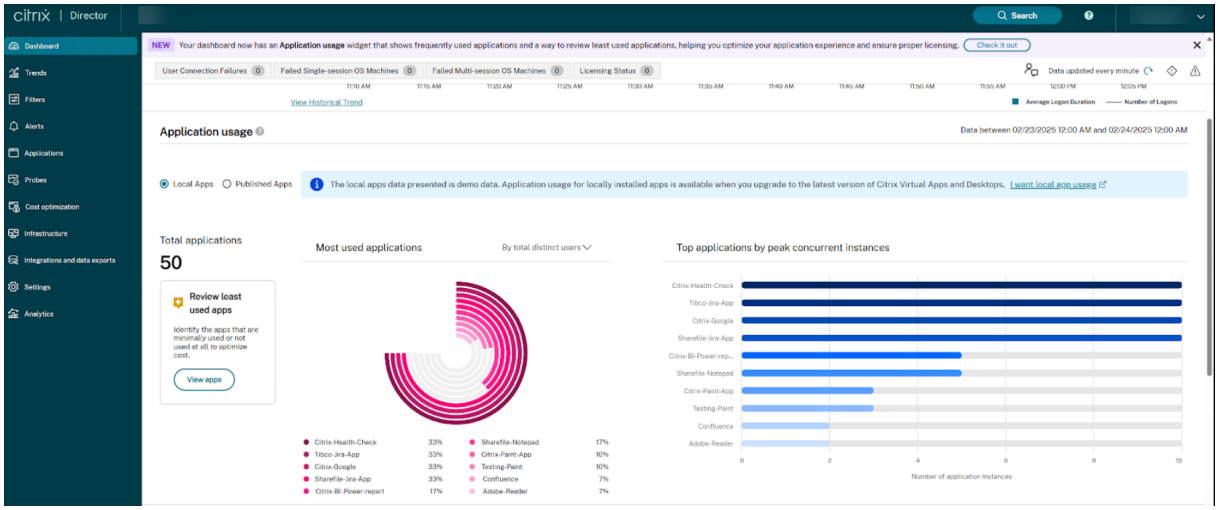
> **Note:**
>
> - This feature is available only for the platinum-licensed sites.
> - uberAgent must be integrated with Director for monitoring usage of local applications. For more information, see Citrix uberAgent integration with Director.
> - If your environment delivers the same application as both a published app and an installed app within the desktop (local app), you might see the app listed in both the published apps and local apps reports.

With this feature, an admin can view which local and 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 Virtual Apps and Desktops™ 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.

Requirements

- Delivery Controllers Version 7.16 or later
- VDAs version 7.15 or later

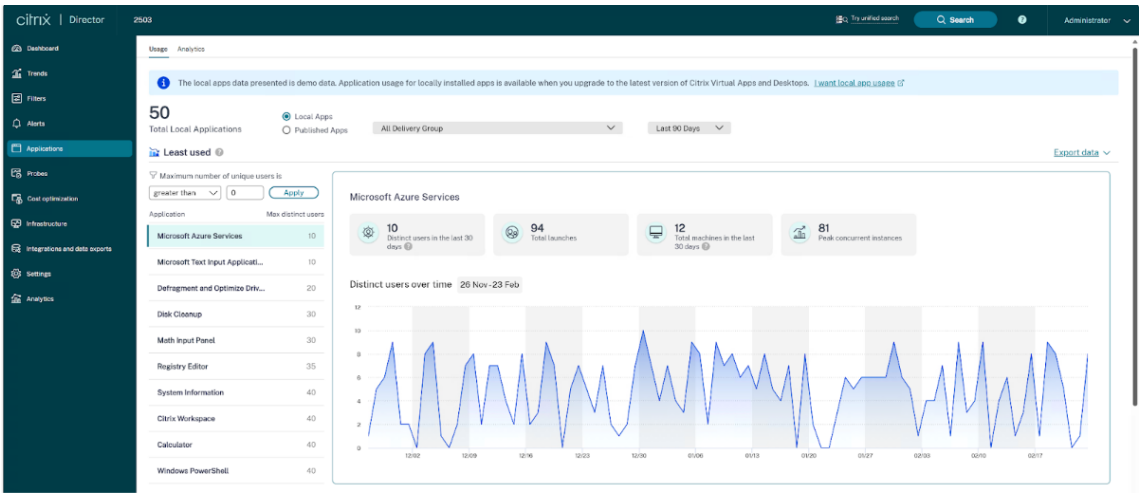
Viewing Application usage details

1. Click the **View apps** link in the **Review least used apps** section on the Dashboard.

   Or,

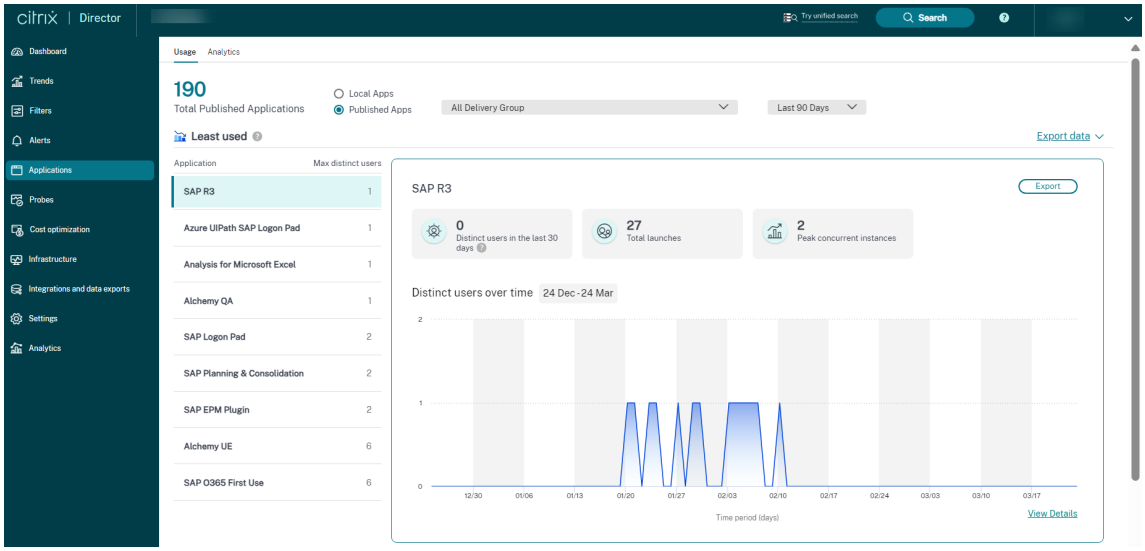
   Click the **Applications** tab. The following page appears:

   When the **Local apps** option is selected:



   When the **Published apps** option is selected:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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:

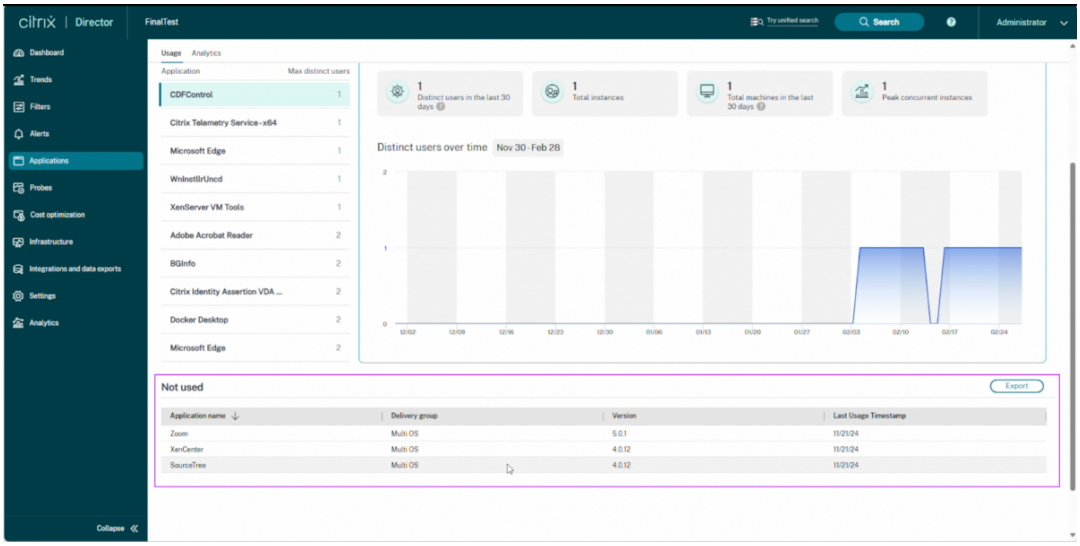
   - **Total Local and published applications:** Displays the total number of local and published applications.
   - **Least used:** Displays the apps with the fewest unique users over the selected time. The calculation is done as follows:

     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 time-frame 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.

     > **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.
    - **Total machines in the last 30 days**: Shows the number of machines installed in the last 30 days. This metric is present only when you view the Local apps details.
    - **Peak concurrent instances:** Displays the highest number of instances running simultaneously.
    - **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 Virtual Apps and Desktops 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 which 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

September 6, 2025

When you click numbers on the Dashboard or select a predefined filter from the Filters menu, the Filters view opens to display data based on the selected machine or failure type.

Predefined filters cannot be edited, but you can save a predefined filter as a custom filter and then modify it. Also, you can create custom filtered views of machines, connections, sessions, and application instances across all delivery groups.

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**. Filter sessions by different time periods, including last 60 minutes, last 24 hours, last 7 days, or custom time period. 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, last 7 days, or custom time period.
    - **Application Instances**. Filter application instances by different time periods, including last 60 minutes, last 24 hours, last 7 days, or custom time period. This view displays the properties of all application instances on VDAs of Server and Single-session OS. The session idle time measurements are available for Application instances on VDAs of Multi-session OS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> If you have launched Desktop sessions on VDAs installed on a Windows 10 1809 computer, the Activity Manager in Director might sometimes display Microsoft Edge and Office as actively running applications while they are actually running only in the background.

2. For **Filter by**, select the criteria.
3. Use the additional tabs for each view, as needed, to complete the filter.
4. Select extra columns, as needed, to troubleshoot further.
5. Save and name your filter.
6. To access filters from multiple Director servers, store the filters on a shared folder accessible from those servers:
   - The shared folder must have modifying permissions for accounts on the Director server.
   - The Director servers must be configured to access the shared folder. To configure, run **IIS Manager**. In **Sites > Default Web Site > Director\ > Application Settings**, modify the **Service.UserSettingsPath** setting to reflect the UNC path of the shared folder.
7. To open the filter later, from the **Filters** menu, select the filter type (Machines, Sessions, Connections, or Application Instances), and then select the saved filter.
8. Click **Export** to export the data to CSV format files. Data of up to 100,000 records can be exported. This feature is available in Delivery Controller™ version 1808 and later.
9. If needed, for **Machines** or **Connections** views, use power controls for all the machines you select in the filtered list. For the Sessions view, use the session controls or option to send messages.
10. 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.
11. 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 Citrix Director failure reasons and troubleshooting.
12. 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.
13. In the **Application Instances** view, sort or filter based on **Idle Time** greater than a threshold time period. Select the idle application instance to end. Log off or Disconnect of an application

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Director, Delivery Controllers, and VDAs are version 7.13 or later.

> **Note:**
>
> Web 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, Director 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 Director. To map the assigned desktop displayed in StoreFront to the delivery group name displayed in Director, 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
```

Monitor historical trends across a site

September 6, 2025

The Trends view accesses historical trend information of each site for the following parameters:

- sessions
- connection failures
- machine failures
- logon performance
- load evaluation
- capacity management
- machine usage
- resource utilization
- network analysis for each site.

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 is affected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To change the default scope of each graph, apply a different filter to the data.

Choose a time period for which you require the historical trend information. Time period availability depends on your Director deployment as follows:

- Trend reports of up to Last year (365 days) are available in Premium licensed sites.
- Trend reports of up to Last month (31 days) are available in Advanced licensed sites.
- Trend reports of up to Last 7 days in non-Premium and non-Advanced licensed sites.

> **Note:**
>
> - In all Director deployments, 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. For the time period chosen as Last month with a custom ending date or as Last year, the trend information is available as graphs and not as tables.
> - Grooming retention values of the Monitor Service control the trends data availability. The default values are available in Data granularity and retention. Customers on Premium licensed sites can change the grooming retention to their desired number of retention days.
> - The following parameters in IIS Manager control the range of custom ending dates available for selection. However, the data availability for selected dates depends on the grooming retention setting for the specific metric being measured.

Parameter	Default values
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Auto client reconnect comes into effect between 3 and 5 minutes where the client tries to connect to the VDA.

Both reconnects are captured and displayed to the user. This information can take a maximum time of 5 minutes to appear on the Director UI after the reconnect has occurred.

The auto reconnect information helps you view and troubleshoot network connections having interruptions. It also analyzes 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 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 Delivery Controller™ version 7 1906 or later, and 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 Director for the following reasons:

- Workspace app is not sending auto reconnect data to VDA.
- VDA is not sending data to the monitor service.
- Delivery Controllers discard VDA payloads as they might not have the corresponding sessions.

> **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 and VDA 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 and VDA duration phases, such as brokering duration and VM start time. This data is specifically for user logons and VDA logons and does

© 1997–2026 Citrix Systems, Inc. All rights reserved.

not include users trying to reconnect from disconnected sessions.
The table below the graph shows Logon Duration by User Session. You 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 or to a PDF. The graph is also exported to these reports. 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 the Multi-session OS machine in a Delivery Group was selected), and range.

View hosted applications usage: The availability of this feature depends on your organization's license.
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 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-session 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, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The number of machines displayed in Available Counter includes machines in maintenance mode.

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 Delivery Controllers and VDAs **version 7.11** or later.
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 processes consuming CPU.

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. For more information, see Monitoring policy settings.
> - 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 could mean that sometimes fewer than 10 processes are listed.

View network analysis data: The availability of this feature depends on your organization's license and your administrator permissions. This feature requires Delivery Controllers **version 7.11** or later.

From the **Network** tab, monitor your network analysis, which provides a user, application, and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment through HDX Insight reports from Citrix ADM. For more information, see Configure network analysis

© 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 Delivery Controllers and 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.

View probe results: The **Probe Results** tab displays the results of probe for applications and desktops that have been configured for probing in the Configuration page. Here, the stage of launch during which the failure occurred is recorded.

For more information see Application and Desktop Probing.

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.

This feature requires Delivery Controllers **version 7.12** or later.

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 additional 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 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.

> **Note:**
>
> - HDX™ connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - Delivery Groups deleted in Citrix Studio are available for selection in the Director 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

September 6, 2025

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 in Web Studio. For more information, see Autoscale.
You can monitor the key metrics of Autoscale enabled machines using Director.

Machine Usage

The **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.

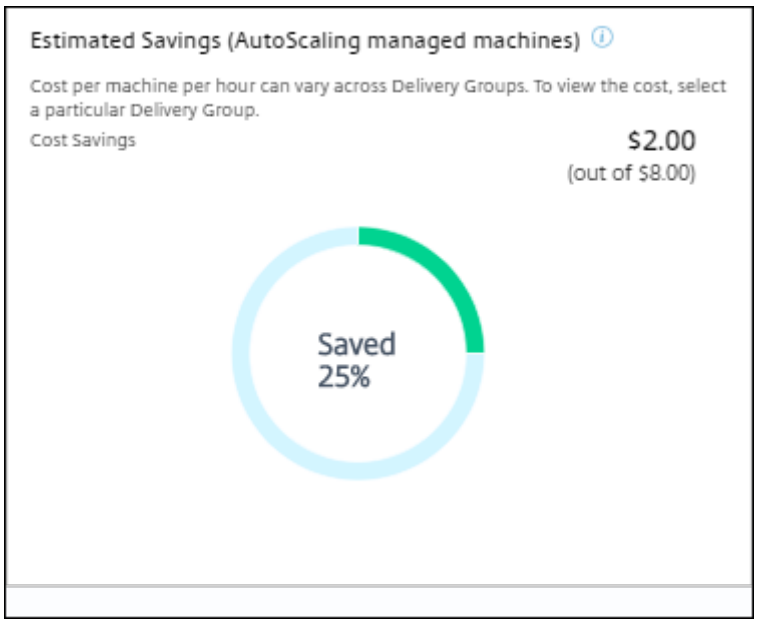
The chart plots the following metrics:

- **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 **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 **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 Director Dashboard displays alert notifications that can be further drilled down. Alert details are displayed on the **Alerts** page.

- To create an alert policy in a delivery group, go to **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

- **Filters** > **Machines** displays the power state of all machines in a tabular format. You can filter by a specific delivery group.
- **Filters** > **Sessions** displays filter by the Machine name to see the associated sessions and their real-time status.
- In **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 **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

September 6, 2025

As a help desk administrator, you can search for the user reporting an issue and display details of sessions or applications associated with that user. Similarly, search for machines or endpoints where issues are reported. Resolve issues quickly by monitoring the relevant metrics and performing suitable actions.

Available actions include:

- 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

September 6, 2025

Real-time application monitoring

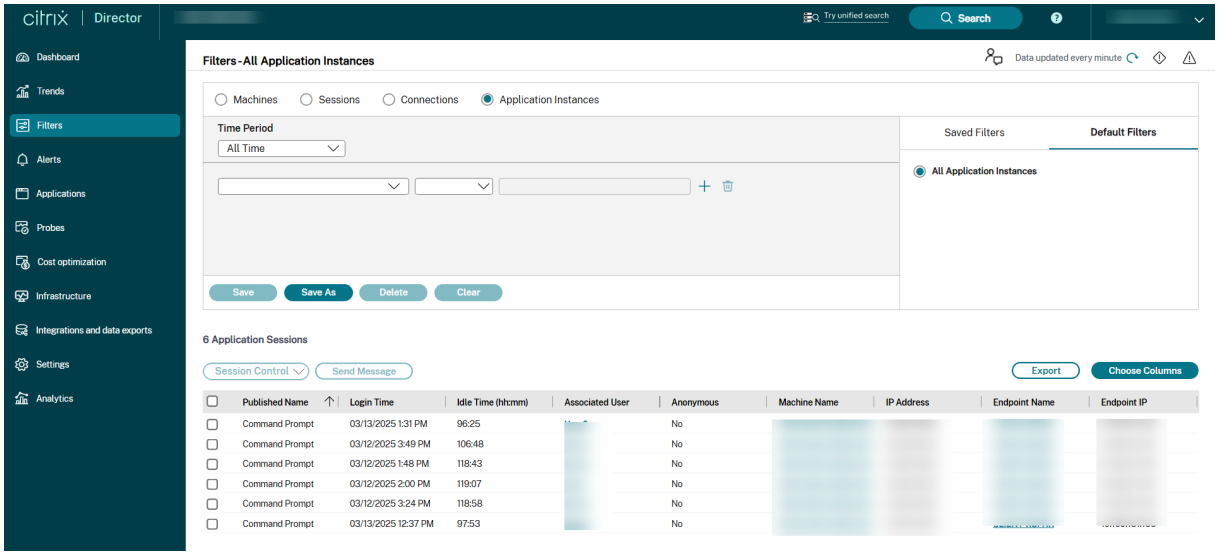
You can troubleshoot applications and sessions by using the idle time metric to identify instances that are idle beyond a specific time limit.

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 Server 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.



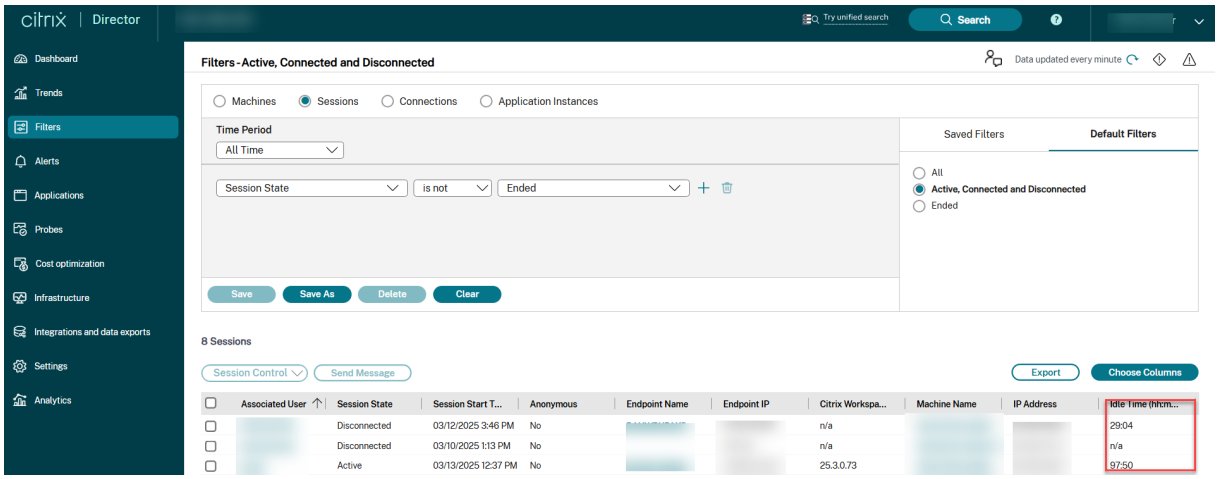
An example of a filter would be as follows. As **Filter by** criteria, choose **Published Name** (of the application) and **Idle Time**. Then, set **Idle Time** to **greater than or equal to** a specific time limit and save

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

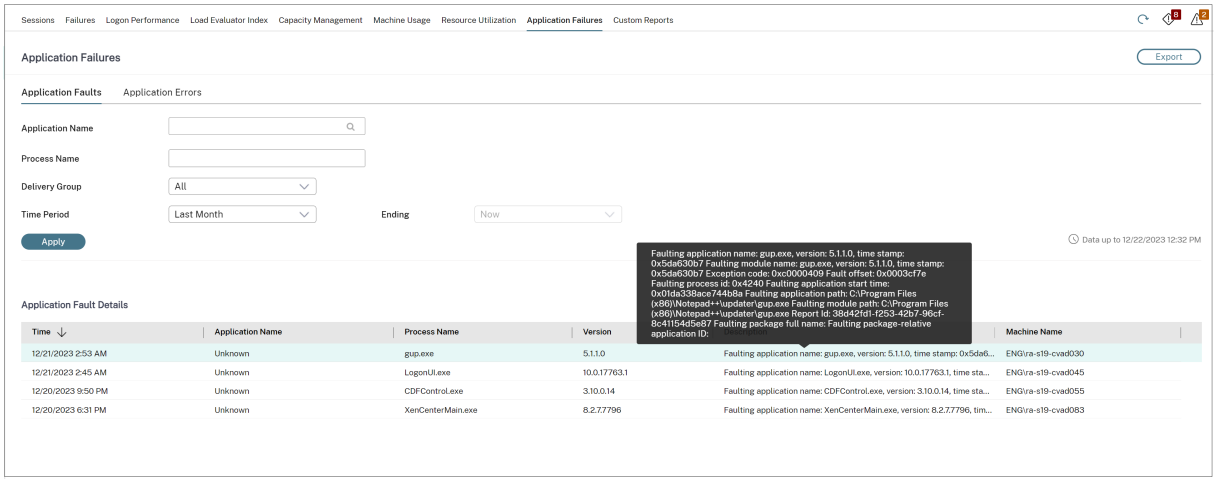
The **Trends** -> **Application Failures** tab displays failures associated with the published applications on the VDAs.

Application failure trends are available for the last 2 hours, 24 hours, 7 days, and month for Premium and Advanced licensed sites. They are available for the last 2 hours, 24 hours, and 7 days for other license types. 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 grooming retention settings for application failure monitoring, GroomApplicationErrorsRetentionDays and GroomApplicationFaultsRetentionDays are set to one day by default for both Premium and non-Premium licensed sites. You can change this setting using the PowerShell command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PowerShell command Set-MonitorConfiguration -\<setting name\> \<value \>



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.

The **Trends > Application Probe Results** page displays the results of application probing run in the site for the last 24 hours and 7 days. For more details on how to configure application probes, see Application Probing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot machines

July 28, 2026

> **Note:**
>
> **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 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 Director console 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 actions for machine and connection failures are available in Citrix Director failure reasons and troubleshooting.

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.

Prerequisite

- uberAgent® must be installed on the VDAs
- **Windows VDA version**: 2511 or later

Metrics

Metrics	Description
Average CPU Usage (%)	
Average RAM Usage (%)	
Average Disk IOPS	
Average Disk Latency (ms)	

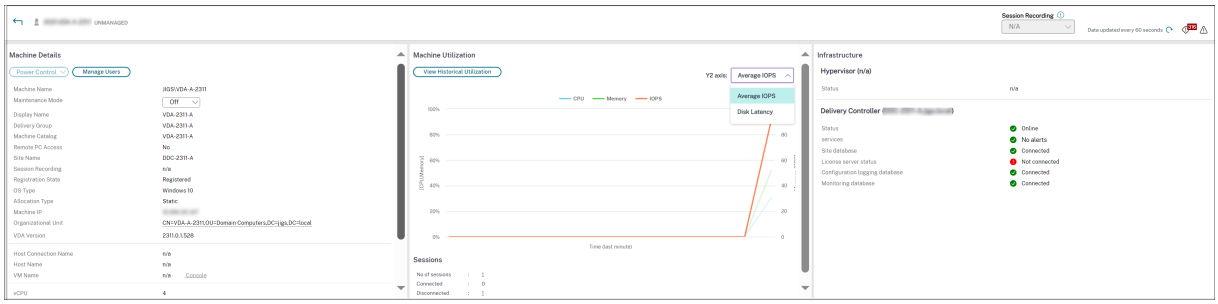
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Metrics	Description
Average GPU Usage (%)	
Average Network Utilization (%)	
Average Load Index	
Average Disk Usage (%)	
Average Profile Disk Usage (%)	
Average CPU Idleness (%)	
Average Pagefile Usage (%)	
Average CPU Relative Frequency (%)	

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 Delivery Controllers and VDA versions **7.14** or 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.



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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.
  - For NVIDIA, only GRID drivers are supported. CUDA drivers do not work with the NVadsA10 v5-series and aren't 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.
  - 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 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 the GPU
  - Check Task Manager. If drivers are installed properly, the GPU must show up in Task Manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Check if the machine is registered. Sometimes machines might 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**.

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 are 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
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 before 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 the 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”.

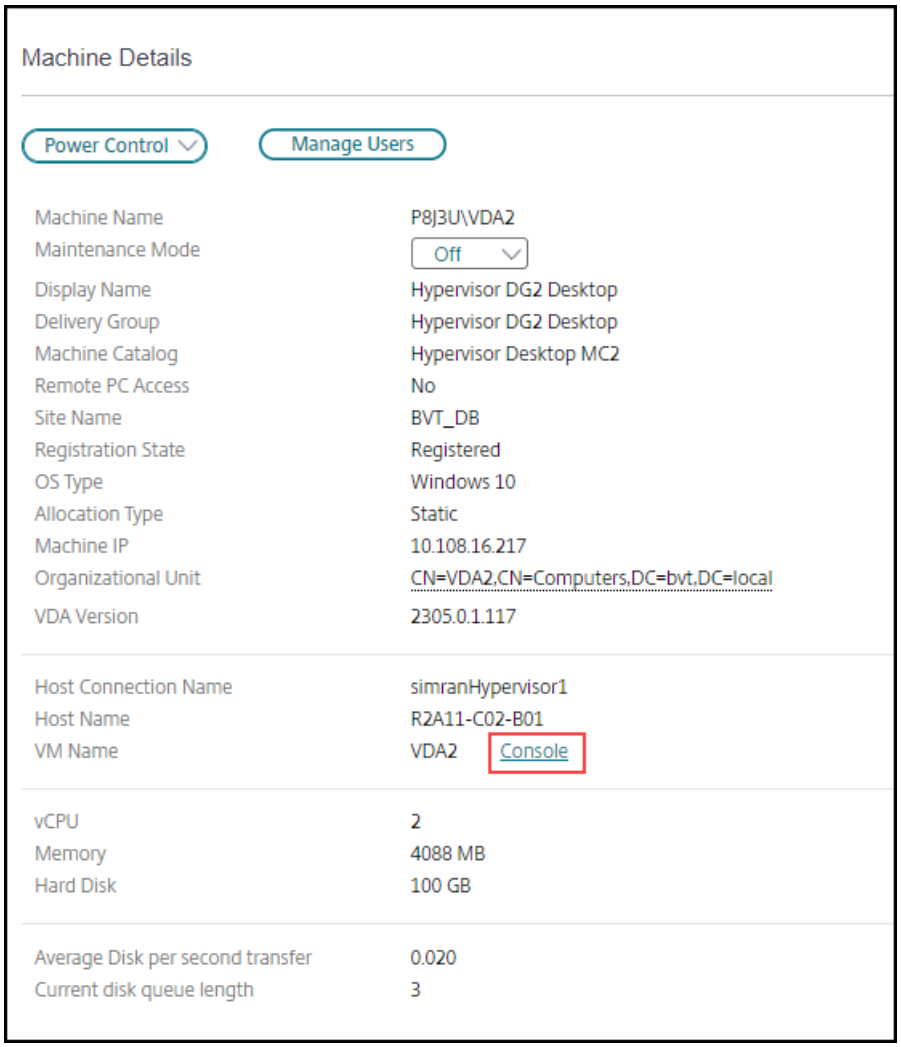
3. To view the historical trend on the resource consumption of a particular process, drill into any of the Top 10 processes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machine Console access

You can access the consoles of Single-session and Multi-session OS machines hosted on XenServer Version 7.3 and later directly from Director. This way, you don't require XenCenter to troubleshoot issues on XenServer hosted VDAs. For this feature to be available:

- Delivery Controller of Version 7.16 or later is required.
- The XenServer hosting the machine must be of Version 7.3 or later and must be accessible from the Director UI.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If the mouse pointer on the machine console is misaligned, see CTX230727 for steps to fix the issue.
- Director launches console access in 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*.

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

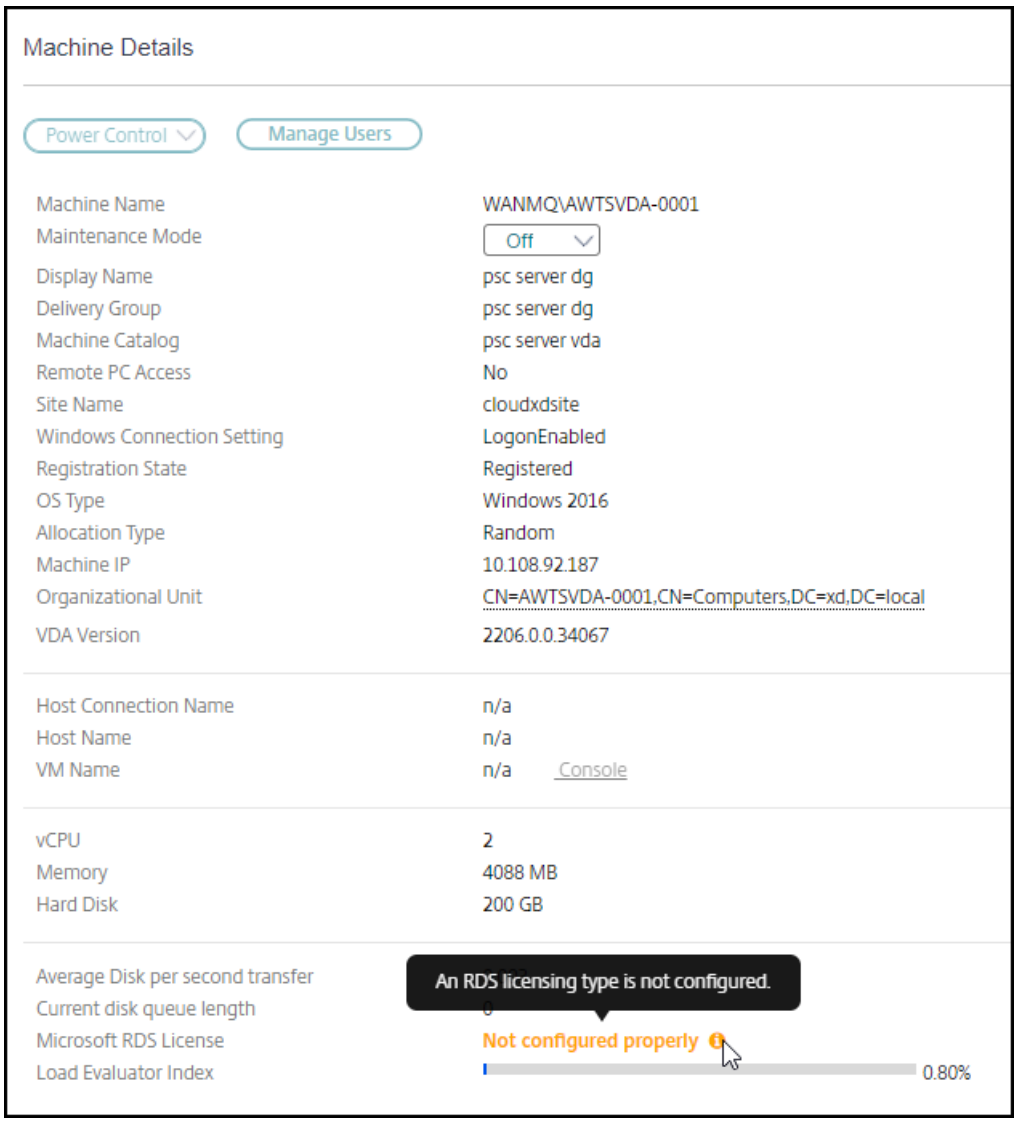
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter	Description
	• 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 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
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 the 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)
- 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 licenses before they expire.

For warning and error messages, hover over the info icon to view additional information as given in the following table.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Message Type	Messages in Director
Error	Available for VDAs version 7.16 and later.
Error	New RDS connections aren't 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.
Warning	With the Per Device Client Access licensing type, the Client Device license cannot 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).

Troubleshoot user issues

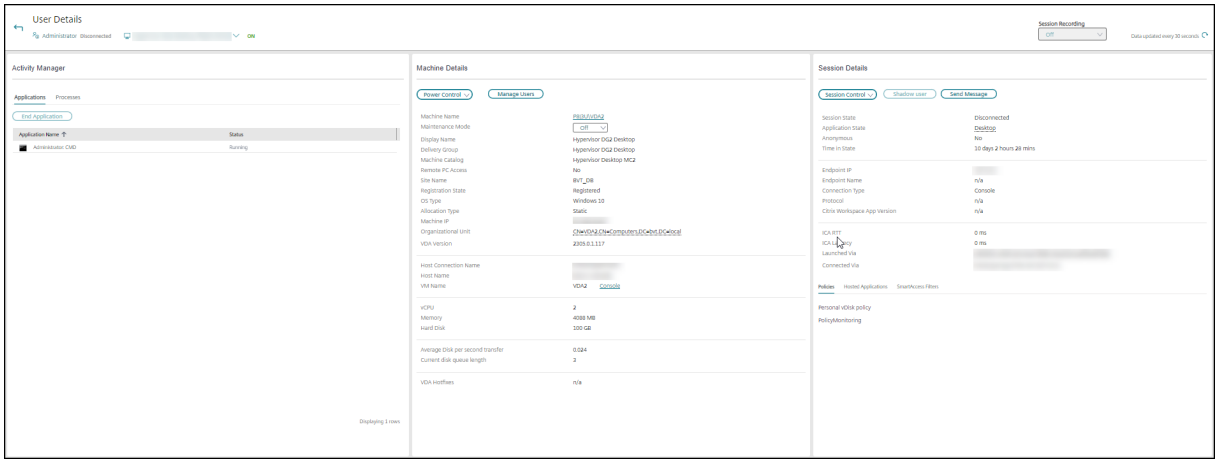
September 6, 2025

Use the Director's **Help Desk** view (**Activity Manager** page) to view information about the user or session:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Clicking **View Details** from the Activity Manager for a user opens the **User Details** page.

Clicking **View Details** from the Activity Manager for an endpoint opens the **Endpoint Details** page.



Session Selector

If the user has started several sessions, the session selector helps select a session.

Choose a session to view the details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Check details about the session, user's sign in experience, session startup, connection, and applications.
- you can Shadow the user's machine.
- Record the ICA® session.

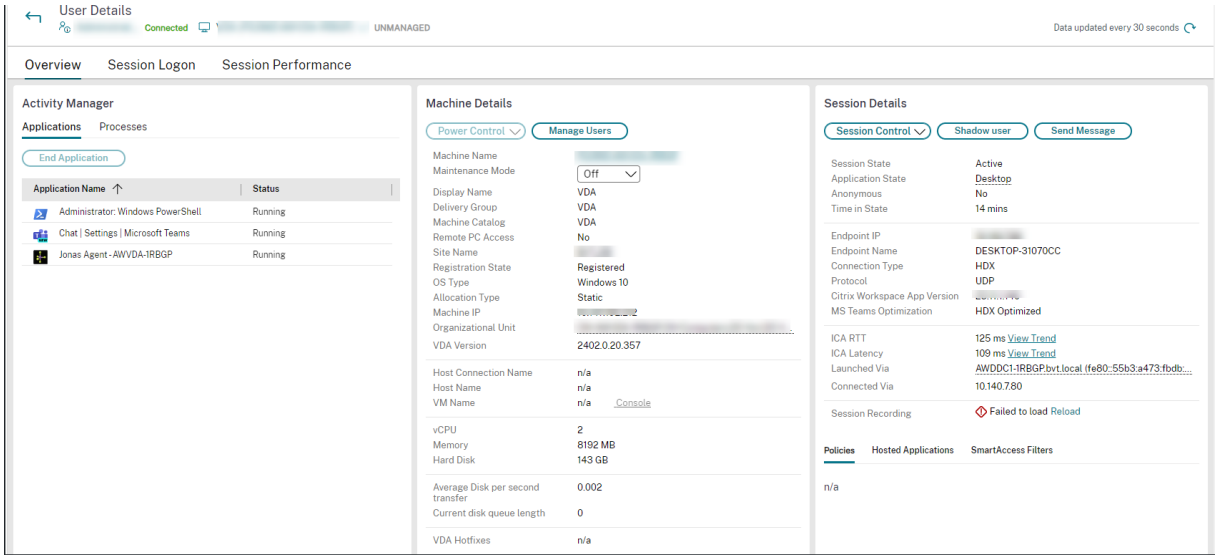
Microsoft Teams optimization status

Director displays the Microsoft Teams optimization status for HDX™ sessions in the **User Details** page > **Session Details** panel > **MS Teams Optimization** field. Microsoft Teams being 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 Director supports Microsoft Teams version 2.1 or earlier.

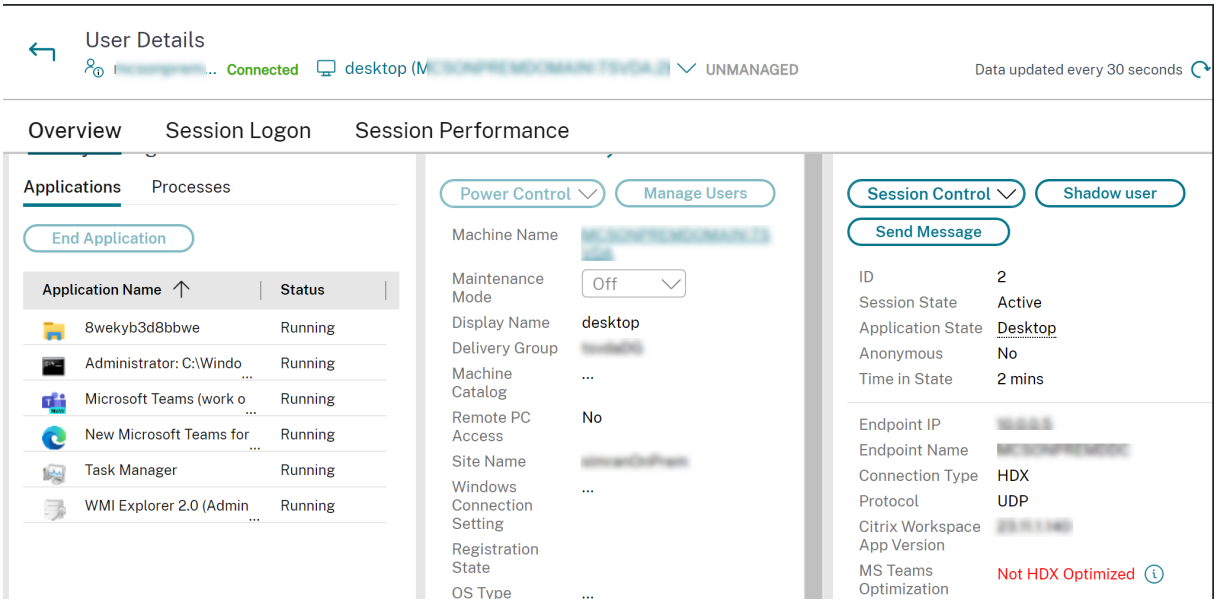
Prerequisites:

- 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

Troubleshoot the issue with the recommended actions in the following table, and, if needed, escalate the issue to the appropriate administrator.

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
Session response is slow or not responding	Diagnose session performance issues
Application is slow or does not respond	Resolve application failures
Connection failed	Restore desktop connections
Session is slow or not responding	Restore sessions
Record sessions	Record sessions
Video is slow or poor quality	Run HDX channel system reports

> **Note:**
>
> To make sure that the machine isn't in maintenance mode, from the User Details view, review the Machine Details panel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session Logon

The **User Details** view > **Session Logon** tab displays a comprehensive view of the session logon process. This tab shows the total logon duration, client and controller duration, and VDA duration. The **Session Logon** tab contains the Logon Duration phases chart with the various logon phases plotted. Use this data to troubleshoot user logon issues. For more information, see Diagnose user logon issues.

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

When you type the user's name in a Search field, Director searches for users in the Active Directory for users across all sites that are configured to support Director.

When you type a multiuser machine name in a Search field, Director displays the Machine Details for the specified machine.

When you type an endpoint name in a Search field, Director uses the unauthenticated (anonymous) and authenticated sessions that are connected to a specific endpoint. This search enables troubleshooting unauthenticated sessions. Ensure that endpoint names are unique to enable troubleshooting of unauthenticated sessions.

The search results also include users who are not currently using or assigned to a machine.

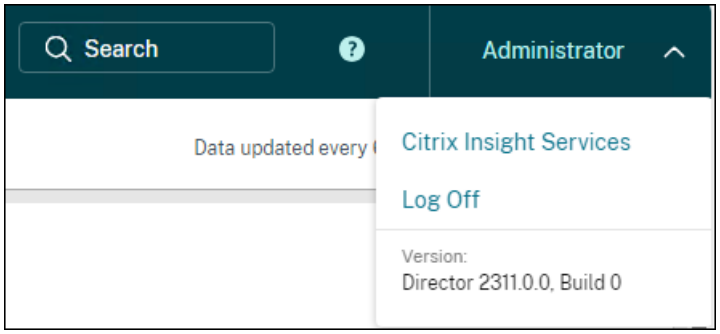
- Searches aren't case-sensitive.
- Partial entries produce a list of possible matches.
- After you type a few letters of a two-part name, separated by a space, the results include matches for both strings. The examples for two-part names are user name, family name and first name, or display name. For example, if you type jo rob, the results might include strings such as "John Robertson" or "Robert Jones".

To return to the landing page, click the **Director logo**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access Citrix Insight Services

You can access Citrix Insight Services (CIS) from the **User** drop-down list in Director to access extra diagnostic insights. The data available in the CIS comes from sources including Call Home and Citrix Scout.



Upload troubleshooting information to Citrix Technical Support

Run Citrix Scout from a single Delivery Controller™ or VDA to capture key data points and Citrix Diagnostics Facility (CDF) traces to troubleshoot selected computers. Scout offers the ability to securely upload the data to the CIS platform to assist Citrix Technical Support on troubleshooting. Citrix Technical Support uses the CIS platform to reduce the time to resolve customer-reported issues.

Scout is installed with Citrix Virtual Apps and Desktops™ components. Depending on the version of Windows, Scout appears in the **Windows Start** menu or Start Screen when you install or upgrade to Citrix Virtual Apps and Desktops.

To start Scout, from the Start menu or Start Screen, select **Citrix > Citrix Scout**.

For information on using and configuring the Scout, and for an FAQ, see CTX130147.

Diagnose session startup issues

September 6, 2025

In addition to the logon process phases mentioned in the Diagnose user logon issues section, Director displays the session startup duration. This is divided into Workspace App Session Startup and VDA Session Startup duration on the **User Details** page and **Machine 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. This feature is available on Delivery Controller version 7 1906 and later and VDAs 1903 and later.

Prerequisites

Ensure that the following prerequisites are met for session startup duration data to be displayed:

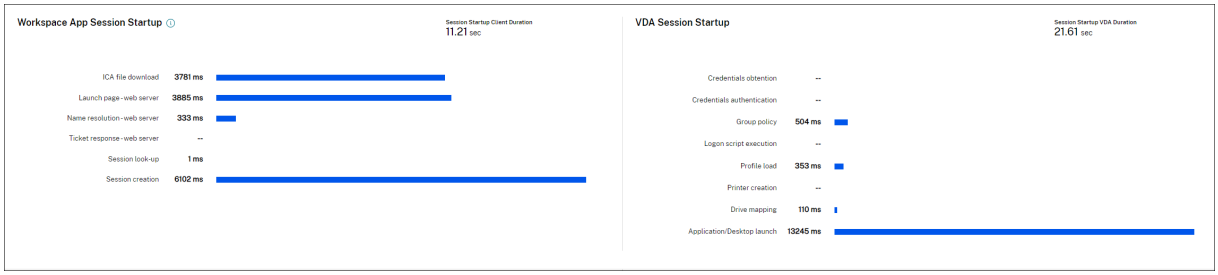
- Delivery Controller™ 7 1906 or later.
- VDA 1903 or later.
- Citrix End User Experience Monitoring (EUEM) service must be running on the VDA.

Limitations

The following limitations apply when Director 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.
- ICA® File Download Duration (IFDCD) is available only when Workspace App is detected while launching from a browser.
- For session launches from Mac OS, IFDCD is available for Workspace App 1902 or later only.
- 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 browser with Workspace app detected.

> **Notes:**
>
> - If you face issues in the sessions startup duration display after the prerequisites are met, view the Director 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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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). It ends when the ICA connection between the client device and VDA has been established. In the case of 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 following level down, there are several detailed metrics available.

ICA File Download Duration

This 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) in the Workspace Application.
2. A request from the user is sent to the StoreFront™ through the Citrix Gateway (if configured), which sends the request to the Delivery Controller.
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 the slowdown by checking the Internet Information Services (IIS) logs and monitoring tools, Task Manager, Performance Monitor and so on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- StoreFront is having issues communicating with other components such as the 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.

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 encompasses 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Credentials Obtention VDA Duration (COVD)

The time taken for the VDA to obtain the user credentials.

This duration can increase artificially if a user fails to provide credentials in a timely manner. So, it is 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. They 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.

Consider making asynchronous the user or group's login scripts. Consider optimizing 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, consider 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 the logon. This takes extra resources. Sometimes, this can consume significant amount of the CPU usage. Consider using the **Terminal Services home** folders with redirected personal folders to mitigate this problem. In general, consider using 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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, the value is not 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™ has to create every locally mapped printer on the client device. Consider reconfiguring 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. For example, 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. Userinit represents the duration between the start of userinit.exe to the start of the user interface for the virtual desktop or 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 any miscellaneous delay in session creation time on VDA.

Diagnose user logon issues

September 6, 2025

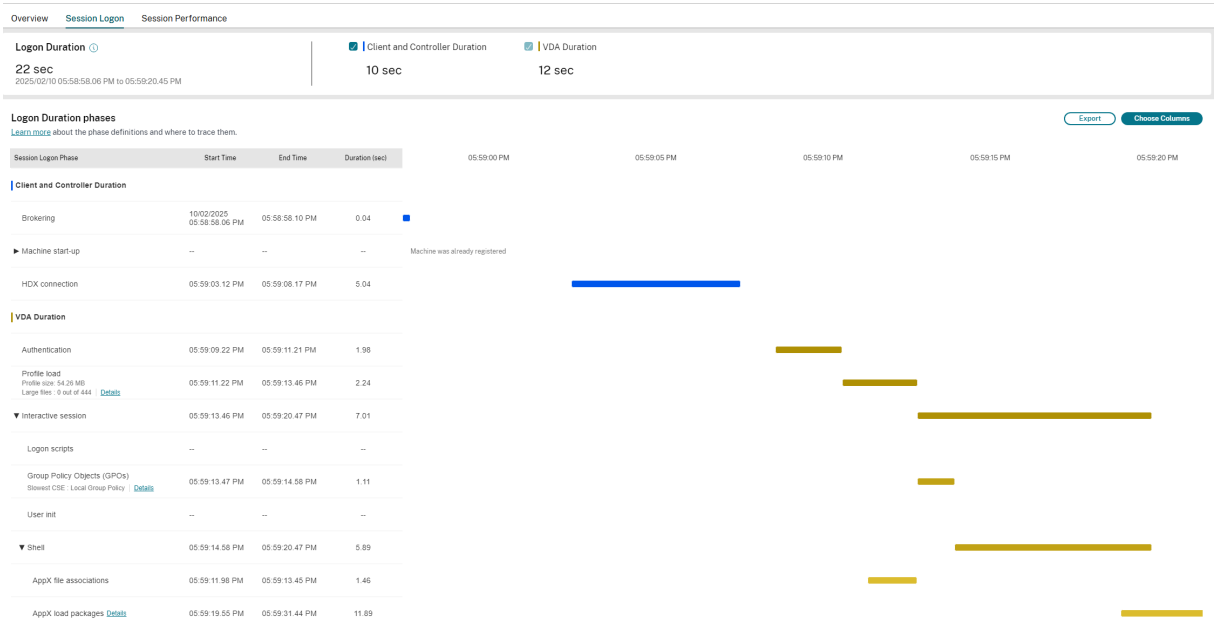
The **User Details** view > **Session Logon** tab displays a comprehensive view of the session logon process. This tab shows the total logon duration, client and controller duration, and VDA duration. Use this data to troubleshoot user logon issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 log on to Citrix Virtual Apps and Desktops™, 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 app or 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 Delivery Controller™ 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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

> **Notes:**
>
> - Logon duration is supported only on the default Windows shell (explorer.exe) and not on custom shells.
> - Logon duration for Remote PC Access is available only when **Citrix User Profile Manager** and the **Citrix User Profile Manager WMI Plugin** are installed as extra components during Remote PC Access installation. For more information, see Step 4 in Remote PC Access configuration and sequence considerations.

Steps to troubleshoot user logon issues

1. From the **User Details** view > **Session Logon** tab, troubleshoot the logon state using the Logon Duration chart.
    - 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.

Logon process phases

Client and Controller duration

Time taken since the user clicked on the app or desktop icon until the keyboard and mouse controls are handed over to the end user to interact with the session.

Brokering Time taken to decide which desktop to assign to the user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

VDA duration

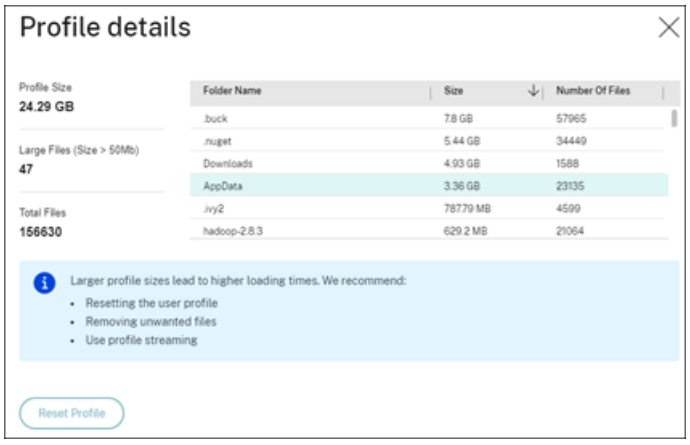
Time taken on the VDA to create a session.

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.

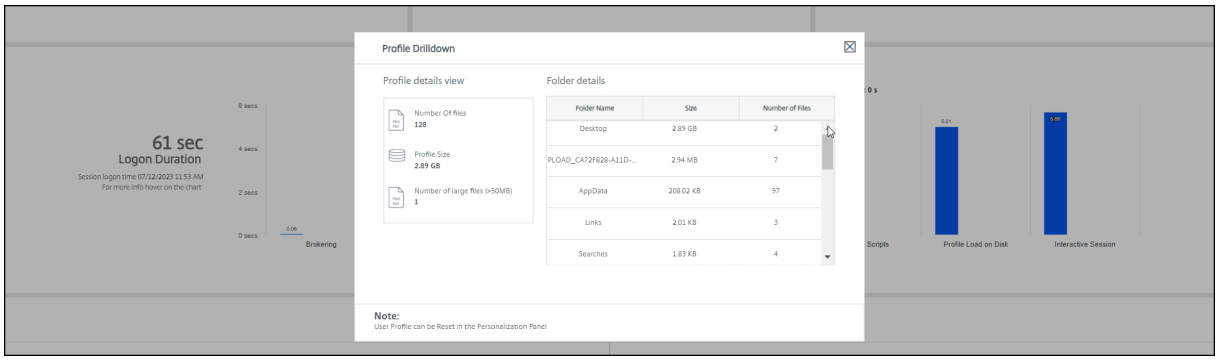
If Citrix Profile Management and FSLogix are configured, the Profile Load bar includes the time taken by Citrix Profile Management and FSLogix to process user profiles. This information helps administrators to troubleshoot high profile processing duration issues. When Profile Management and FSLogix are 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.



© 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 Delivery Controller version 7 1811 or later and VDAs 1811 or 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 folders in the profile root are displayed in the drilldown. To hide folder visibility, edit the following registry value on the VDA machine:

> **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 Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. On the VDA, add a new registry value **ProfileFoldersNameHidden** at HKEY_LOCAL_MACHINE\Software\Citrix
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 commands 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The 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**.
- Certain hidden files in the AppData folder are not included in the Profile drilldown.
- The number of files and profile size data might not match with the data in the Personalization panel due to certain Windows limitations.

Interactive Session

Interactive Session 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 Interactive Session to see a tooltip showing the following:

- subphases
- time taken for each subphase
- total cumulative time delay between these subphases

You can use the collapsible button to collapse or expand the options under the **Interactive Session**.

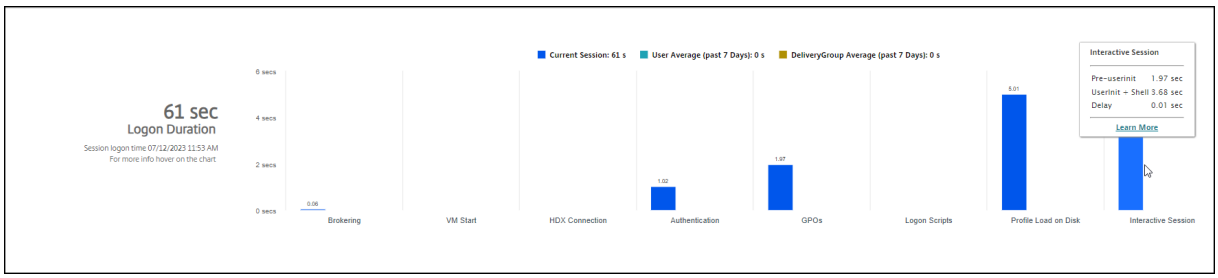
> **Note:**
>
> This feature is available on VDAs 1811 and later. If you have launched sessions on sites earlier than 7.18 and then upgraded to 7.18 or later, a 'Drilldown unavailable due to server error'message is displayed. However, if you have launched sessions after upgrading, no error message is 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 Audit process tracking in the Microsoft documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Logon Duration panel in the User Details view.

- **Interactive Session –Pre-userinit:** 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 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 the 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, more 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 the ICA file upon application launch, configure your browser for automatic ICA file launch upon download of an ICA file. For more information, see CTX804493.

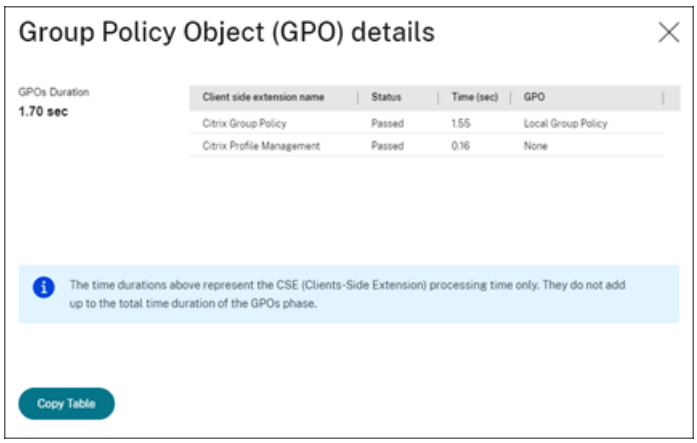
> **Note:**
>
> The Logon Duration graph shows the logon phases in seconds. Any duration values below one second are displayed as subsecond values. The values above one second are rounded to the nearest 0.5 second. The graph has been designed to show the highest y-axis value as 200 seconds. Any value 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CSEs (Clients-Side Extension) is available as a tooltip when you hover on the GPO bar.



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 Director for collecting AppX packages loading duration during the new VDA session. For more information, see Citrix uberAgent integration with Director.

© 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.

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 logon 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**.

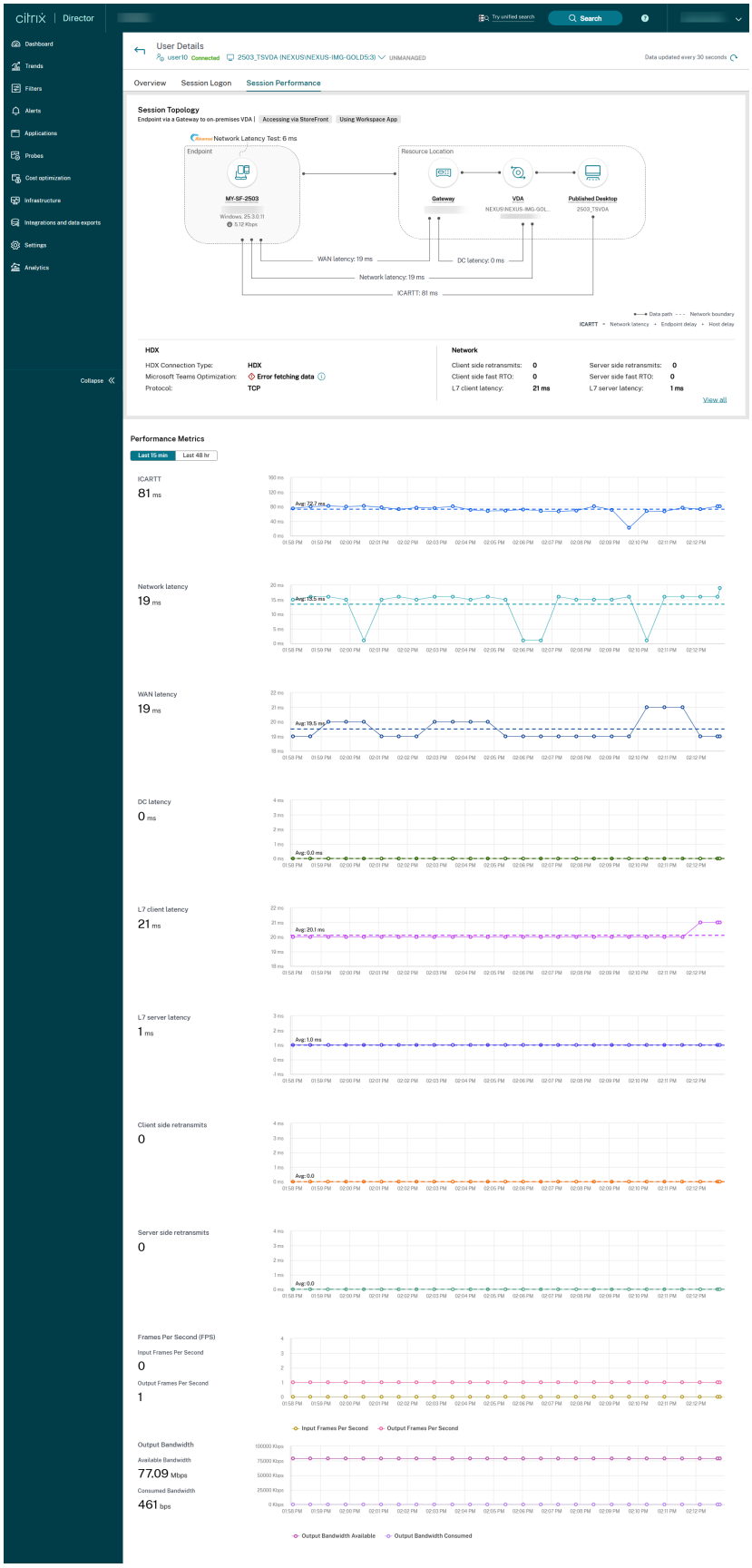
Diagnose Session Performance issues

October 10, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy name	Policy Description	UI metrics	Default value	Value options	Virtual Delivery Agent 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
Endpoint location data collection	Allows the collection of endpoint location and ISP details from the user endpoint using the Locus service - https://locus.analytics.cloud.com	Public IP address, Country, City, and Internet Service Provider.	Disabled	Enabled or Disabled	2411 or later
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

© 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 ChromeOS 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
	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

© 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 ChromeOS version
	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 service provider	2411 or later	NA	NA	2409 or later	2409 or later	2408 or later	2411 or later	2411 or later
	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
	Endpoint GPU	2411 or later	NA	NA	2409 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 ChromeOS version
	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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UI parameter	Description
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 Workspace or 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 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.

Use the policies in Citrix Studio to enable or disable collection of listed network 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	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. Option to modify the frequency between 60s - 3600s. 60s is suggested value	2411 or later for Gateway service. 2503 or later for Citrix Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 metrics	L7 Server latency	2411 or above	2507 or later	2507 or later	2409 or later	2505 or later	2505 or later	NA	NA
	L7 Client latency	2411 or above	2507 or later	2507 or later	2409 or later	2505 or later	2505 or later	NA	NA
	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	NA	NA
	Throughput	2411 or above	NA	NA	2409 or later	2505 or later	2505 or later	NA	NA

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	NA	NA
	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	NA	NA
	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	NA	NA
	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	NA	NA
	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	NA	NA
	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	NA	NA

© 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	NA	NA
	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	NA	NA
	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	NA	NA
	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	NA	NA

Data definitions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 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.

Feature name	UI parameters	Citrix Workspace app for Windows version	Virtual Delivery Agent version
ICA metrics	ICA RTT ICA® Latency	Citrix Workspace app for Windows version 2405.10 or later	Citrix Virtual Apps and Desktops 2407 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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:

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.

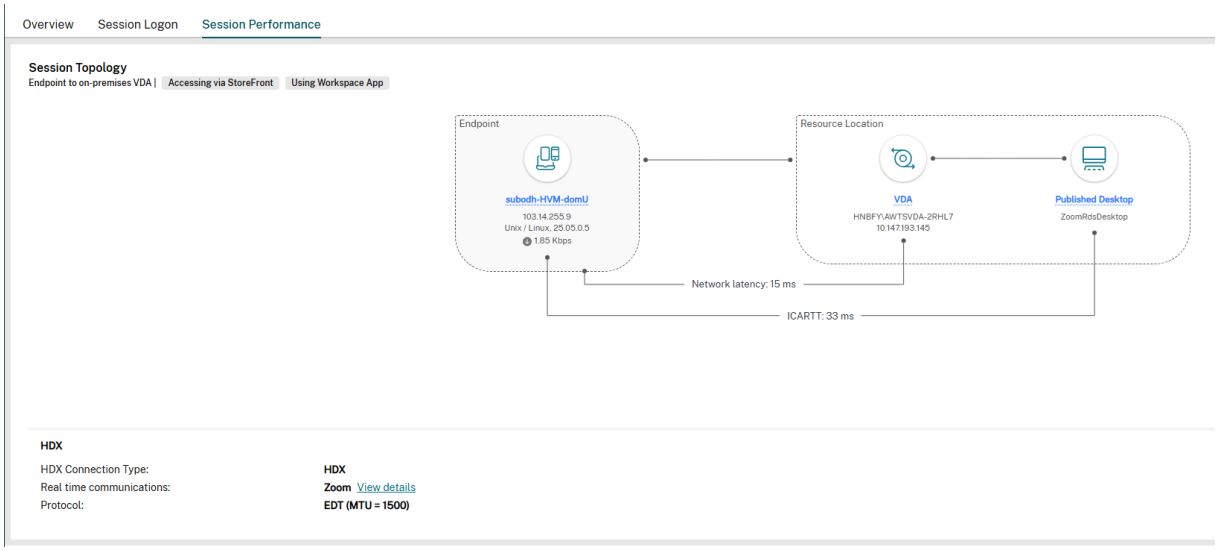
Real-time communications optimization visibility The session topology provides comprehensive visibility into the optimization status of real-time communication (RTC) applications like Microsoft Teams, Zoom, and WebEx within Citrix sessions. It pinpoints whether an application is optimized, and identifies 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.

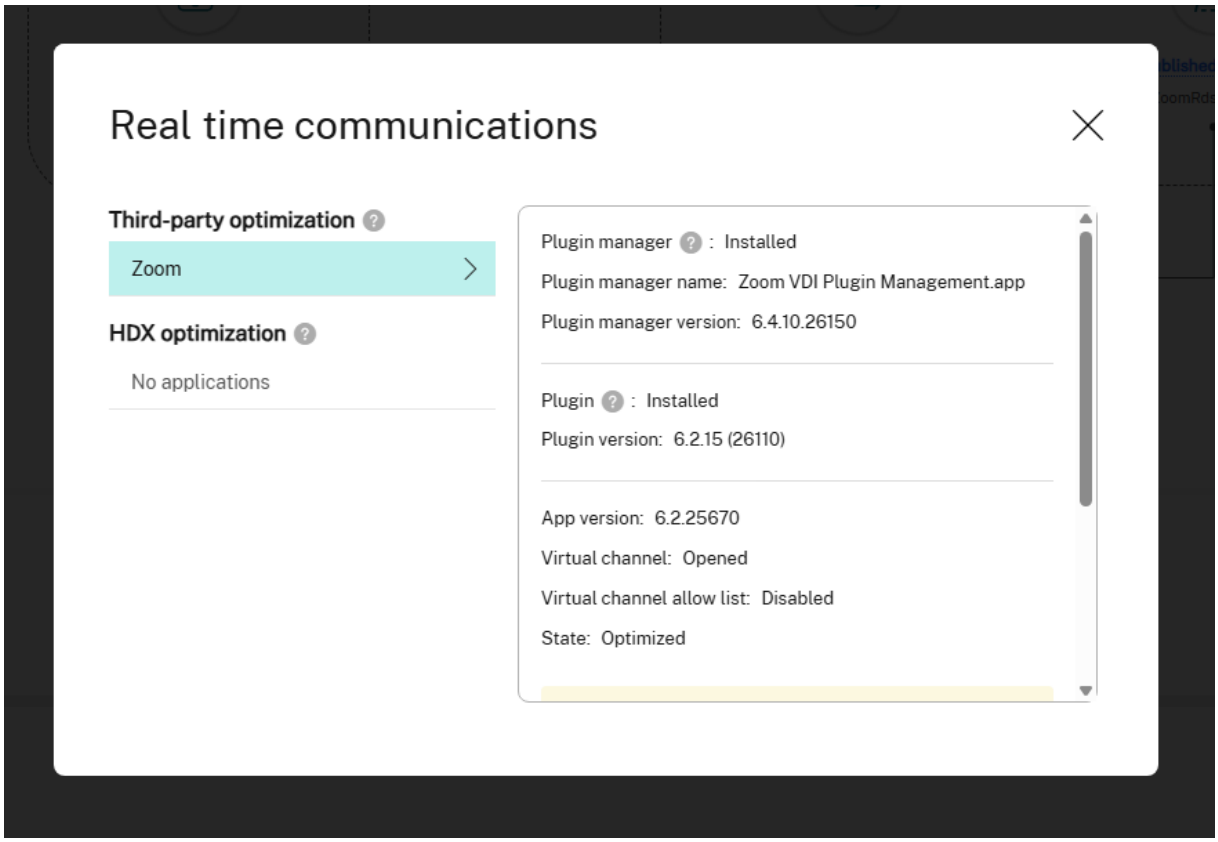
Use the **Real time communications** field in the **Session Topology** to view optimization details for each application.

© 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:

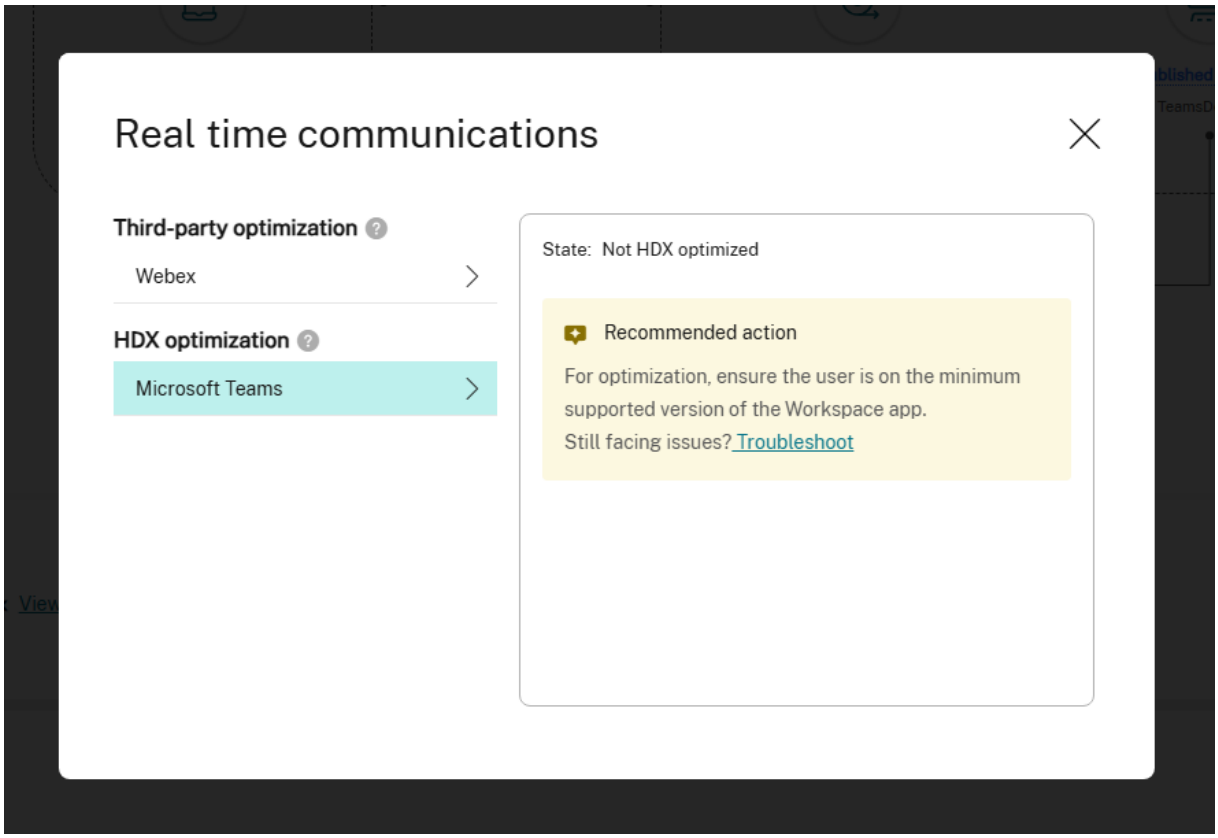


HDX-optimized applications use the Citrix virtual channel and are directly impacted by Citrix configu-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

rations and settings.

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
	Plugin, Plugin version, State	2507	2503	2505	Plugin Not Available

© 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
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

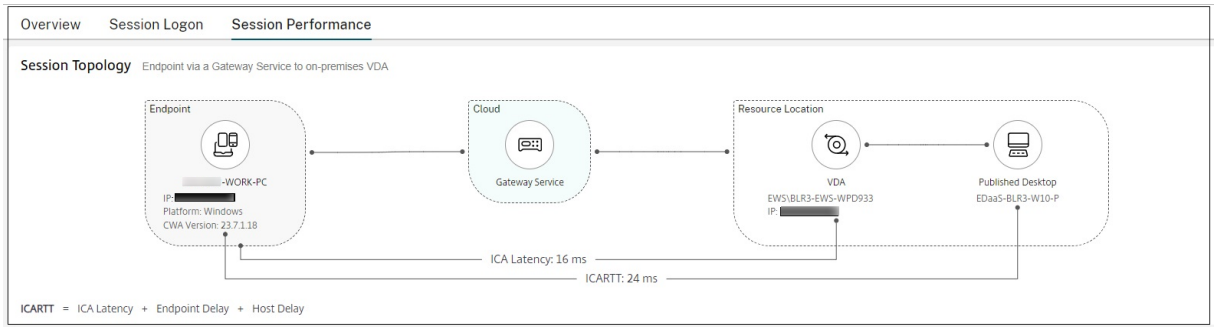
Depending on the deployment scenario of the site, the components involved in a session are all or any of the following:

- 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

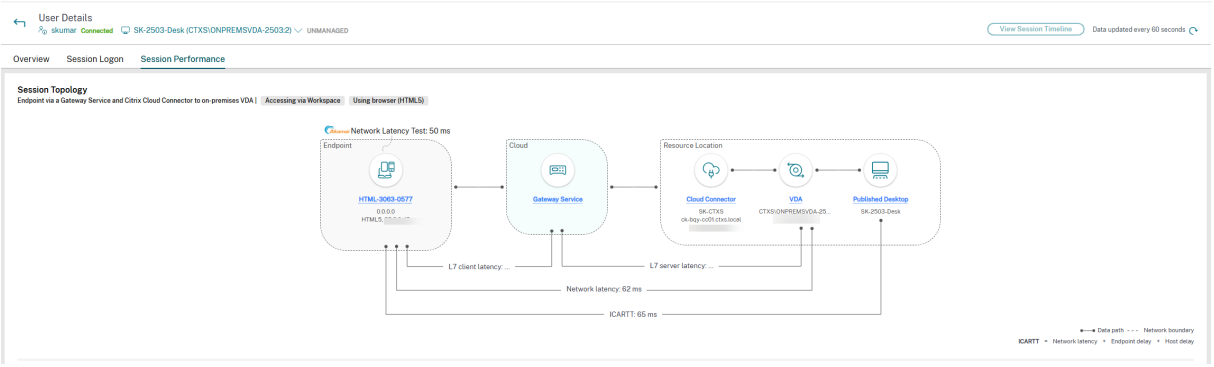
Accordingly, the possible network topologies are as follows:

- Citrix Workspace app on the endpoint connects via Citrix Workspace and Gateway Service to an on-premises VDA. No Cloud Connector is used to connect to VDA.

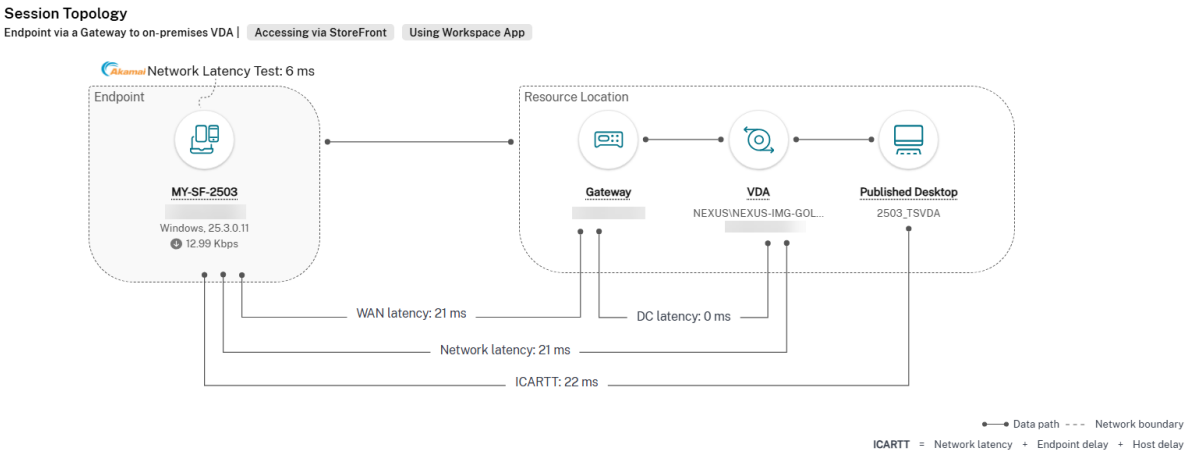
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Citrix Workspace app on the endpoint connects via Citrix Workspace and Gateway Service to an on-premises VDA via Cloud Connector.

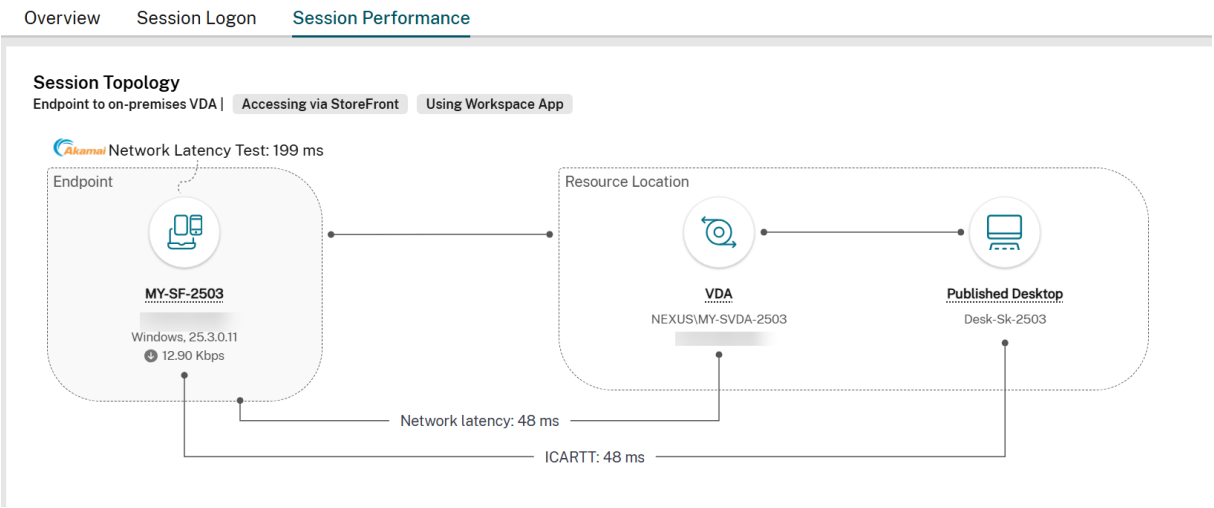


- Citrix Workspace app on the endpoint connects via StoreFront™ and on-premises Gateway to on-premises VDA.



- Citrix Workspace app on the endpoint connects via StoreFront to on-premises VDA.

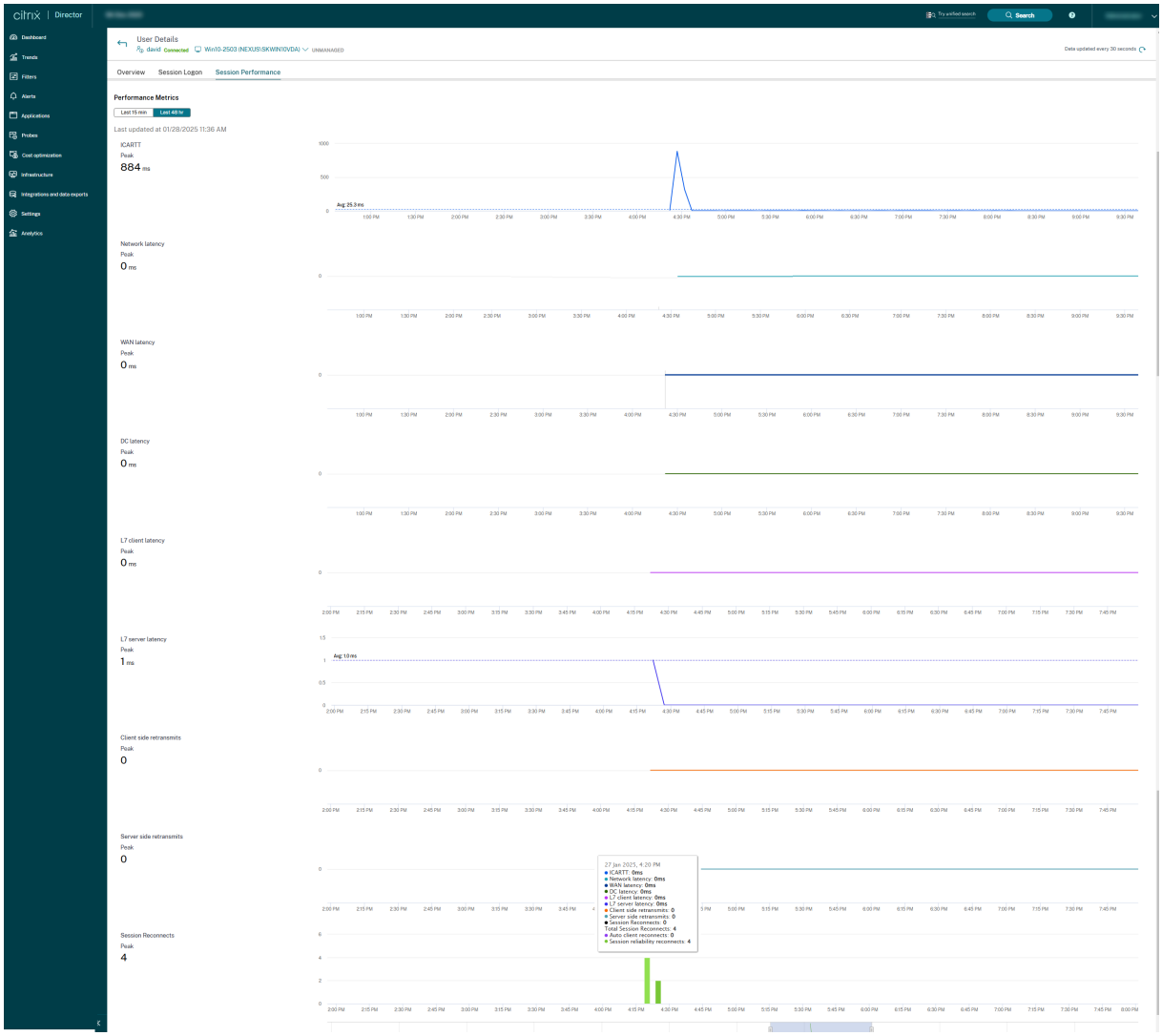
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 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 re-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sponsiveness.

- 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 Monitoring is not running.**	1. Open the Services console. To 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error type	Error	Error message	Solution
			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. 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 Wf-Shell.exe/PicaShell.exe process is running under **Activity Manager** > **Process** tab. If it is not running, reopen the desktop session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error type	Error	Error message	Solution
			4. If the preceding steps are not working, run the following command to ensure that the Citrix_Euem_RoundTrip instance is present: `Get-CimInstance -Namespace 'ROOT\Citrix\Euem'-Query "select * from 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error type	Error	Error message	Solution
			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, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error type	Error	Error message	Solution
			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' -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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diagnose ended user sessions

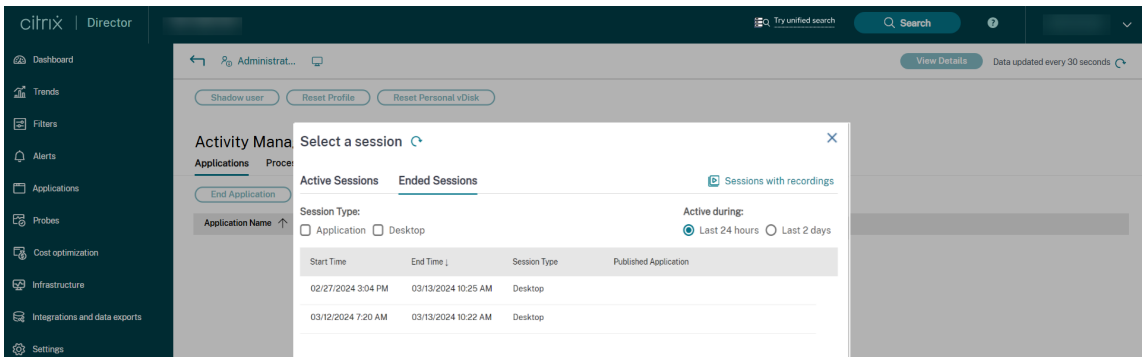
September 6, 2025

Citrix Director 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.
- 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:

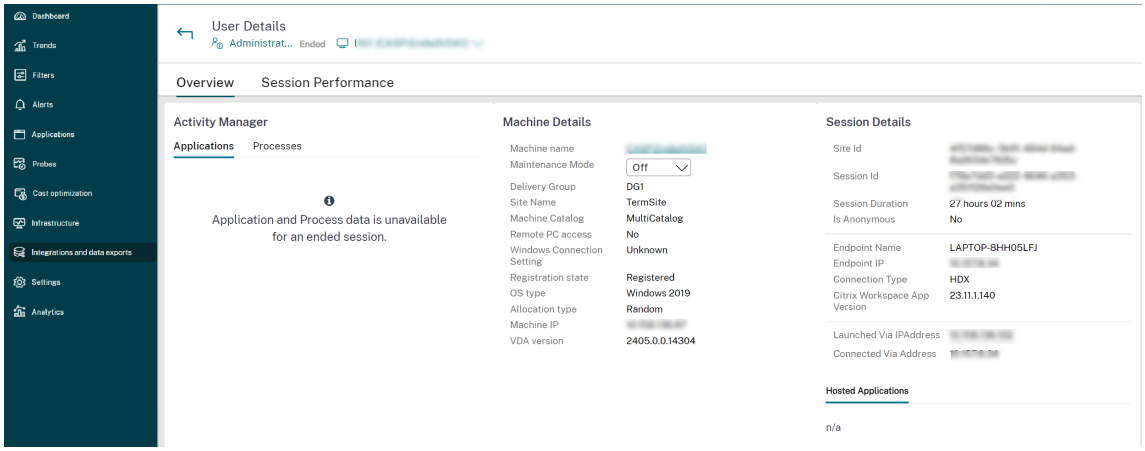
1. Click **Filter** > **Session** view.
2. Click the **Associated User** to open the Activity Manager for the user.



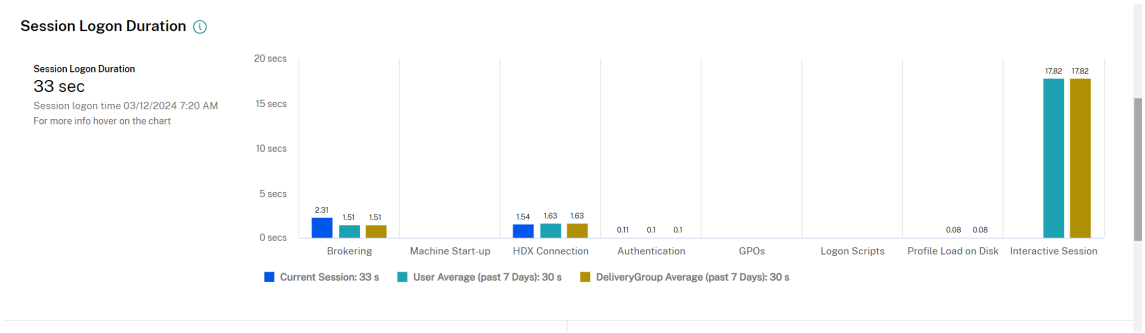
3. Select the required session from the **Ended Sessions** section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

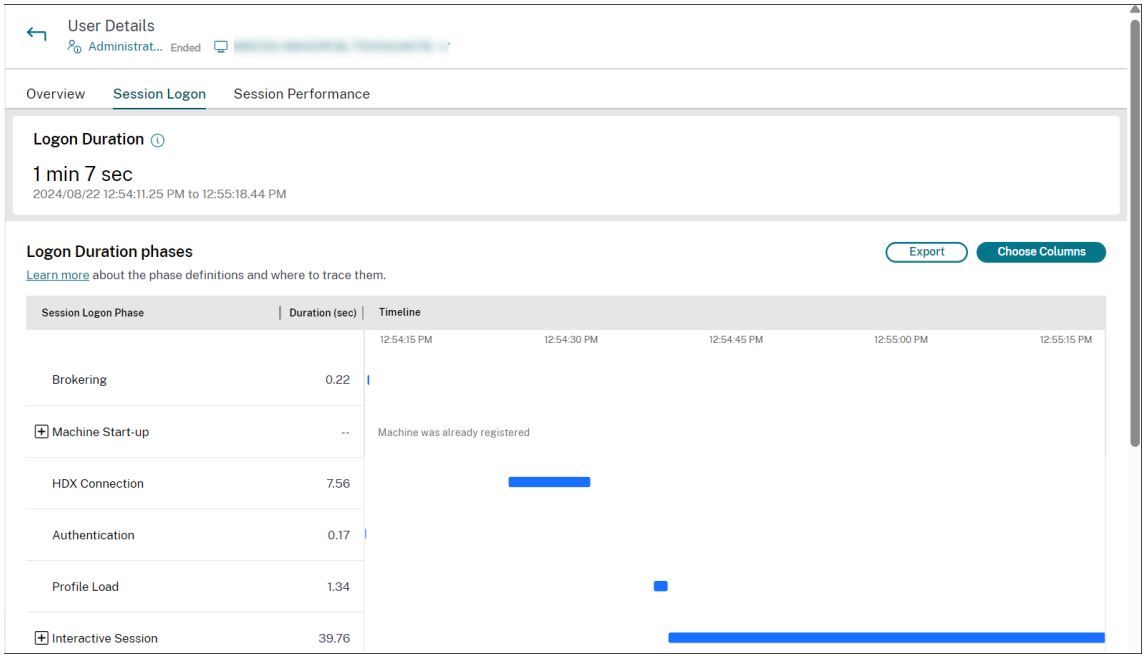
4. View the **Machine Details** and **Session Details** panels.



5. Scroll down and view the **Session logon duration** for the ended session.

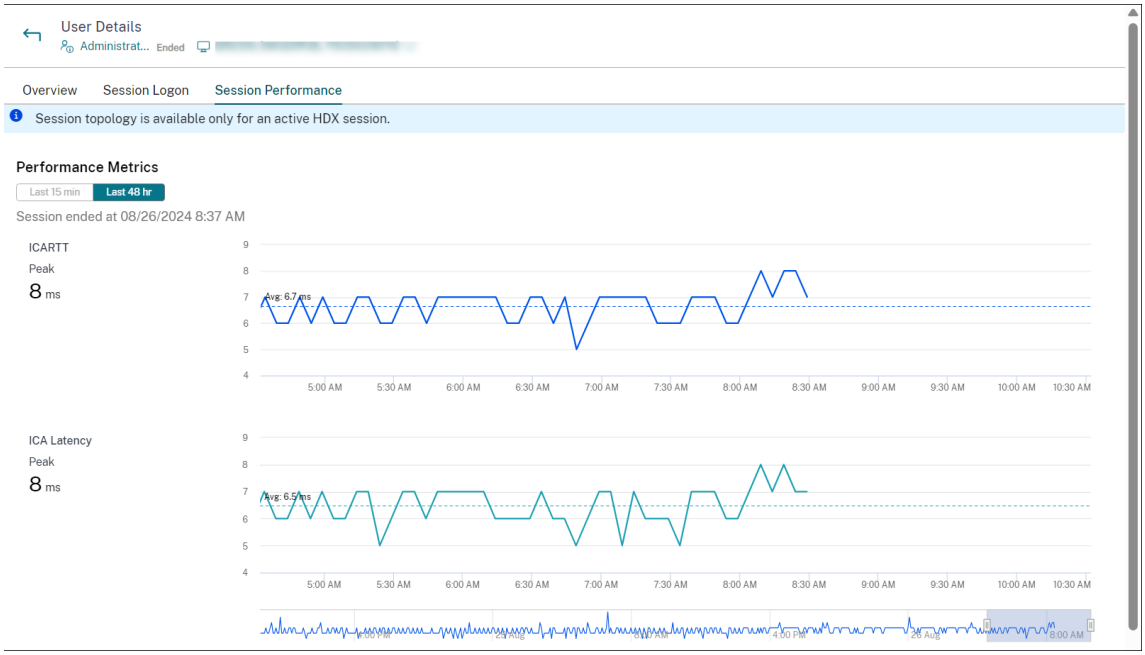


6. Click the **Session Logon** tab and view the details.



7. Click the **Session Performance** tab and view the details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Shadow users

May 5, 2025

From Director, 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.

Director launches shadowing in a new tab, update your browser settings to allow pop-ups from the Director 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.

> **Note:**
>
> - The VDA must be accessible from the Director UI for shadowing to work. Hence, shadowing is possible only for Linux VDAs in the same intranet as the Director client.
> - Director uses FQDN to connect to the target Linux VDA. Ensure that the Director client can

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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 Director 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 the **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:

Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone > Automatic prompting for file downloads.

By default, this option is enabled for sites in the Local intranet zone. If the Director site is not in the Local intranet zone, consider manually adding the site to this zone.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Send messages to users

May 5, 2025

From Director, send a message to a user who is connected to one or more machines. Use this feature to send immediate notices about administrative actions such as impending desktop maintenance, machine logoffs and restarts, and profile resets.

1. In the Activity Manager view, select the user and click Details.
2. In the User Details view, locate the Session Details panel and click Send Message.
3. Type your message information in the Subject and Message fields, and click Send.

If the message is sent successfully, a confirmation message appears in Director. The message appears in the user's machine.

If the message is not sent successfully, an error message appears in Director. Troubleshoot the problem according to the error message. When you have finished, type the subject and message text again and click **Try** again.

Resolve application failures

September 6, 2025

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.

> **Note:**
>
> If the Applications tab is grayed out, contact an administrator with the permission to enable the tab.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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.

Restore desktop connections

May 5, 2025

From Director, 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. For example, when the machine is using an unusually high amount of CPU resources, which can make the CPU unusable.

Restore sessions

September 6, 2025

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 from the user's 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

September 6, 2025

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.

1. In the HDX panel, click Download System Report.
2. You can view or save the .xml report file.
    - To view the .xml file, click Open. The .xml file appears in the same window as the Director application.
    - To save the .xml file, click Save. The Save As window appears, prompting you for a location on the Director machine to download the file to.

Reset a user profile

September 6, 2025

> **CAUTION:**
>
> When a profile is reset, the user's folders and files are saved and copied to the new profile. However, most user profile data is missing (for example, the registry is reset and application settings might be deleted).

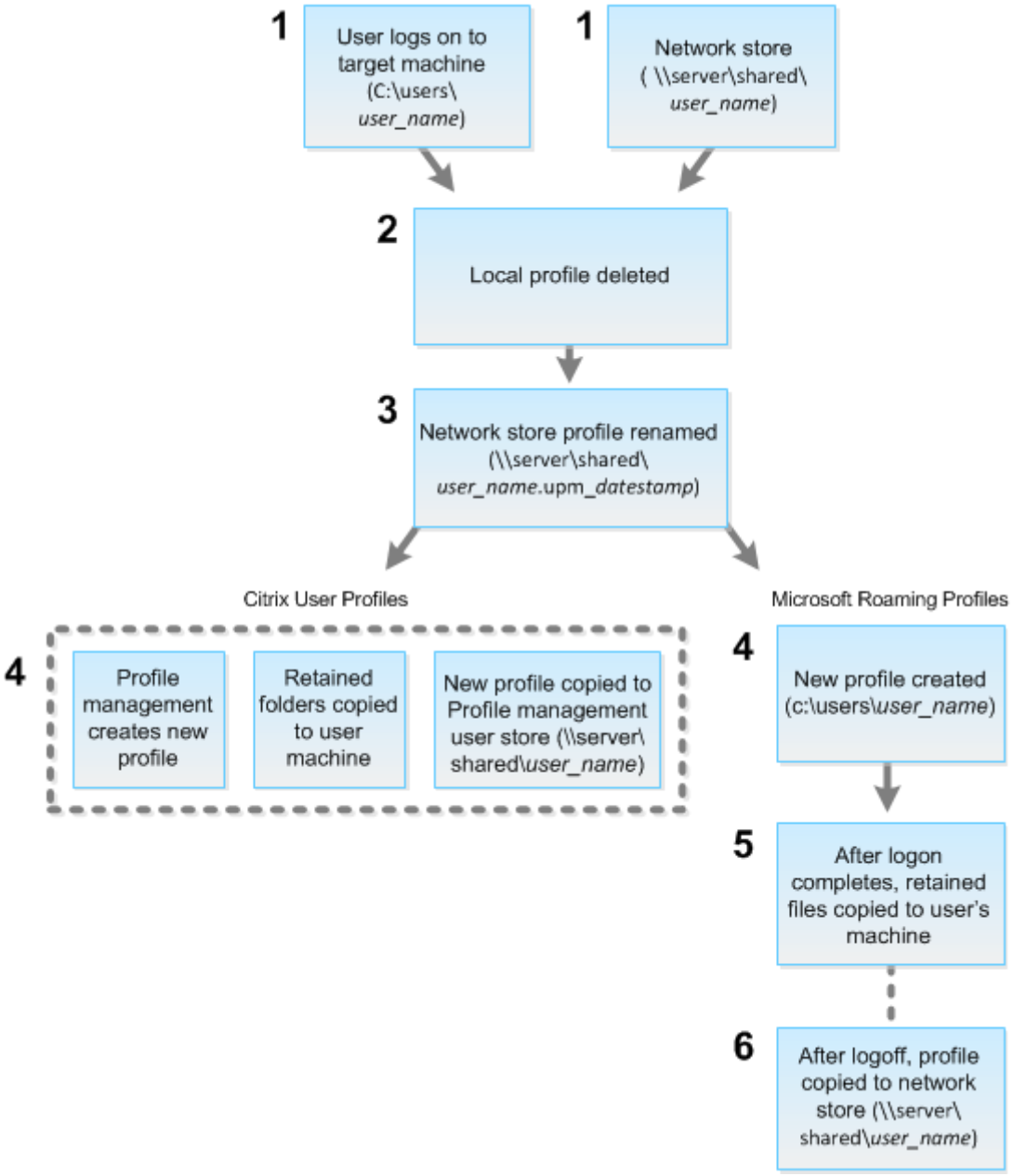
The reset function applies to both file-based and container–based profile solutions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Director or using the PowerShell SDK), Director first identifies the user profile in use and issues an appropriate reset command. Director receives the information through Profile Management, including information about the profile size, type, and logon timings.

This diagram illustrates the process following the user logon, when a user profile is reset.



The reset command issued by Director 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 the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

user is processed by Profile Management, 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.
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. 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 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 reset a user profile in Director

If you are using the Citrix Virtual Desktops™ (Desktop VDA), do the following:

1. From **Director**, search for the user whose profile you want to reset, and then select this user's session.
2. Click **Reset Profile**.
3. Instruct the user to log off from all sessions.
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.

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.

> **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 logon action ensures that the correct profile is reset. If the profile is a Citrix user profile, the profile is already reset by the time the user's desktop appears. If the profile is 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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note the following:

- If the user store is enabled as the user profile solution, the new profile contains the following personal folders from the original user profile:
  - Desktop
  - Cookies
  - Favorites
  - Documents
  - Pictures
  - Music
  - Videos
- Starting with Citrix Profile Management version 2407, if the profile container is enabled as the entire user profile solution, the new profile retains the preceding personal folders.
- In Windows 8 and later, cookies are not copied to the new profile when profiles are reset.

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.

To reset a profile using PowerShell SDK

You can reset a profile using the Broker PowerShell SDK.

New-BrokerMachineCommand

Creates a command queued for delivery to a specific user, session, or machine. For more information about this cmdlet, see https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/.

Examples

See the following examples for details about how to use the PowerShell cmdlets to reset a profile:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reset a Profile Management profile

- Suppose you want to reset the profile for user1. Use the New-BrokerMachineCommand PowerShell command. For example:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **Important:**
>
> The `CommandData $byteArray` must be in the following format: `<SID>[,<backup path>]`. If you do not provide the backup path, Profile Management generates a backup folder named by current date and time.

Reset a Windows roaming profile

- Suppose you want to reset the roaming profile for user1. Use the New-BrokerMachineCommand PowerShell command. For example:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

Record sessions

September 6, 2025

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

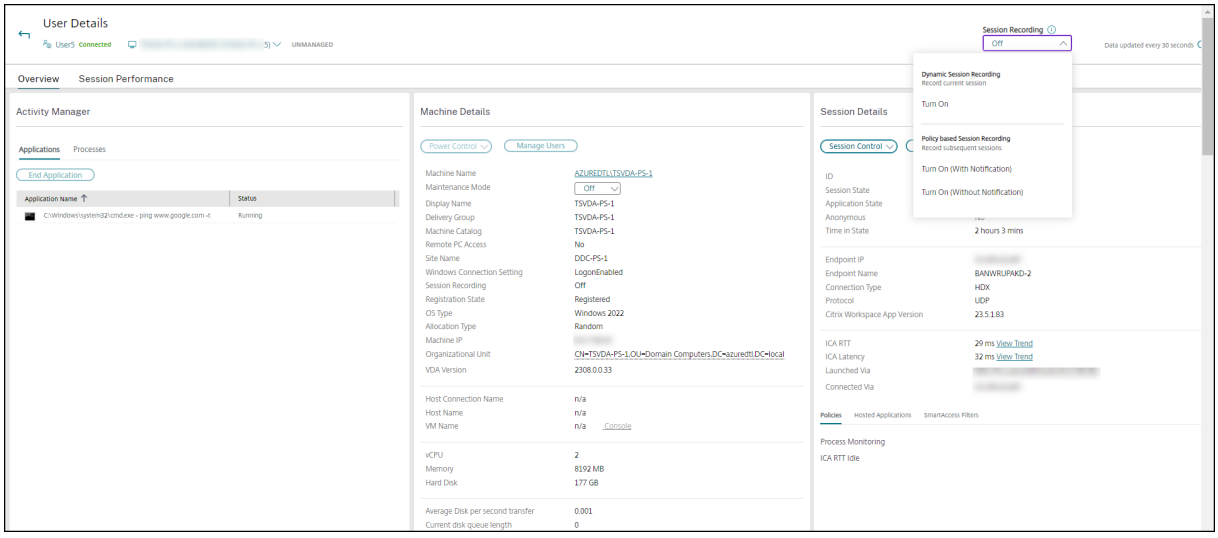
> **Note:**
>
> Changes made to the Session Recording settings through Director or the Session Recording Policy console take effect starting from the subsequent ICA session.

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

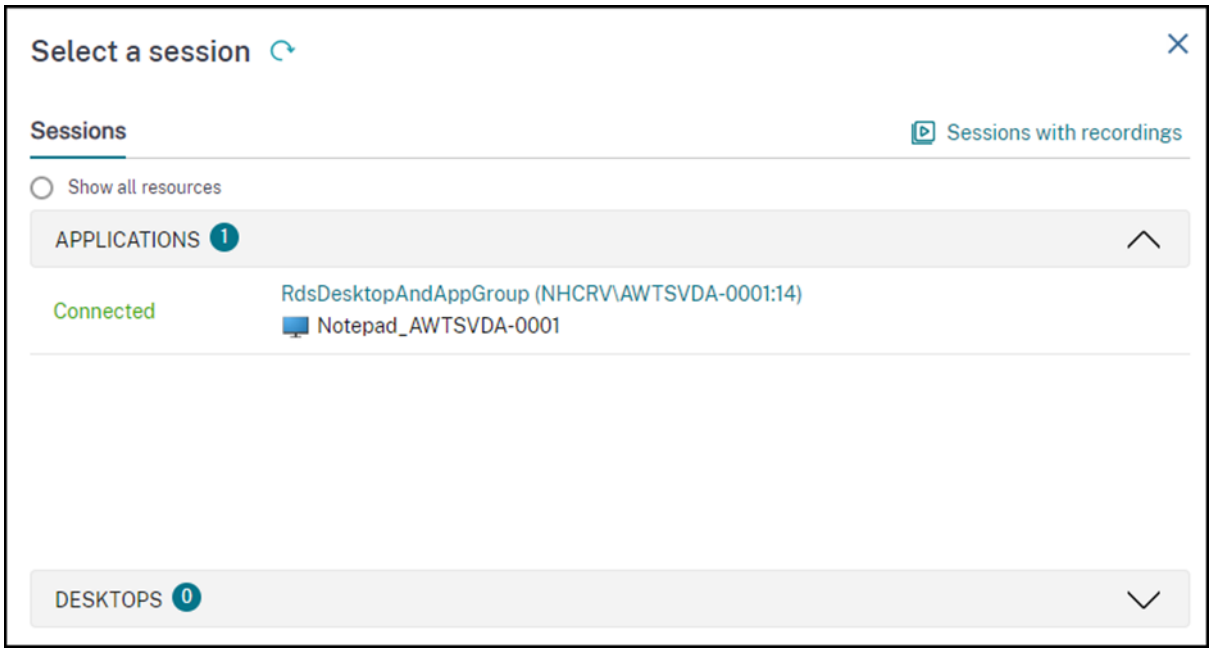
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

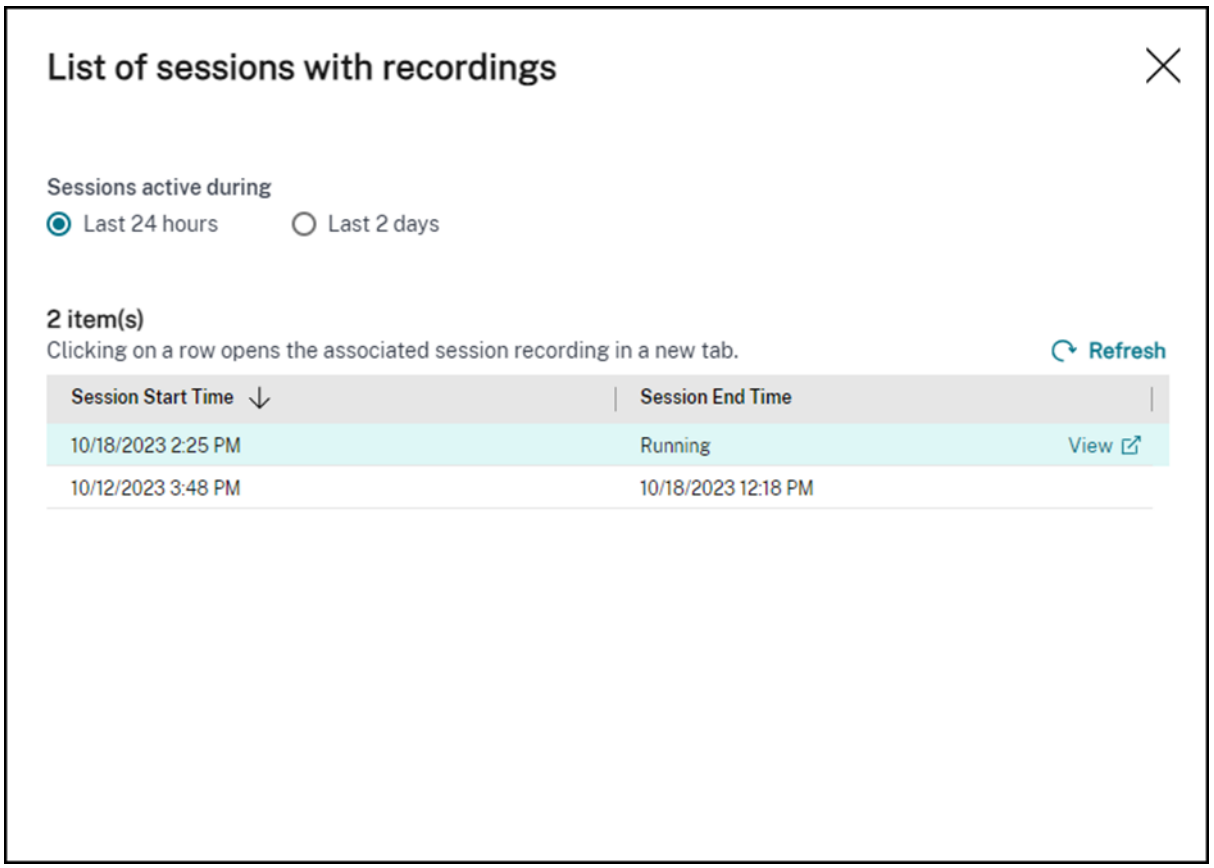
- VDA and the Session Recording servers are on version 2308 or later.
- Delivery Controller™ and Director are on version 2311 or later.

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.

Unified search for Hybrid multi-cloud deployments

September 6, 2025

Previously, during triage when you search for a user in Director, you get the user details only if the user is from an on-premises site. If the user is from a cloud site, you had to go to Monitor and search again.

With this enhanced search functionality, you can search for users from cloud sites or on-premises sites using the **Search** option in Director. You can use this feature when you use hybrid deployments (both cloud and on-premises sites) and when you use Director for triage purposes. You can get the details of users irrespective of on-premises or cloud sites. If the site is present on Director, you can directly navigate to the selected session's Activity Manager in Director. If the site isn't present in Director, you can directly navigate to the selected session's Activity Manager in Monitor. And, then continue with triage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can use the unified search console through Citrix Director.

This feature reduces the mean time to resolve issues and provides a seamless experience with a single console for both cloud and on-premises users. The additional benefit is that there is no rapid growth in the size of the database since only the cloud site details are added to Director. User details are saved in the cloud itself.

> **Note:**
>
> You can get search results within three seconds for up to six or lesser cloud sites.

To enable this feature, you need to connect the cloud site to Director.

Connecting cloud site to Director

Prerequisites

To configure Unified Search in Citrix Director, no new components need to be installed. Ensure that the following requirements are met:

- For Unified Search, outbound internet access is available on all Delivery Controllers and the machines on which Director is installed. Specifically, ensure accessibility to the following URLs:
  - Citrix Key Registration: https://*.citrixnetworkapi.net/
  - Citrix Cloud: https://*.citrixworkspacesapi.net/
  - Citrix DaaS: https://*.cloud.com/
  - Microsoft Azure: https://*.windows.net/
- In case, Delivery Controllers and Director machines are within an intranet and outbound internet access is through a proxy server, ensure the following:
  - The proxy server must allow the preceding list of URLs.
  - Add the following configuration in the Director **web.config** and **citrix.monitor.exe.config** files. Ensure that you add this configuration within the **configuration** tags:

```
<system.net>
    <defaultProxy>
        <proxy usesystemdefault="false" proxyaddress="http://<
           your_proxyserver_address>:80" bypassonlocal="true" />
    </defaultProxy>
</system.net>
```

  - The Director **web.config** is located at `C:\inetpub\wwwroot\Director\web.config` on the machine where the Director is installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

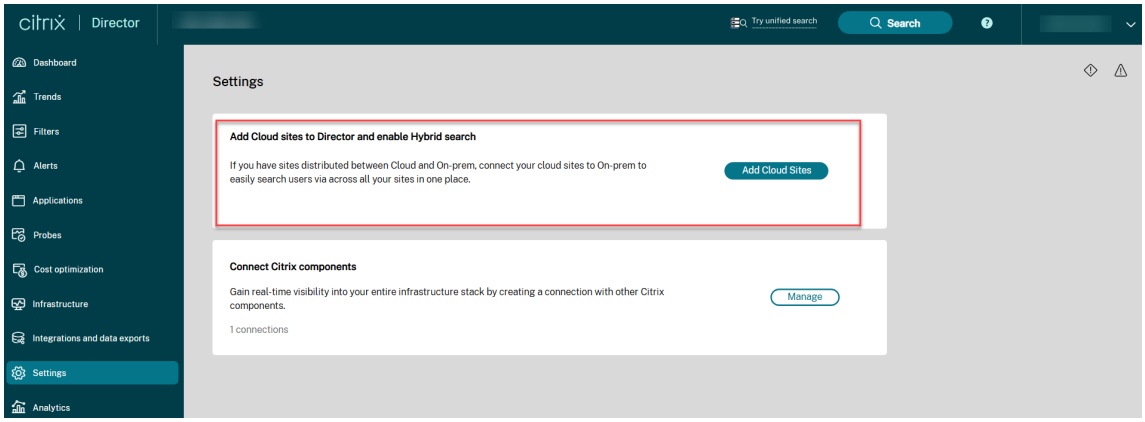
- The **citrix.monitor.exe.config** is located at `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` on the machine where the Delivery Controller is installed.

This setting is provided by Microsoft on IIS. For more information, see Proxy Configuration. The **defaultproxy** field in the config file controls the outbound access of Director and Monitor Service. Configuration and communication with Citrix DaaS requires the **defaultproxy** field to be set to true. It is possible that the policies in effect set this field to false. In this case, you must manually set the field to true. Take a backup of the config files before you make the changes. Restart the Monitoring service on the Delivery Controller for the changes to be affected.

- You have an active Citrix Cloud™ entitlement for DaaS.
- Your Citrix Cloud account is an Administrator account with rights to the Product Registration Experience. For more information about administrator permissions, see Modify Administrator Permissions.
- Ensure that there's internet access for the machine on which Citrix Director is installed.
- To use the Citrix Cloud services, you must be able to connect to the required Citrix addresses through the HTTPS port 443. For more information, see Internet Connectivity requirements.
- Ensure that you have full admin access for performing product registration.

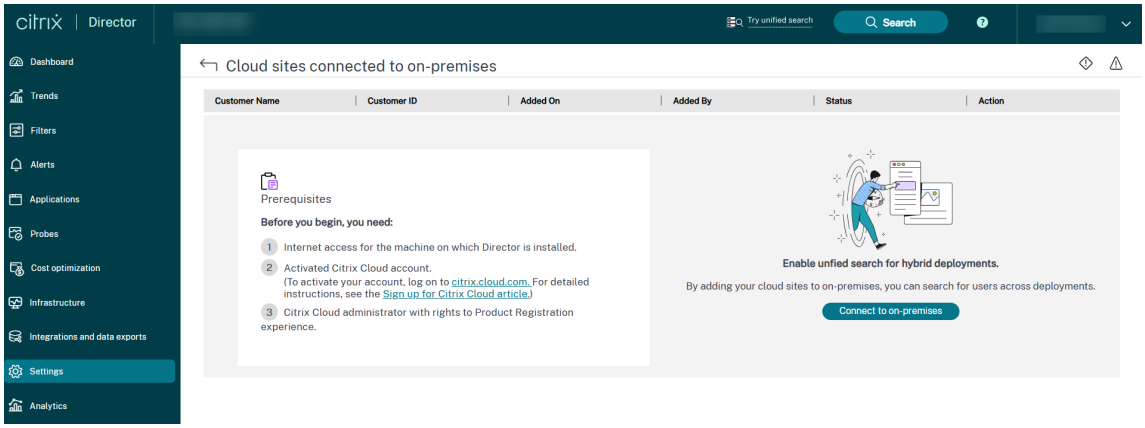
Configuration steps

1. Sign in to Director as a full administrator. The Director Dashboard page appears.
2. Click the **Settings** tab. The **Settings** page appears.

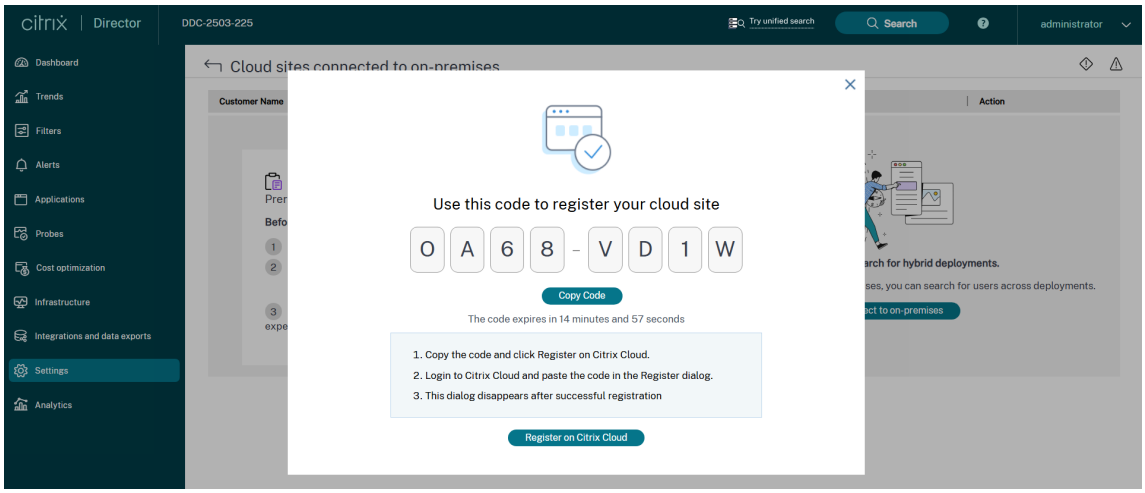


3. Click **Add Cloud Site**. The following page appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

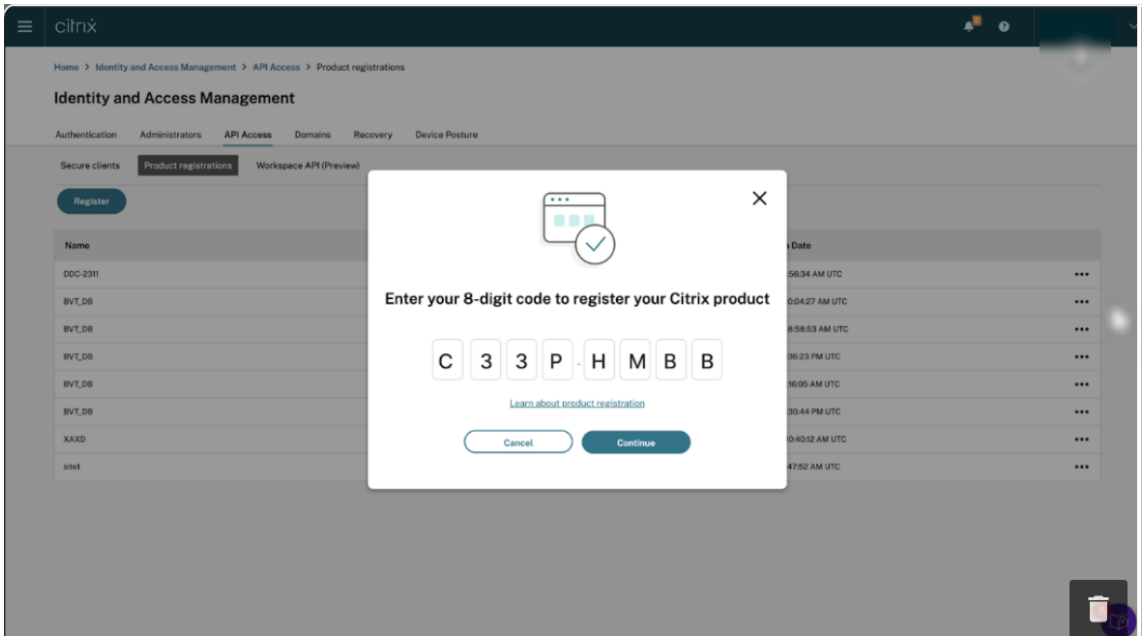


4. Review the prerequisites and then click **Connect cloud sites** to start the configuration process. A unique 8-digit registration code is generated to be used to register this site with Citrix Cloud.

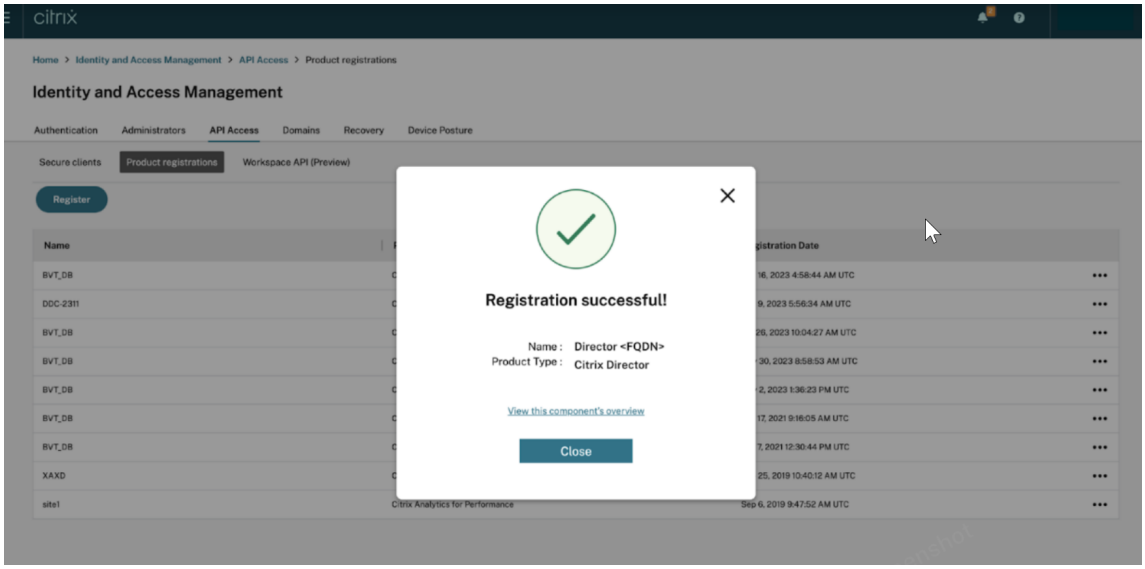


5. Click **Copy Code** to copy the code and then click **Register on Citrix Cloud**. You are redirected to the registration URL in Citrix Cloud.
6. Sign in with your Citrix Cloud credentials and select your customer.
7. Paste the copied registration code in the **Product Registrations** page in Citrix Cloud. Click **Continue** to register the site.

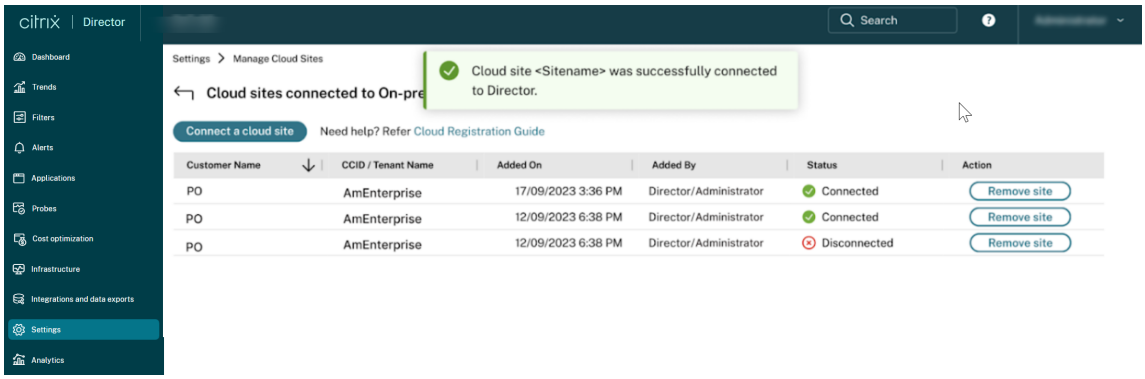
© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Click **Continue**. Your cloud site registers with Citrix Director and you get the following message:



9. Click **Close**. The following screen appears:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. To configure multiple cloud sites with Director, repeat the preceding configuration steps for each site from Director.

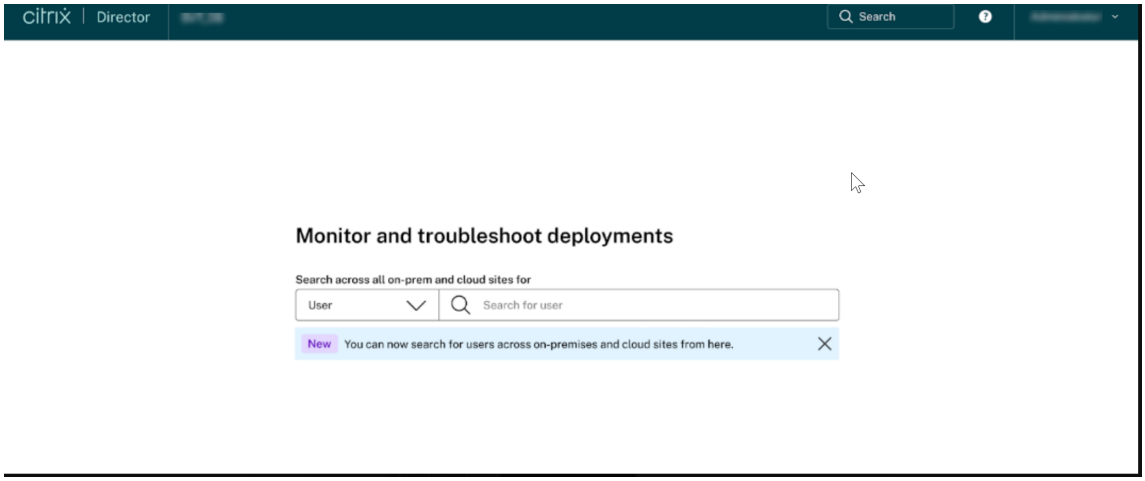
    In case you have more than one Director instance running per site, configure from any one Director instance. All other Director instances connected to the site are updated at the next refresh after the configuration process.

> **Note:**
>
> To disconnect your site from Citrix Director, click **Remove site**. This option deletes the existing configuration.

Searching for a user from hybrid deployments

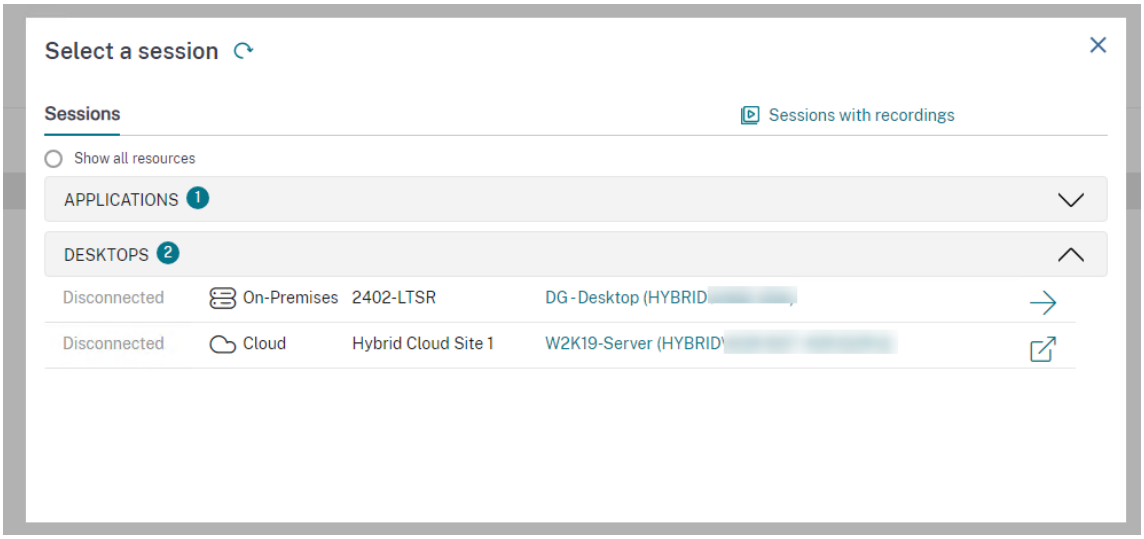
To search for a user, do the following:

1. Click **Search** at the top navigation bar. The **Monitor and troubleshoot deployments** page appears:



2. Select **User** from the drop-down list and enter the user name. A list of active and failed sessions from on-premises and cloud deployments appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Select a session to inspect:

- If it's a session using cloud deployment, the relevant DaaS Monitor URL with the user context is opened to the **Activity Manager** page to quickly begin troubleshooting.
- If it's a session using on-premises deployment, the Activity Manager page opens quickly to begin troubleshooting.

Infrastructure monitoring

September 13, 2025

Director 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 following components is monitored:

- Delivery Controller™
- Citrix Provisioning™ Service
- StoreFront™

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 Director. However, `CitrixInfraMonitor.msi` is not required for monitoring Delivery Controller. The Delivery Controller component is automatically onboarded for monitoring when connected to the Citrix Virtual Apps and Desktops site.

This feature helps you to get critical monitoring data sets and proactive alerts regarding the Delivery Controller, Provisioning Service, and StoreFront servers on a single dashboard in Director. Data is collected every five minutes from the monitored components to ensure the latest information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Delivery Controller, Citrix Provisioning (Provisioning Service) servers, and StoreFront.
- 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:

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

- Citrix Virtual Apps and Desktops version 2407 or later
- Enusre the prerequisites for Provisioning Service or the prerequisites for StoreFront are met.
- For monitoring Citrix Provisioning:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Minimum required version to monitor **DB Connectivity** and **License Server Reachability** is Citrix Provisioning 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 Director permissions:
        - Create\Edit\Enable\Delete Alert Policies
        - Create\Edit\Remove Alert Email Server Configuration
        - Create\Edit\Manage Connections to Citrix components (Infra Monitoring)
        - Dismiss Alerts
        - View Alert Policies
        - View Alerts
        - View Dashboard page
        - View Infrastructure Monitor page

> **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.

For more information, see the following:

- Getting started with Infrastructure Monitoring
- Manage connections
- Infrastructure dashboard
- Advanced alert policies
- Infrastructure policies

Getting started with Infrastructure Monitoring

September 6, 2025

You can connect to Citrix Infrastructure Monitor using:

- Manual connection - Download and install the Citrix Infrastructure Monitor service manually.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Automatic connection - The UI handles the download and installation automatically.

You can optionally configure HTTPS for Citrix Infrastructure Monitor after both manual and automatic connections.

For more information, see the following:

- Manual connection
- Automatic connection
- Configure HTTPS for Citrix Infrastructure Monitor

Manage connections

September 6, 2025

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 name of the server.
Type	The type of the connection. This can be Delivery Controller™, Provisioning Service, and StoreFront.
Version	The version of the `CitrixInfraMonitor.msi` installed on the component. This field isn't applicable to Delivery Controller.
Created by	The name of the person 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	Description
	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 Delivery Controller connections are automatically populated in this view when connected to on-premises Citrix Virtual Apps and Desktops™ sites.

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 remove a component from the Director UI or using the PowerShell command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using Director UI

Removing a component is a process of deregistering a Provisioning Service or StoreFront connection from Director. 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 Director.

Using PowerShell SDK

In the event you need to deregister a given component, run the following PowerShell command on the Delivery Controller:

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component <
    component>
```

A sample command to remove registration of the Citrix Infrastructure Monitor is as follows:

```
Remove-MonitorDirectorAgent -Component PVS -Fqdn [redacted]
```

> **Note:**
>
> Deregistering a component only stops the data flow from the specific component to Director. If you need to uninstall Citrix Infrastructure Monitor, uninstall it from the **Control Panel**.

Infrastructure dashboard

September 6, 2025

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:

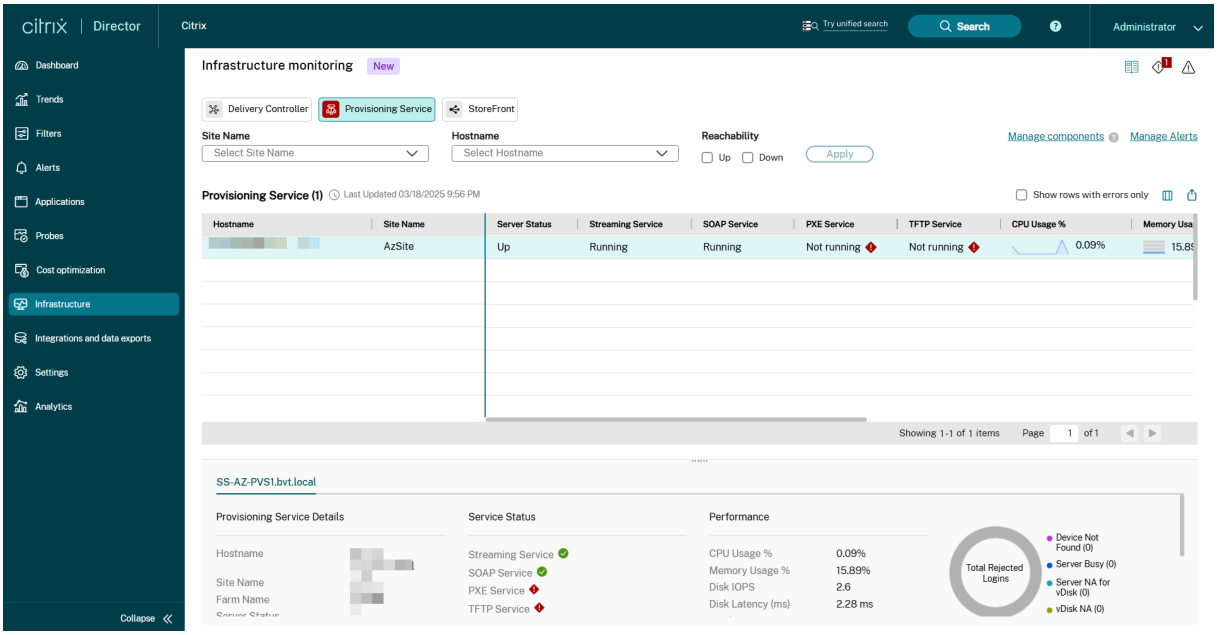
- Host name - Select the host name
- Reachability - Select **Up** (server is reachable) or **Down** (Server isn't reachable) checkbox
- Errors - Select Show rows with errors only checkbox.

Use the **Manage columns** option to choose the data to be seen in your dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Provisioning Service health metrics

Click the **Infrastructure** tab and then select **Provisioning Service**. The Infrastructure dashboard for Provisioning Service appears:



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Metrics	Description
Dependent Services	Server Status	Shows the reachability state of the given server. Possible 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.
	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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Metrics	Description
	License Server Reachability	Displays whether the license server is reachable or not. If you're using the 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).
	Total Reconnect Count	Displays how many times the session got reconnected.
	PXE Service	Displays the status of the Preboot Execution Environment service. This metric shows the Windows services status. The possible values are: *Not running*, *Running*, *Not Installed*, and *n/a* (with help icon).
	TFTP Service	Displays the status of the Trivial File Transfer Protocol service. 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 5 mins.
	Average CPU %	Displays the average CPU percentage of the Provisioning Service server aggregated over the last 10 mins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

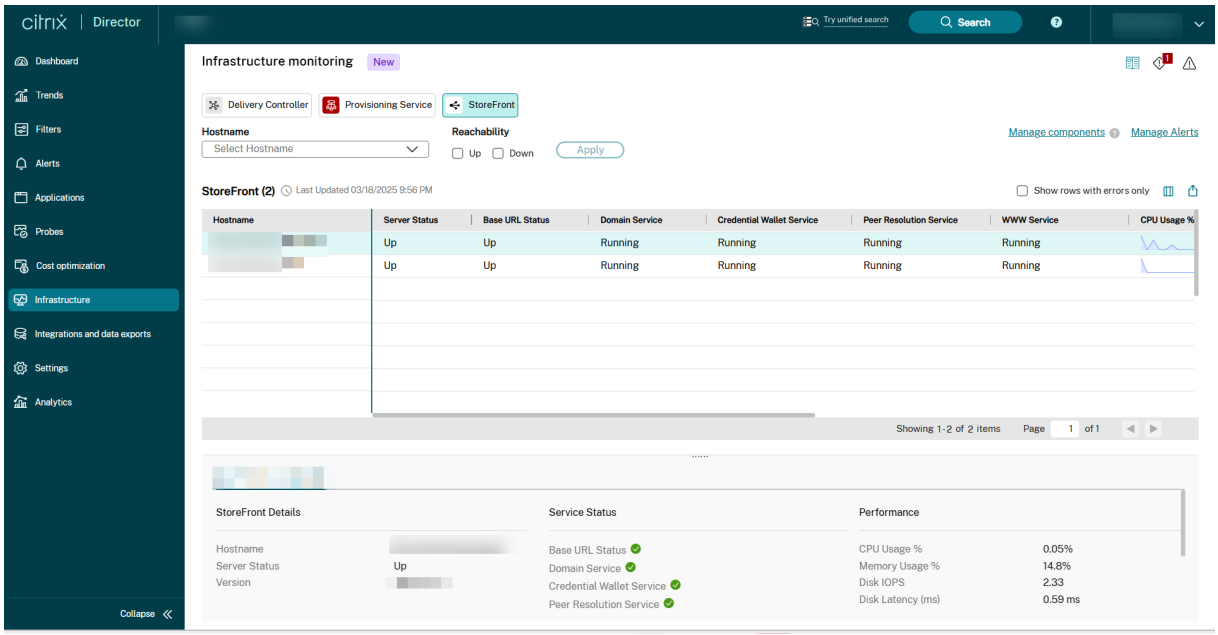
Category	Metrics	Description
	Peak CPU %	Displays the peak CPU percentage of the Provisioning Service server in the last 5 mins.
	Memory Usage %	Displays the usage of memory in percentage using a stack chart. The value displayed is the latest one at the end of the last 5 mins.
	Average Memory %	Displays 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.
	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 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.
	Average 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Metrics	Description
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:



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Metrics	Description
	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.
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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Metrics	Description
Resource Utilization	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).
	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.
	Average 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.
	Average 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Metrics	Description
Impact	Average 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.
	Disk Latency (Ms)	Displays the latency value of the disk using a line chart.
	Average 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.
	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*.

Delivery Controller™ health metrics

The Delivery Controller component is added by default as part of Infrastructure monitoring. The Delivery Controller component that is connected to the Citrix Virtual Apps and Desktops™ site is auto onboarded for monitoring.

This feature enables customers to monitor controllers' health under the infrastructure monitoring

© 1997–2026 Citrix Systems, Inc. All rights reserved.

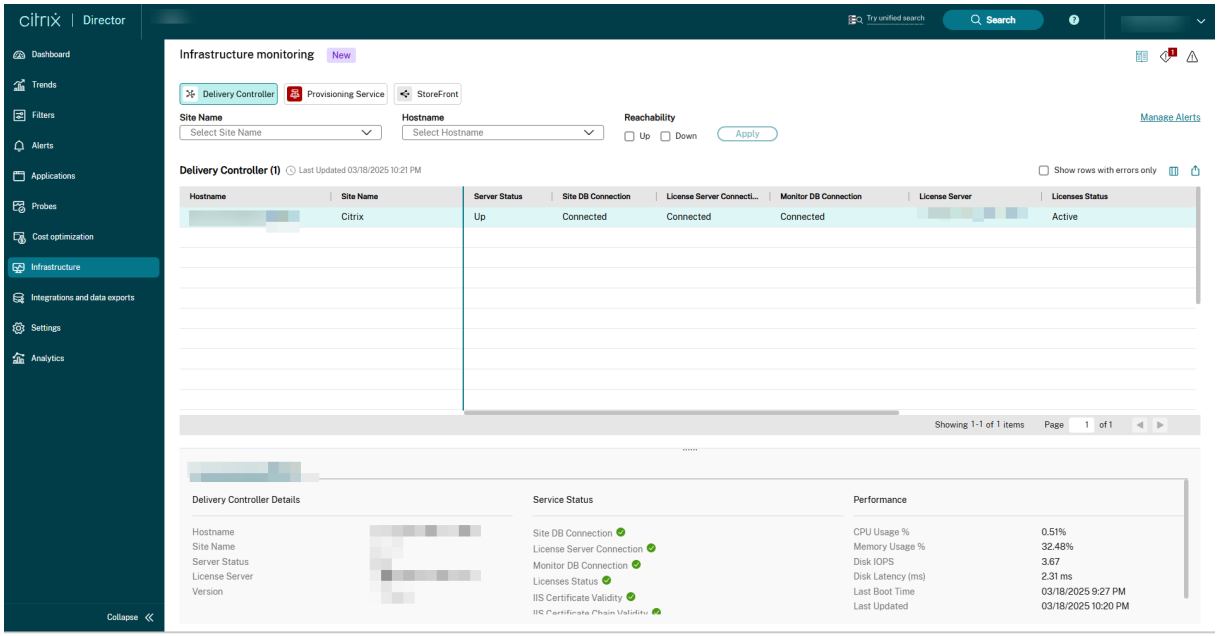
dashboard and configure alerts for it. The alerting functionality enables customer admins to get alerted if any of the policies created for delivery controllers are in the critical or warning stage.

You can select the required Site Name and the details are displayed according to the selected site name. You can also select the **Reachability Status** such as *Up* or *Down*.

Note: The `CitrixInfraMonitor.msi` file is not required for monitoring Delivery Controllers.

You can monitor both single-site and multi-site details for the infrastructure details.

Click the **Infrastructure** tab and then select **Delivery Controller**. The infrastructure dashboard for the Delivery Controller appears:



The following details are monitored for the Delivery Controller:

Category	Metrics	Description
Reachability	Server Status	Shows the reachability state of the given Delivery Controller. Possible values are *Up* and *Down*.
	Version	The version of the Delivery Controller.
	Last Boot Time	Displays the time when the Delivery Controller was last booted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Metrics	Description
Dependent Services	Last updated	Displays the time when the data was collected from the Delivery Controller.
	Site DB Connection	Displays the status of the site database connection. The possible values are *Not Connected*, *Connected*, *Unknown*, and *n/a* (with help icon). **Unknown:** This value appears when no metrics are collected or available. **n/a:** Not applicable. This value appears when the server status is down.
	License Server Connection	Displays the status of the license server connection. The possible values are *Not Connected*, *Connected*, *Unknown*, and *n/a* (with help icon).
	Monitor DB Connection	Displays the status of the monitor database connectivity. The possible values are *Not Connected*, *Connected*, *Unknown*, and *n/a* (with help icon).
	License Server	Displays whether the license server is reachable or not.
	License Status	Displays the status of the license.
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 Delivery Controller 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 Delivery Controller 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 Delivery Controller server aggregated over the last 10 mins.
	Peak Memory %	Displays the peak memory percentage of the Delivery Controller 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 Delivery Controller server aggregated over the last 10 mins.
	Peak Disk IOPS %	Displays the peak disk IOPS percentage of the Delivery Controller 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 Delivery Controller server aggregated over the last 10 mins.
	Peak Disk Latency %	Displays the peak disk latency percentage of the Delivery Controller server in the last 5 mins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Metrics	Description
Impact	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 whether the StoreFront IIS Certificate Chain is valid or not. The possible value is *Yes* or *No*.

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. You can create the alerts related to infrastructure from the **Advanced Alert Policies** section.

For more information, see the Advanced alert policies page.

Application and Desktop Probing

September 8, 2025

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 Director.

Requirements

- Delivery Controller runs version 7.18 or later for application probing and version 1906 or later for desktop probing.
- 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 authentication via StoreFront and Citrix Workspace using Active Directory credentials. In cases where the endpoint device is connected to StoreFront / Workspace

© 1997–2026 Citrix Systems, Inc. All rights reserved.

via 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).

> **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.

- 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.

User accounts or permissions required to run Probing:

- A unique StoreFront user to probe on each endpoint machine. The StoreFront user need not be an administrator; the probes can run in a non-administrator 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Probe Agent version 2103 and later supports site aggregation. When you configure Citrix 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:

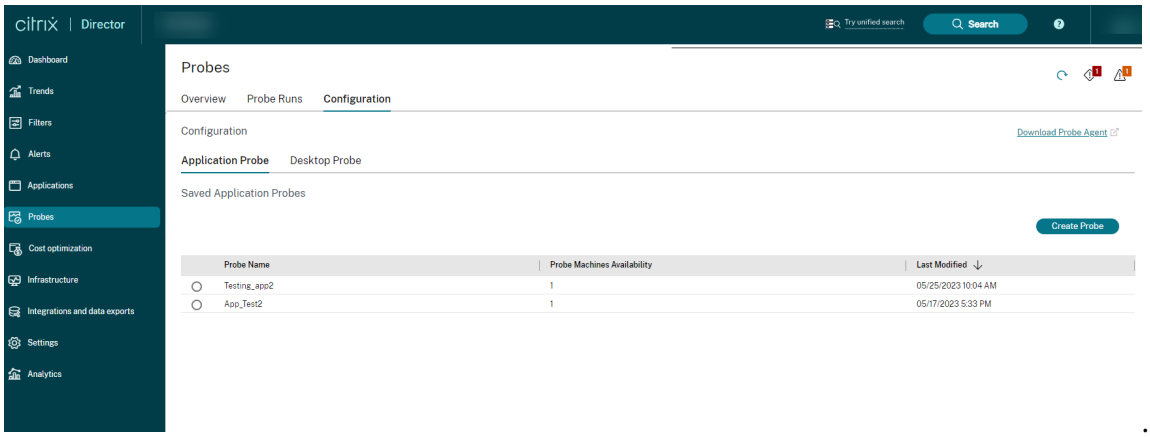
- Multiple on-premises sites having one StoreFront URL.
- On-premises and cloud sites having either a StoreFront or Workspace URL.
- Multiple cloud sites having one Workspace URL.
- On-premises sites connected to StoreFront or Workspace via Citrix Gateway.

> **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 Director and reports back the results to Director.

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. The download link is also available in the **Probes** tab in Director.

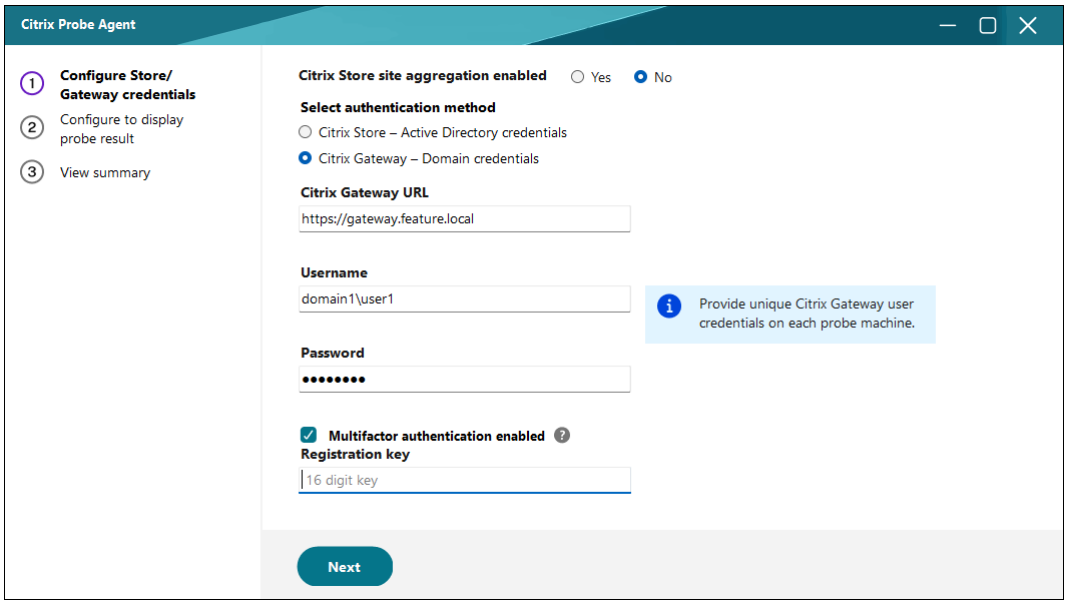


3. If you have aggregated sites, select the Workspace (StoreFront) Site Aggregation Enabled option to enable enumeration of applications and desktops from aggregated sites.
4. Select an authentication method and enter the relevant credentials. Credentials are encrypted and stored securely.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Configure with your StoreFront Active Directory credentials. Configure a unique Workspace (StoreFront) user on each endpoint machine.

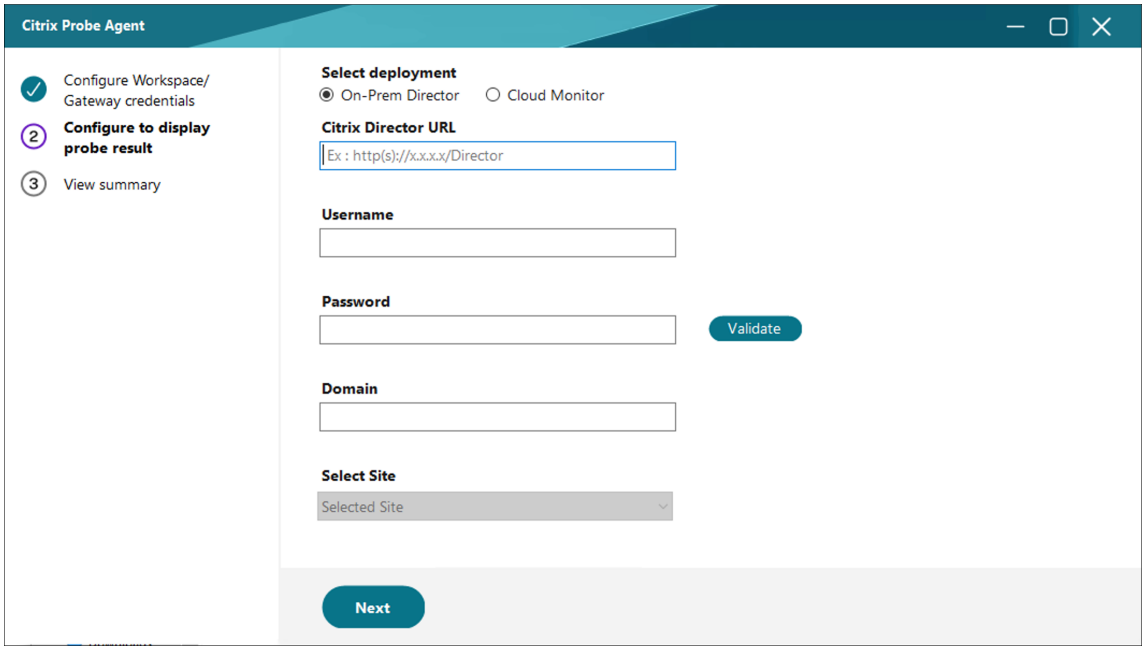
6. Choose the Citrix Gateway option if your endpoint is connected to StoreFront via Citrix Gateway and configure with your Citrix Gateway Domain credentials.



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 your Director credentials, and click **Validate**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. Select your site and click **Next**.
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.

> **Note:**
>
> You can use the PowerShell script contained in Automating Citrix Probe Agent Installation and Configuration to automate the installation and configuration of Citrix Probe Agent.

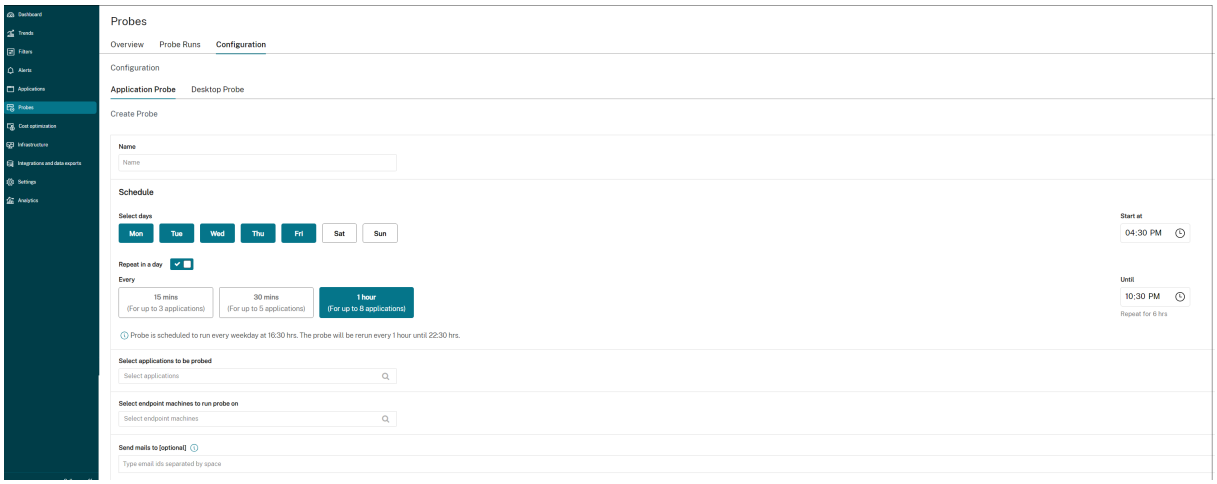
Step 2: Configure Probing in Director

> **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> 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 **Probes** > **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.
6. Enter the email addresses of admins to send the results of failed probes. 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> to prevent overlaps.

Step 3: Probe execution

The agent runs probing as per the probe configuration that it fetches from Director periodically.

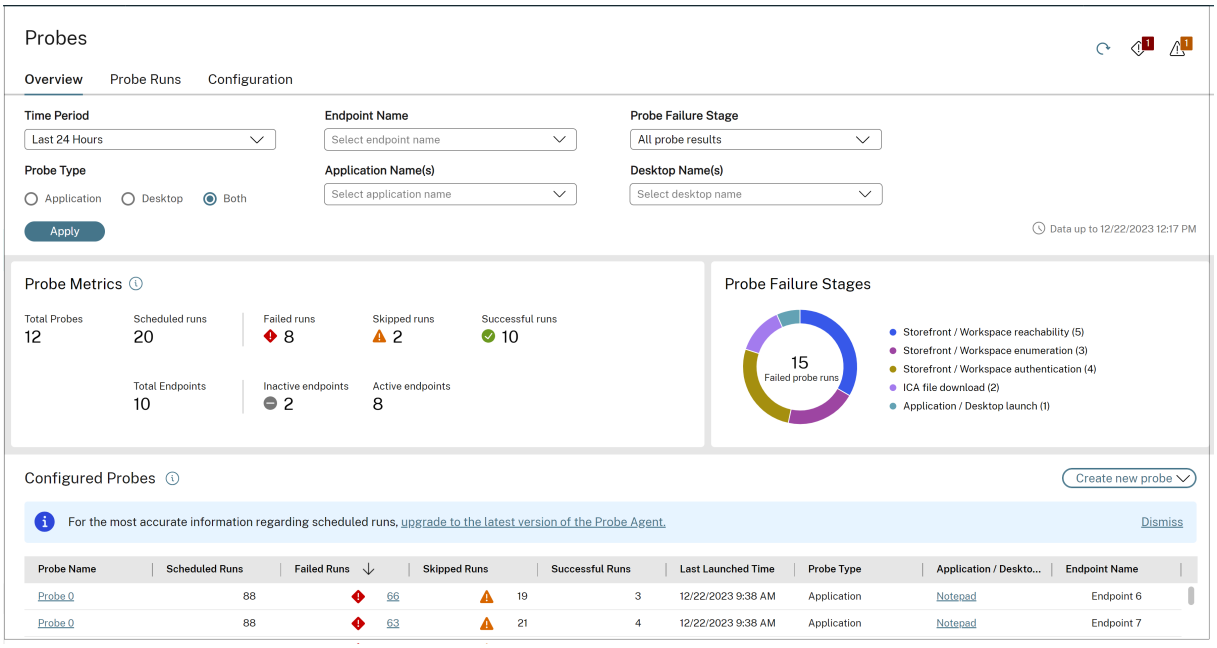
It launches selected applications serially using StoreFront. The agent reports the results back to Director via the Monitor database. Failures are reported in five specific stages:

- **StoreFront Reachability** - configured StoreFront URL is not reachable.
- **StoreFront Authentication** - configured StoreFront credentials are invalid.
- **StoreFront Enumeration** - StoreFront Enumerate applications list does not contain the application or desktop to be probed.
- **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 runs that did not run to completion due to either the endpoint being inactive, or services being unavailable.
- Successful Runs –the number of probes that completed successfully with no failures in any stage during the app/desktop launch.

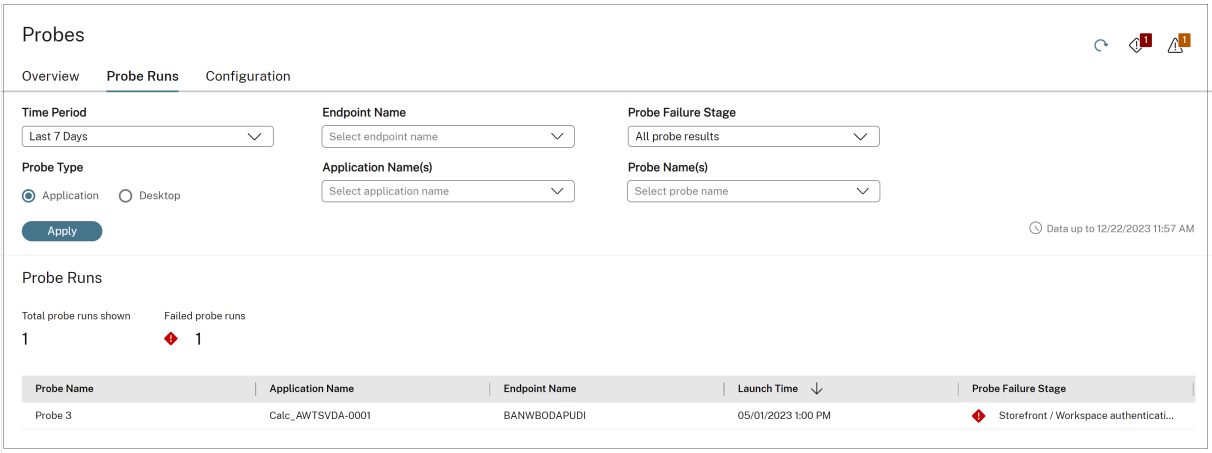
The total number of endpoint machines is also displayed, with the count of active and inactive machines.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cost optimization

May 5, 2025

Citrix Director 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:

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

The **Cost Optimization** page includes the following features:

- Cost savings
- Infrastructure rightsizing

How is the cost calculated for optimizing the cost?

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

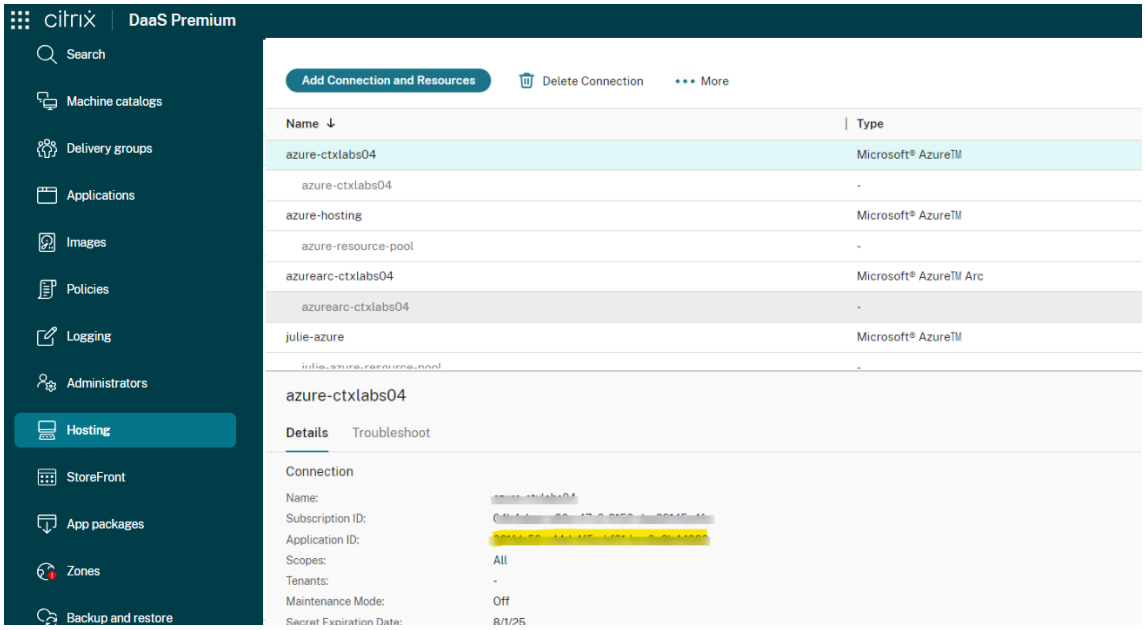
The order of priority for calculating the cost is as follows:

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.
2. If permissions aren't available, the Azure retail price is displayed. For more information, see Azure Retail Prices overview.
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.
4. If there is no cost mentioned in the Web Studio, the default cost of $1 is considered.

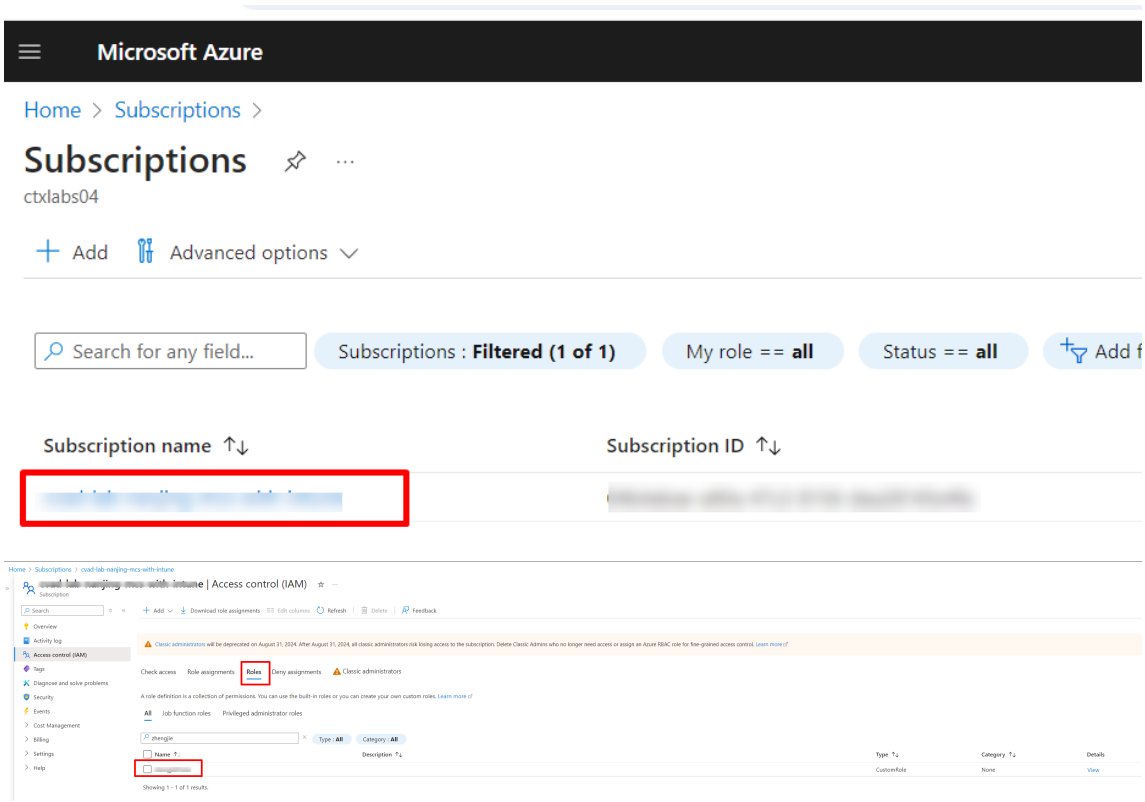
To find the account details of Azure and add the required permission to find the effective price, do the following:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Go to the Azure AD 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.



6. Add the *Microsoft.Consumption/pricesheets/read* permission to the role.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

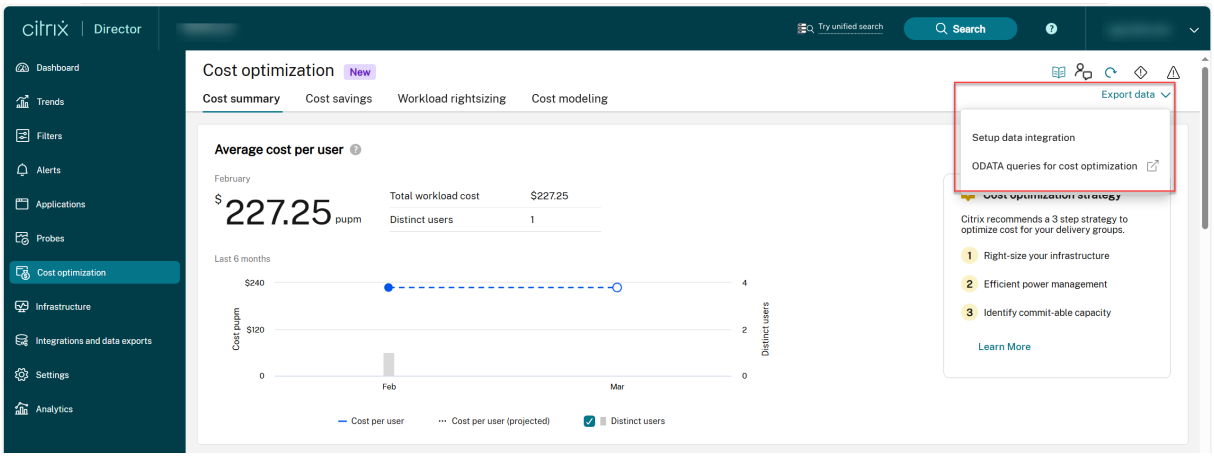
Calculating costs for machines other than Azure

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



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
- Monitor model
- Monitor notifications

Sample ODATA queries

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://<DDC URL>/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://[<DDC URL>|https://api-us.cloud.com/monitorodata/
    ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /
    monitorodata/ResourceUtilizationSummary?$apply=filter(desktopGroupId
     eq desktop-group-id and granularity eq 1440 and SummaryDate ge
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        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:

```
1  https:// <DDC URL> /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,FailureDate,CurrentPowerState,
       CurrentSessionCount,IsInMaintenanceMode,LastPowerActionFailureReason
       ,LastPowerActionCompletedDate
```

Find out total savings For more information on cost savings, see the Cost savings page.

Sample query:

```
1  https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
       ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /
       monitorodata/MachineCostSavingsSummaries?$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:

```
1  https:// <DDC URL> /monitorodata/MachineCostSavingsSummaries?$filter=
       SummaryDate eq 2024-08-09T06:00:00Z&$select=TotalMachinesCount,
       PowerManagedMachinesOff,PowerManagedMachinesInHibernate,
       PowerManagedMachinesOnWithSessions,
       PowerManagedMachinesOnWithoutSessions
```

Cost savings

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
- 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. Similarly, 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.

© 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 includes **Estimated 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 savings: This graphical representation helps to evaluate the efficient utilization of infrastructure resources. The cost savings are displayed in the currency of the hypervisor or as a percentage of the cost incurred. This graph shows the savings achieved from the compute-related savings and storage savings.

Note:

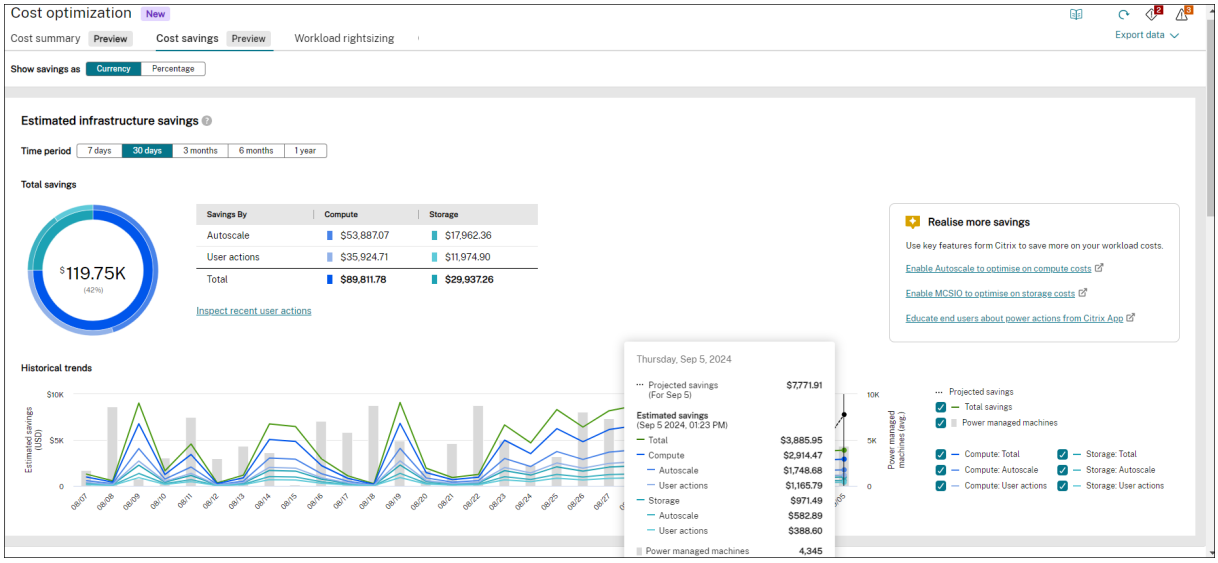
> To view the savings from storage:
>
> - Autoscale must be enabled to optimize compute costs. For more information, see Get started with Autoscale.
> - Change the storage type to a lower tier when a VM is shut down to optimize storage costs. For more information, see Change the storage type to a lower tier when a VM is shut down documentation.
> - This feature is currently applicable only to Azure machines.

You can view the results for last:

- Seven days
- Thirty days
- Three months
- Six months
- Twelve months

The following picture shows the Estimated infrastructure savings section:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following table lists the elements of the Estimated infrastructure savings graph:

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 the total savings achieved from the storage savings.
Storage - Autoscale	Displays total savings achieved from the storage savings that are using the Autoscale feature.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Element	Description
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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Catalog details**

  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**

  With Autoscale enabled, the power-managed machines are turned off when not in use to optimize costs. You can get the following details:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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. This data provides you the opportunity 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.

Workload rightsizing

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Workload rightsizing** (previously **Infrastructure rightsizing**) page helps you to analyze the provisioning and sizing aspects of your delivery group based on resources utilization. Based on this analysis, you can:

- Reduce spending on the unused resources
- Identify the machine net active usage which is calculated based on the average machine uptime and net wastage time.
- Identify if the machines for the given delivery group consumption are over, under, or right sized
- Identify if the utilization is mainly driven by Power users (indicated by higher utilization by top 5 percentile machines compared to the rest of the group)

You can filter the Workload 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 Workload rightsizing page offers:

- Insight in to machine net active usage
- Insight in to the utilization details
- Insight into details of power users and export these data
- Summary of the resource utilization
- Trends on the resource utilization

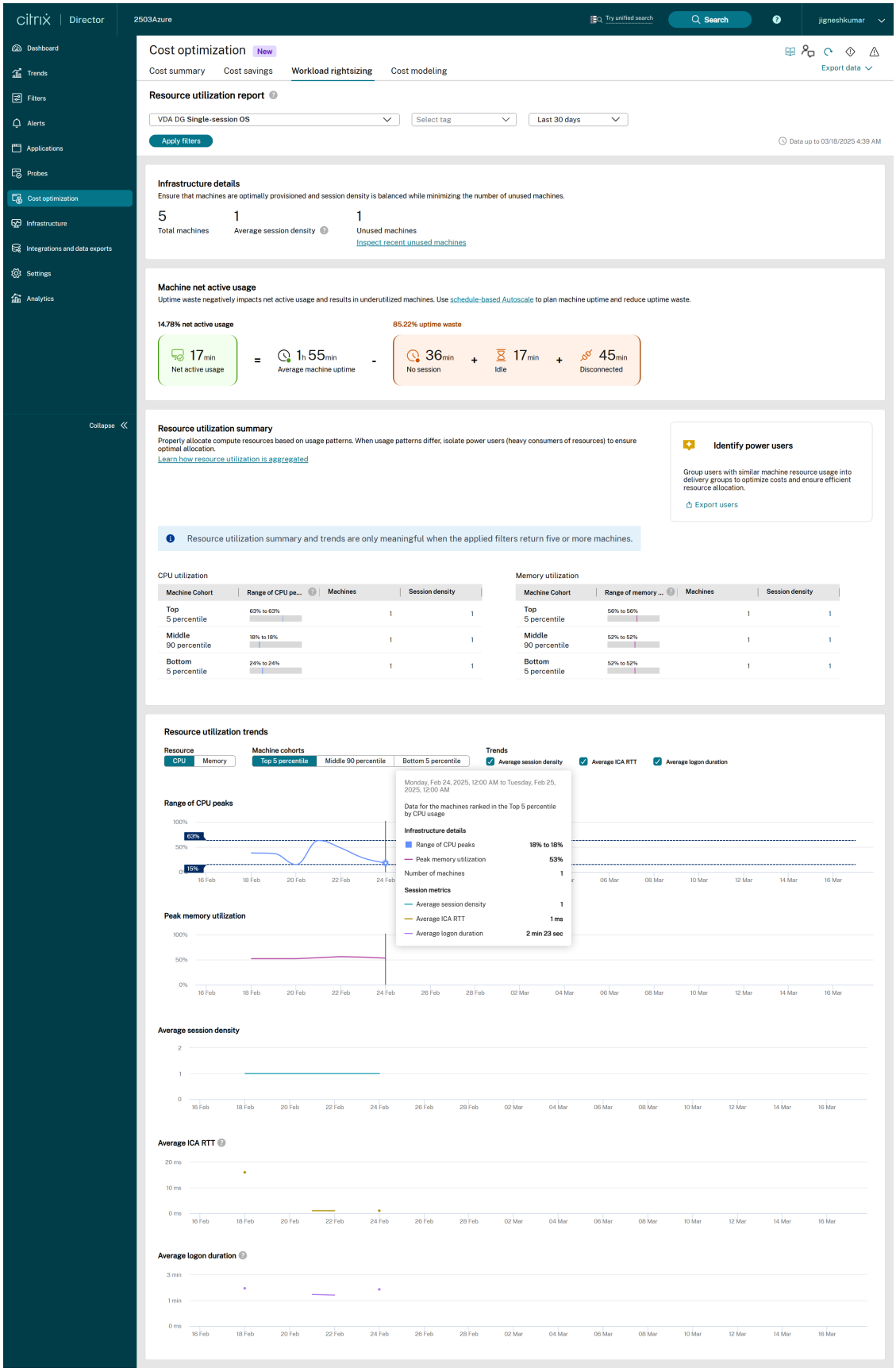
The aggregated data displayed on this page is updated as follows:

- One hour for Last 24 hours, and Last 7 days filter
- One day for Last 30 days filter

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.

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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Workload rightsizing** page includes:

- Machine net active usage
- Utilization details
- Resource utilization summary
- Resource utilization trends

Machine net active usage:

This section displays detailed machine usage information, enabling you to optimize costs. By understanding the average net active usage time of machines in a Delivery Group, administrators can determine the best power management and billing strategies to maximize savings. Net active usage is calculated by deducting the total uptime waste from the average machine uptime. All times are in minutes.

The **Machine Net Active Usage** section provides the following:

- **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:** The wasted uptime due to idle sessions. This is the time when all sessions on the machine are idle.
- **Disconnected Time:** The wasted uptime due to disconnected sessions. This is the time when all sessions on the machine are disconnected.

Utilization details:

This section provides details on the utilization of the selected delivery group and for the selected tags. You can view the details for the last 24 hours, 7 days, and 30 days. The **Utilization details** section provides details for the entire duration of the selected time filter. For example, if 7 days is selected, the total machine count is the total number of machines that were on at any point during the 7 days. The **Utilization details** section provides the following:

- **Total machine** - Displays the total number of machines. This data includes all the machines which were powered on during the selected period. For example, If 7 days is selected, the total machine count is the total number of machines that were on at any point during the 7 days.
- **Average session density** - This data 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.
- **Average machine uptime** - It is the ratio of total uptime of the power managed machines and for the selected time period. How much time the machine was up, per day per machine. Suppose that there are two machines in one delivery group or in the selected tag, and one machine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

was used for 24 hours and the other machine was used for 1 hour. The average machine uptime is 12 hours 30 minutes. In this example, the selected filter value is Last 24 hours.

- **Unused machines** - Displays the number of machines which had no sessions over the selected time period but which was still powered on. Click the **Unused Machines** link to open the **Filters** tab where you can view all the machines in that same delivery group which are currently powered on and have no sessions.

Resource utilization summary:

This section provides a summary on how the resources were used for the selected delivery group and for the selected tags. You can select multiple tags up to five tags. You can view the details for the last 24 hours, 7 days, and 30 days. The machines are ranked based on the utilization. The **Resource utilization summary** section provides details on CPU utilization and memory utilization for the machines with active sessions. This section also provides an option to identify power users and helps you to export the power users data.

- **CPU utilization**:
  - Machine cohort - Provides information about the machine groups categorized into top, middle, and bottom based on its CPU utilization. 5% of the most used machines are categorized under **Top 5 percentile**, 5% of the least used machines are categorized under **Bottom 5 percentile**, and the remaining 90% are categorized under **Middle 90 percentile**.
  - 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.
- **Memory utilization**:
  - Machine cohort - Provides information about the machine groups categorized into top, middle, and bottom based on its memory utilization. 5% of the most used machines are categorized under **Top 5 percentile**, 5% of the least used machines are categorized under **Bottom 5 percentile**, and the remaining 90% are categorized under **Middle 90 percentile**.
  - Range of memory Peaks - Displays the memory 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.
  - Identify power users - This option 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.

The following table provides information on the possible action items that you can do based on the values present in the **Resource Utilization summary** section:

Scenario	Action item
CPU utilization is more	Increase the CPU specifications of the delivery group. Or, identify the higher usage users and move them to a different delivery group with better specifications.
CPU utilization is less	Decrease the CPU specification of the delivery group.
Memory utilization is more	Increase the memory specifications of the delivery group.
Memory utilization is less	Decrease the memory specification of the delivery group.

How is the data populated in the Resource utilization summary section?

The data in the **Resource utilization summary** section is populated based on the data in the **Resource utilization trends**. The summary gives you details only for the machines with active sessions. The summary gives you better results when there are more than five machines.

Based on the number of machines in the selected delivery group, the maximum and minimum utilization values are calculated.

For example, consider that you have selected Last 7 days as a time period and you have 20 machines in the selected delivery group. These 20 machines are further categorized into **Top 5 percentile**, **Middle 90 percentile**, and **Bottom 5 percentile**. The CPU and memory utilization is calculated when there are active sessions. For example, in this case, the first and last machines into the top 5 and bottom 5. The remaining 18 machines are categorized into the middle 90 percentile. In this case since there is only one machine in the **Top 5 percentile**, the maximum and minimum value is the same. When there is more than one machine in the cohort, the highest and lowest value of the cohort is based on the maximum value of the highest-ranked machine in that group, and the maximum value of the lowest-ranked machine in that group respectively.

When you select **CPU** as the **Resource** type, the **Range of CPU peaks** and the **Peak memory utilization** for the selected machines are displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you select Memory as the Resource type, the Range of memory peaks and the Peak CPU utilization for the selected machines are displayed.

Resource utilization trends: This section provides a graphical representation for the Range of CPU peaks, peak memory utilization, average Session density, average ICA® RTT, and average logon duration.

You can filter the details for the following:

- Resource - CPU and Memory
- Machine cohorts - Top 5 percentile, Middle 90 percentile, and Bottom 5 percentile
- Trends - Average session, Average ICA RTT, Average logon duration.

You can view the following charts:

- **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 is started during the selected time.

Cost summary

September 6, 2025

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

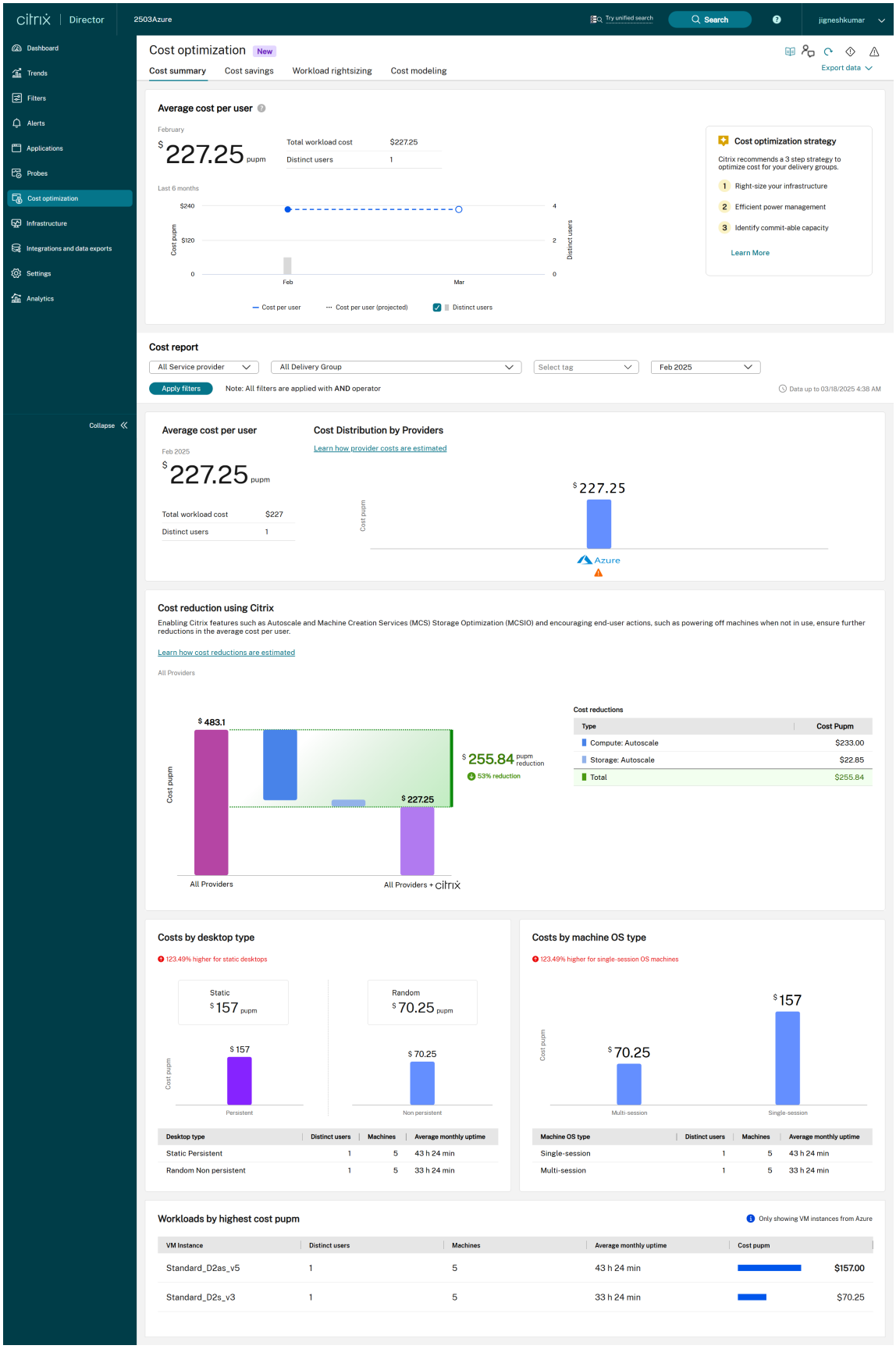
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Information on costs and savings categorized by:
  - Platform provider
  - OS type
  - 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 **Director** > **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.

  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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Feature compatibility matrix

September 13, 2025

Citrix Director 7 2503 is compatible with:

- Citrix Virtual Apps and Desktops™ 7 2112 and later
- Citrix Virtual Apps and Desktops 7 1912 LTSR

Within each site, although you can use Director with earlier versions of Delivery Controller™, all the features in the latest version of Director might not be available. Citrix recommends having Director, Delivery Controller, and the VDAs at the same version.

> **Note:**
>
> After you upgrade a Delivery Controller, you are prompted to upgrade the site when you open Studio. For more information, see the **Upgrade Sequence** section in Upgrade a deployment.

The first time you log in after a Director upgrade, a version check is performed on the configured sites. If any site is running a version of the Controller earlier than that of Director, a message appears on the Director console, recommending a site upgrade. Additionally, as long as the version of the site is older than that of Director, a note remains displayed on the Director Dashboard indicating this mismatch.

> **Note:**
>
> Earlier versions of Citrix Director do not display policies applied to user sessions running on recent VDA versions. Citrix Director 1912 and earlier versions do not display policies applied to user

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> sessions running on VDA versions 2003 and later. Use Citrix Director versions 2003 and later to view those policies.

Specific Director features with the minimum version of Delivery Controller (DC), VDA and other dependent components required along with License Edition are listed below.

Director Version	Feature	Dependencies - min version required	Edition
2507	Microsoft call quality dashboard for monitoring and troubleshooting	None	All
2507	Improved handling of vertical and horizontal load balancing alerts	None	All
2507	Change in default policy behavior of the endpoint data collection used in Session topology	None	All
2507	Enhanced definitions of ICA RTT and Network latency measurements in Director	None	All
2507	Enhanced visibility of plug-in manager and optimization state for real-time communication applications	None	All
2503	Cost modeling for Azure workloads	None	All
2503	Enhancements to Cost savings page	None	All
2503	Director integration with uberAgent	VDA 2503 (uberAgent installed)	All

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director Version	Feature	Dependencies - min version required	Edition
2503	Local application usage reporting	VDA 2503	Platinum-licensed sites
2503	Monitoring VDA logon duration details	VDA 2503	All
2503	Additional metrics collection for Provisioning Service	VDA 2503	All
2503	Option to extend monitoring of HDX optimization beyond Microsoft Teams	VDA 2503	All
2503	Session auto reconnect details in Filters view and Session Performance tab	VDA 2503	All
2503	Unified platform experience for Citrix Director	None	All
2503	Custom role to limit bulk action option for user actions	None	All
2503	Provision to set site level alerts for Provisioning Service and Delivery Controller	VDA 2503	All
2503	Integration with Webhook	None	All
2411	Least used and unused published apps report on the Applications page	DDC 7.16, VDAs 7.15	Platinum-licensed sites

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director Version	Feature	Dependencies - min version required	Edition
2411	Enumerated application details for TCP or UDP apps on the Activity Manager	VDA 2411 and DDC 2411	All
2411	Webhook configuration using PowerShell SDK	VDA 2411 and DDC 2411	All
2411	Bulk alert dismissal	VDA 2411 and DDC 2411	All
2411	Machine net active usage in Workload rightsizing page	None	All
2411	Cost savings by optimizing storage usage (Preview)	None	All
2411	Cost summary (Preview)	None	All
2411	Delivery Controller monitoring (Preview)	VDA 2411	All
2411	Connecting Citrix components from the UI (Preview)	VDA 2411	All
2407	Cost optimization	None	All
2407	Integrations and data exports	VDA 2407	All
2407	Diagnose historical user sessions (Preview)	VDA 2407	All
2407	Activity Manager for Secure Private Access session (Preview)	VDA 2407	All

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director Version	Feature	Dependencies - min version required	Edition
2407	Secure Private Access integration for TCP and UDP apps with Director (Preview)	VDA 2407	All
2407	Infrastructure monitoring (Preview)	VDA 2407	All
2407	Unregistered machines alert	VDA 2407 and DDC 2407	All
2407	Machine uptime alert	VDA 2407 and DDC 2407	All
2407	Failed power on action and Failed Power off action alert	VDA 2407 and DDC 2407	All
2407	Capability to include CSV attachment in alert emails and JSON payload in alert Webhook	VDA 2407 and DDC 2407	All
2407	Inspect machines with recent power actions	VDA 2407	All
2407	Advanced alert policies	VDA 2407 and DDC 2407	All
2407	Unified search for cloud and on-premises users	DDC 2407	All
2407	Published application usage monitoring charts on Dashboard	VDA 2407 and DDC 2407	Platinum-licensed sites
2402 LTSR	Secure Private Access integration for web and SaaS apps with Director (Preview)	VDA 2402 LTSR	All

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director Version	Feature	Dependencies - min version required	Edition
2402 LTSR	Support for Microsoft Teams version 2.1 or earlier	VDA 2402 LTSR	All
2311	Play Back live and recorded sessions	VDA 2308 and DDC 2311	All
2311	Session topology and performance metrics	Multiple versions - link	All
2311	Optimal screen resolution	None	All
2311	MS Teams Optimization	VDA 2311 and DDC latest	All
2311	Probes Overview enhancements	None	All
2311	Revamped Session Logon Duration view	None	All
2308	Probes summary and drilldown	None	All
2308	Citrix Probe Agent support for Citrix Gateway Multi-factor authentication	Citrix Gateway	All
2308	Disable Hypervisor Alerts	None	All
2308	Trends for Session Experience metrics	None	All
2305	Support authentication via Citrix Gateway	None	All
2305	Autoscale management in Director	None	All
2303	Failed Machines Alert	DC 7 2303	Premium

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director Version	Feature	Dependencies - min version required	Edition
2203	TLS 1.3 support	-	All
2212	Real-time GPU Utilization available for AMD GPUs	DC 7.14 and VDA 7.14 running 64-bit Windows and HDX 3D Pro enabled	All
2212	Advanced Probe Scheduling	DC 7 1906 and Citrix Probe Agent 2209	Premium
1909	Configure on-prem sites with Citrix Analytics for Performance	DC 7 1906 and VDA 1906	All
1906	Session Auto Reconnect	DC 7 1906 and VDA 1906	All
1906	Session startup duration	DC 7 1906 and VDA 1903	All
1906	Desktop probing	DC 7 1906 and Citrix Probe Agent 1903	Premium
7.9 and later	Citrix Profile Management Duration in Profile Load	VDA 1903	All
1811	Profile Drilldown	DC 7 1811 and VDA 1811	All
1811	Hypervisor Alerts Monitoring	DC 7 1811	Premium
1811	Application probing	DC 7 1811 and Citrix Application Probe Agent 1811	Premium
1811	Microsoft RDS license health	DC 7 1811 and VDA 7.16	All
1811	Key RTOP Data display	DC 7 1811 and VDA 1808	Premium
1808	Export of Filters data	DC 7 1808	All
1808	Interactive Session drill down	DC 7 1808 and VDA 1808	All

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director Version	Feature	Dependencies - min version required	Edition
1808	GPO drill down	DC 7 1808 and VDA 1808	All
1808	Machine historical data available using OData API	DC 7 1808	All
7.18	Application probing	DC 7.18	Premium (formerly Platinum)
7.18	Smart alert policies	DC 7.18	Premium (formerly Platinum)
7.18	Health Assistant link	None	All
7.18	Interactive Session drill-down	None	All
7.17	PIV smart card authentication	None	All
7.16	Application Analytics	DC 7.16 and VDA 7.15	All
7.16	OData API V.4	DC 7.16	All
7.16	Shadow Linux VDA users	VDA 7.16	All
7.16	Domain local group support	None	All
7.16	Machine console access	DC 7.16	All
7.15	Application failure monitoring	DC 7.15 and VDA 7.15	All
7.14	Application-centric troubleshooting	DC 7.13 and VDA 7.13	All
7.14	Disk Monitoring	DC 7.14 and VDA 7.14	All
7.14	GPU Monitoring	DC 7.14 and VDA 7.14	All
7.13	Transport protocol on Session Details panel	DC 7.x and VDA 7.13	All

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director Version	Feature	Dependencies - min version required	Edition
7.12	User-friendly Connection and Machine failure descriptions	DC 7.12 and VDA 7.x	All
7.12	Increased historical data availability in Enterprise edition	DC 7.12 and VDA 7.x	Enterprise
7.12	Custom Reporting	DC 7.12 and VDA 7.x	Premium (formerly Platinum)
7.11	Resource utilization reporting	DC 7.11 and VDA 7.11	All
7.11	Alerting extended for CPU, memory and ICA RTT conditions	DC 7.11 and VDA 7.11	Premium (formerly Platinum)
7.11	Export report improvements	DC 7.11 and VDA 7.x	All
7.11	Integration with Citrix ADM	DC 7.11, VDA 7.x, and MAS version 11.1 Build 49.16	Premium (formerly Platinum)
7.9	Logon Duration breakdown	DC 7.9 and VDA 7.x	All
7.7	Proactive monitoring and alerting	DC 7.7 and VDA 7.x	Premium (formerly Platinum)
7.7	Windows Authentication Integration	DC 7.x and VDA 7.x	All
7.7	Single-session and Multi-session OS Usage	DC 7.7 and VDA 7.x	Premium (formerly Platinum)
7.6.300	Support for Framehawk virtual channel	DC 7.6 and VDA 7.6	All
7.6.200	Session recording integration	DC 7.6 and VDA 7.x	Premium (formerly Platinum)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director Version	Feature	Dependencies - min version required	Edition
7	HDX Insight integration	DC 7.6, VDA 7.x, and Citrix ADM	Premium (formerly Platinum)

Data granularity and retention

September 6, 2025

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.

Concurrent data evaluation

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 of time. These metrics are aggregated into the summary table for complete intervals. There are 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 do not have any data. Although raw data might exist for those partial intervals, it is never summarized. You can determine the earliest and latest aggregate interval for a particular data granularity by pulling the min and max SummaryDate from a particular summary table. 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 consider that there are 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.
- **Connection High Availability.** During connection high availability, there will be gaps in the summary data counts of current connections, but the session instances will still be 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Granularity and retention

The granularity of aggregated data retrieved by Director is a function of the time (T) span requested. The rules are as follows:

- 0 < T <= 1 hour - uses per-minute granularity
- 0 < T <= 30 days - uses per-hour granularity
- T > 31 days - uses 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. Grooming ensures better performance while maintaining the granularity required for reporting. Customers on Premium licensed sites can change the grooming retention to their desired number of retention days, otherwise the default is used. In case there was a connectivity loss with the Site database, Monitor Service will use the default retention days for Premium entitlement as specified in the table below.

To access the settings, run the following PowerShell commands on the Delivery Controller™:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
```

#	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.Connection tables	This setting impacts session details, Logon Duration by User Session, Application Based Usage tables on the Trends page.	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
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLog and MonitorData.ConnectionFailureLog	Trends page: This setting impacts the Failure Log 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.Hypervisor entities that have a LifecycleState of ‘Deleted’. This setting also deletes any related Session, SessionDetail, Summary, Failure, or LoadIndex records.	Machine, Catalog, DesktopGroup, and Hypervisor entities that have a LifecycleState of ‘Deleted’. This setting also deletes any related Session, SessionDetail, Summary, Failure, or LoadIndex records.	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
5	GroomSummariesRetentionDays	Monitor-Data.DesktopGroupSummary, Monitor-Data.FailureLogSummary, and Monitor-Data.LoadIndexSummary	This setting impacts all summary data on the Trends page.	365	31
6	GroomMachineHotfixLogRetentionDays	Monitor-Data.HotfixLog	This setting impacts the VDA hotfix data shown on the Machine Details page.	90	31
7	GroomMinuteRetentionDays	All Summary tables	This setting impacts the charts for the “Last 2 Hours” Time Period shown on the Trends page.	3	3
8	GroomHourlyRetentionDays	all Summary tables	This impacts the weekly graphs shown on the Trends page.	32	31
9	GroomApplicationInstanceRetentionDays	Monitor-Data.ApplicationInstance	This setting impacts the chart and tables on the Capacity management tab and application usage tables on the Trends page.	90	Not applicable

© 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
10	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	This setting impacts the Alerts shown on Monitor.	90	Not applicable
11	GroomResourceUsageRawDataRetentionDays	MonitorData.ResourceUtilization	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”.	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
12	GroomResourceUsageMinuteDataRetentionDays	MonitorDataDetailed	This setting impacts CPU and Memory charts for the “Last 2 Hours” Time Period seen in “Historical Machine Utilization” Machine Details page and the data calculation on Cost optimization area “Workload rightsizing tab”.	7	7

© 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
13	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
14	GroomResourceUsageDayDataRetentionDays	MonitorData.ResourceUtilizationSummary	This setting impacts the CPU and Memory chart seen on Machine “Resource utilization”on Trends page and “Machine utilization” page for specific machine.	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
15	GroomProcessUsageRawData	MonitorData	This setting impacts the resource trend per process information shown on machine historical usage page.	1	1
16	GroomProcessUsageMinuteData	MonitorData	This setting impacts the CPU and Memory usage per process charts for the “Last 2 Hours”shown on the Historical Machine Utilization page.	3	3
17	GroomProcessUsageHourData	MonitorData	This setting impacts the CPU and Memory usage trend per process shown on the machine historical usage page.	7	7

© 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
18	GroomProcessUsageDayData.RetentionDaysSummary	MonitorData.ProcessUsageDaysSummary	This setting impacts the CPU and Memory usage trend per process shown on the machine historical usage page.	30	30
19	GroomSessionMetricsDataRetentionDaysSummary	MonitorData.SessionMetricsDaysSummary	This setting impacts all the charts seen on the “Session Performance” tab of the user details page.	1	1
20	GroomMachineMetricsDataRetentionDaysSummary	MonitorData.MachineMetricsDaysSummary	This setting impacts the chart and table on the “Resource Utilization” tab on the Trends page.	3	3
21	GroomMachineMetricsDataRetentionDaysSummary	MonitorData.MachineMetricsDaysSummary	This setting impacts the chart and table on the “Resource Utilization” tab on the Trends page.	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
22	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationErr	Daily error impacts error details shown in the "Application Errors" column on the Applications page.	1	1
23	GroomApplicationFaultsRetentionDays	MonitorData.ApplicationFau	Daily failure impacts the "Application Faults" column on the Applications page.	1	1

> **Caution:**
>
> Modifying values on the Monitor Service database requires restarting the service for the new values to take effect. You are advised to make changes to the Monitor Service database only under the direction of Citrix Support.

The settings GroomProcessUsageRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays, and GroomSessionMetricsDataRetentionDays are limited to their default values of 1, while GroomProcessUsageMinuteDataRetentionDays is limited to its default value of 3. The PowerShell commands to set these values have been disabled, as the process usage data tends to grow quickly. Also, license based retention settings are as follows:

- **Premium licensed sites -** the grooming retention for all settings is limited to 1000 days (Citrix recommends 365 days).
- **Advanced licensed sites -** the grooming retention for all settings is limited to 31 days.
- **All other sites -** the grooming retention for all settings is limited to 7 days.

Exceptions:

- GroomApplicationInstanceRetentionDays can be set only in Premium licensed sites.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- GroomApplicationErrorsRetentionDays and GroomApplicationFaultsRetentionDays are limited to 31 days in Premium licensed sites.

Retaining data for long periods have 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. Given that the dashboard data is drawn from this table, the requirements on the database server might be large. Excessively large amounts of data might have a dramatic impact on performance.

- **Session and event data.** Data 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.

Citrix Director failure reasons and troubleshooting

September 13, 2025

The following tables describe the various failure categories, the reasons, and the action you need to take to resolve the issues. For more information, see Enums, error codes, and descriptions.

Connection failure errors

Category	Reason	Issue	Action
N/A	[0] Unknown. This error code is not mapped.	The Monitoring service cannot determine the reason for the reported launch or connection failure from information shared by the Brokering service.	Collect CDF logs on the controller and contact Citrix support.
[0] None	[1] None	None	N/A

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[2] MachineFailure	[2] SessionPreparation	Session preparation request from the delivery controller to the VDA failed. Possible causes: Communication issues between the controller and the VDA, issues experienced by the Broker Service while creating a prepare request, or network issues resulting in the VDA not accepting the request.	Refer to troubleshooting steps listed in Knowledge center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops for common problems that cause communication issues between the controller and the VDA.
[2] MachineFailure	[3] RegistrationTimeout	The VDA was powered on, but a time-out occurred while it was attempting to register with the delivery controller.	Verify that the Citrix Broker Service is running on the delivery controller and that the Desktop service is running on the VDA. Start each if stopped.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[1] ClientConnection-Failure	[4] ConnectionTimeout	The client did not connect to the VDA after the VDA was prepared for session launch. The session was successfully brokered, but a time-out occurred while waiting for the client to connect to the VDA. Possible causes: Firewall settings, network interruptions, or settings that prevent remote connections.	Check the Director console to see if the client currently has an active connection, which means no user is impacted. If no session exists, review the event logs on the client and on the VDA for any errors. Resolve any issues with network connectivity between the client and the VDA.
[4] NoLicensesAvailable	[5] Licensing	The licensing request failed. Possible causes: Insufficient number of licenses, or the license server has been down for more than 30 days.	Verify that the license server is online and reachable. Resolve any network connectivity issues to the license server or reboot the license server if it appears to be malfunctioning. Verify that there are sufficient licenses in the environment and allocate more if necessary.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[1] ClientConnection-Failure	[6] Ticketing	A failure occurred during ticketing, indicating that the client connection to the VDA does not match the brokered request. A launch request ticket is prepared by the Broker and delivered in the ICA® file. When the user attempts to launch a session, the VDA validates the launch ticket in the ICA file with the Broker. Possible causes: ICA file is corrupt or the user is attempting to make an unauthorized connection.	Verify that the user has access to the application or desktop based on user groups defined in the delivery groups. Instruct the user to relaunch the application or desktop to determine whether this is a one off issue. If the issue occurs again, review the client device event logs for errors. Verify that the VDA to which the user is attempting to connect is registered. If unregistered, review the event logs on the VDA and resolve any registration issues.
[1] ClientConnection-Failure	[7] Other	A session has been reported as terminated from the VDA after the client has initially contacted the VDA but before it completed the connection sequence.	Verify if the session was not terminated by the user before launch. Try relaunching the session, if the problem persists, collect CDF logs and contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[1] ClientConnection-Failure	[8] GeneralFail	The session failed to launch. Possible causes: A brokered launch was requested while the broker was still starting up or initializing, or internal error during the brokering phase of a launch.	Verify that the Citrix Broker Service is running and retry launching the session.
[5] Configuration	[9] MaintenanceMode	The VDA, or the delivery group to which the VDA belongs, is set in maintenance mode.	Determine whether maintenance mode is required. Disable maintenance mode on the delivery group or machine in question if it is not needed and instruct the user to attempt to reconnect.
[5] Configuration	[10] ApplicationDisabled	The application cannot be accessed by end users because it has been disabled by the administrator.	If the application is intended to be available for production use, enable the application and instruct the user to reconnect.
[4] NoLicensesAvailable	[11] LicenseFeature Refused	The feature being used is not covered by the existing licenses.	Contact a Citrix sales representative to confirm the features that are covered by the existing Citrix Virtual Apps and Desktops™ license edition and type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[3] NoCapacityAvailable	[13] SessionLimitReached	All VDAs are in use and there is no capacity to host more sessions. Possible causes: All VDAs are in use (for single-session OS VDAs), or all VDAs have reached the configured maximum concurrent sessions allowed (for multi-session OS VDAs).	Verify if there are any VDAs in maintenance mode. Disable maintenance mode if it is not needed to free up more capacity. Consider increasing the value of **Maximum Number of Sessions** in the Citrix policy setting to allow more sessions per server VDA. Consider adding more multi-session OS VDAs. Consider adding more single-session OS VDAs.
[5] Configuration	[14] DisallowedProtocol	The ICA and RDP protocols are not allowed.	Run the **Get-BrokerAccessPolicyRule** PowerShell command on the delivery controller and verify that the **AllowedProtocols** value has all the desired protocols listed. This issue occurs only if there is a misconfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[5] Configuration	[15] ResourceUnavailable	The application or desktop to which the user is attempting to connect is not available. This application or desktop might not exist, or there are no VDAs available to run it. Possible causes: The application or desktop has been unpublished, or the VDAs hosting the application or desktop have reached maximum load, or the application or desktop is set in maintenance mode.	Verify that the application or desktop is still published and the VDAs are not in maintenance mode. Determine whether the multi-session OS VDAs are at full load. If so, provision more multi-session OS VDAs. Verify that there are single-session OS VDAs available for connections. Provision more single-session OS VDAs if necessary.
[5] Configuration	[16] ActiveSessionReconnectDisabled	The ICA session is active and connected to a different endpoint. However, because the **Active Session Reconnection** is disabled, the client cannot connect to the active session.	On the delivery controller, verify that **Active Session Reconnection** is enabled. Verify that the value of **DisableActiveSessionReconnect** in the registry, under **HKEY_LOCAL_MACHINE\Software** is set to 0.
[2] MachineFailure	[17] NoSessionToReconnect	The client attempted to reconnect to a specific session but the session was terminated.	Retry the workspace control reconnection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[2] MachineFailure	[18] SpinUpFailed	The VDA cannot be powered on for session launch. This is a hypervisor reported issue.	If the machine is still powered off, attempt to start the machine from Citrix Studio. If this fails, review the hypervisor connectivity and permissions. If the VDA is a PVS-provisioned machine, verify in the PVS console that the machine is running. If not, verify that the machine is assigned a Personal vDisk, log in to the hypervisor to reset the VM.
[2] MachineFailure	[19] Refused	The delivery controller sends a request to the VDA to prepare for a connection from an end user, but the VDA actively refuses this request.	Verify via ping, that the delivery controller and the VDA can successfully communicate. If not, resolve any firewall or network routing issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[2] MachineFailure	[20] ConfigurationSet Failure	The delivery controller did not send required configuration data, such as policy settings and session information, to the VDA during session launch. Possible causes: Communication issues between the controller and the VDA, issues experienced by the Broker Service while creating a configuration set request, or network issues resulting in the VDA not accepting the request.	-
[3] NoCapacityAvailable	[21] MaxTotalInstance-sExceeded	The maximum number of instances of an application has been reached. No additional instances of the application can be opened on the VDA. This issue is related to the application limits feature.	Consider increasing the application setting, **Limit the number of instances running at the same time** to a higher value if licensing permits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	The user is attempting to open more than one instance of an application but the application is configured to allow only a single instance of the application per user. This issue is related to the application limits feature.	Only one instance of the application is allowed per user by default. If multiple instances per user are required, consider clearing the **Limit to one instance per user** setting in the application setting.
[1] ClientConnectionFailure	[23] Communication error	The delivery controller attempted to send information to the VDA, such as a request to prepare for a connection, but an error occurred during the communication attempt. This can be caused due to network disruptions.	If already started, restart the Desktop service on the VDA to restart the registration process and verify that the VDA registers successfully. Confirm that the delivery controllers configured for the VDA are accurate via the details in the application event log.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Reason	Issue	Action
[3] NoCapacityAvailable	[100] NoMachineAvailable Monitoring service converts [12] NoDesktopAvailable to this error code.	The VDA assigned to launch the session is in an invalid state or is unavailable. Possible causes: Power state of the VDA is unknown or unavailable, the VDA did not reboot since the last user's session, session sharing is disabled while the current session requires it to be enabled, or the VDA was removed from the delivery group or from the site.	Verify that the VDA is in a delivery group. If not, add it to the appropriate delivery group. Verify that there are sufficient VDAs registered and in ready state to be able to launch the published shared desktop or application requested by the user. Verify that the hypervisor hosting the VDA is not in maintenance mode.
[2] MachineFailure	[101] MachineNotFunctional. Monitoring service converts [12] NoDesktopAvailable to this error code.	The VDA is not operational. Possible causes: The VDA was removed from the delivery group, the VDA is unregistered, the VDA power state is unavailable, or the VDA is experiencing internal issues.	Verify that the VDA is in a delivery group. If not, add it to the appropriate delivery group. Verify that the VDA shows as powered on in Citrix Studio. If the power state is unknown for several machines, resolve any issues with connectivity to the hypervisor or host failures. Verify that the hypervisor hosting the VDA is not in maintenance mode. Restart the VDA once these issues have been addressed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Machine failure type

Error Code	Error Code ID	Issue	Action
Unknown	-	-	-
Unregistered	3	-	-
MaxCapacity (represented as Max Load on Director)	4	Machine is reporting itself at maximum capacity i.e. Max Load Index	Ensure that all hypervisors are powered on. Add more machines to the affected Delivery Groups by adding more capacity to the hypervisor or by adding more hypervisors.
StuckOnBoot	2	The VM did not complete its boot sequence and is not communicating with the hypervisor.	Ensure that the VM booted successfully on the hypervisor. Check for other messages on the VM, such as OS issues. Ensure that the hypervisor tools are installed on the VM. Ensure that the VDA is installed on the VM.
FailedToStart	1	The VM experienced issues when trying to start on the hypervisor.	Check the hypervisor logs.
None	0	-	-

Machine deregistration reason (applicable when failure type is Unregistered or Unknown)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
AgentShutdown	0	The VDA experienced a graceful shutdown.	Power on the VDA if you do not expect it to be off based on existing power management policies. Review any errors in the event logs.
AgentSuspended	1	The VDA is in hibernation or sleep mode.	Take the VDA out of hibernation mode. Consider disabling hibernation for Citrix Virtual Apps and Desktops VDAs via power settings.
IncompatibleVersion	100	The VDA cannot communicate with the delivery controller due to a mismatch in the Citrix protocol versions.	Align the VDA and delivery controller versions.
AgentAddressResolutionFailed	101	The delivery controller was not able to resolve the VDA's IP address.	Verify that the VDA machine account exists in AD. If not, create it. Verify that the name and the IP address of the VDA in DNS are accurate. If not, correct them. If widespread, validate the DNS settings on the delivery controllers. Verify DNS resolution from the controller by running the `nslookup` command.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
	101	The delivery controller was not able to resolve the VDA's IP address.	Verify that the VDA machine account exists in AD. If not, create it. Verify that the name and the IP address of the VDA in DNS are accurate. If not, correct them.
AgentNotContactable	102	A communication issue occurred between the delivery controller and the VDA.	Use a ping to verify that the delivery controller and the VDA can successfully communicate. If not, resolve any firewall or network issues. Refer to the troubleshooting steps listed in Knowledge Center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), for common problems that cause communication issues between the controller and the VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
	102	A communication issue occurred between the delivery controller and the VDA.	Refer to troubleshooting steps listed in Knowledge Center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), for common problems that cause communication issues between the controller and the VDA. Contact Citrix support.
AgentWrongActiveDirectoryOU	103	An Active Directory discovery misconfiguration occurred. The site-specific OU (where the site controller info is stored in AD) configured in the VDA registry is for a different Site.	Ensure the active directory configuration is correct, or check registry settings.
EmptyRegistrationRequest	104	The registration request sent from the VDA to the delivery controller was empty. This can be due to a corrupt VDA software installation.	Restart the Desktop service on the VDA to restart the registration process and verify that the VDA registers correctly via the application event log.
MissingRegistrationCapabilities	105	The VDA version is not compatible with the delivery controller.	Upgrade the VDA or remove the VDA and then reinstall it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
MissingAgentVersion	106	The VDA version is not compatible with the delivery controller.	Reinstall the VDA software if the issue is impacting all machines.
InconsistentRegistrationCapabilities	107	The VDA cannot communicate its capabilities to the Broker. This can be due to incompatibility between the VDA and delivery controller versions. The registration capabilities, which change with each version, are expressed in a form that does not match the registration request.	Align the VDA and delivery controller versions.
NotLicensedForFeature	108	The feature you are attempting to use is not licensed.	Check your Citrix licensing edition, or remove the VDA and then reinstall it.
	108	The feature you are attempting to use is not licensed.	Contact Citrix support.
UnsupportedCredentialSecurityversion	109	The VDA and the delivery controller are not using the same encryption mechanism.	Align the VDA and delivery controller versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
InvalidRegistrationRequest	110	The VDA made a registration request to the Broker but the content of the request is corrupt or invalid.	Refer to the troubleshooting steps listed in Knowledge Center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), for common problems that cause communication issues between the controller and the VDA.
SingleMultiSessionMismatch	111	The VDA's operating system type is not compatible with the machine catalog or delivery group.	Add the VDA to the correct machine catalog type or delivery group containing machines with the same operating system.
FunctionalLevelTooLowForCatalog	112	The machine catalog is set to a higher VDA functional level than the installed VDA version.	Verify that the VDA's machine catalog functional level matches that of the VDA. Upgrade or downgrade the machine catalog to match that of the VDA.
FunctionalLevelTooLowForDesktopGroup	113	The delivery group is set to a higher VDA functional level than the installed VDA version.	Verify that the VDA's delivery group functional level matches that of the VDA. Upgrade or downgrade the machine catalog to match that of the VDA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
PowerOff	200	The VDA did not shut down gracefully.	If the VDA is supposed to be powered on, attempt to start the VDA from Citrix Studio and verify that it boots up and registers correctly. Troubleshoot any boot or registration issues. Review the event logs on the VDA once it is back up to help determine the root cause of the shutdown.
AgentRejectedSettingsUpdate	203	Settings such as Citrix policies were changed or updated but there was an error in sending the updates to the VDA. This can occur if the updates are incompatible with the installed VDA version.	Upgrade the VDA if necessary. Review whether the updates that were applied are supported with the VDA version.
SessionPrepareFailure	206	The Broker did not complete an audit of the sessions that are running on the VDA.	If widespread, restart the Citrix Broker Service on the delivery controller.
	206	The Broker did not complete an audit of the sessions that are running on the VDA.	Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
ContactLost	207	The delivery controller lost connection with the VDA. This can be caused by network disruptions.	Verify that the Citrix Broker Service is running on the delivery controller and the Desktop service is running on the VDA. Start each if stopped. If already started, restart the Desktop service on the VDA to restart the registration process and verify that the VDA registers successfully. Confirm that the delivery controllers configured for the VDA are accurate via the details in the Application event log. Use a ping to verify that the delivery controller and the VDA can successfully communicate. If not, resolve any firewall or network issues.
	207	The delivery controller lost connection with the VDA. This can be caused by network disruptions.	Verify that the Desktop service is running on the VDA. Start if stopped.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
BrokerRegistrationLimitReached	201	The delivery controller has reached the configured maximum number of VDAs that are allowed to concurrently register with it. By default, the delivery controller allows 10,000 concurrent VDA registrations.	Consider adding delivery controllers to the Site or creating a Site. You can also increase the number of VDAs allowed to concurrently register with the delivery controller via the **HKEY_LOCAL_MACHINE\Software** registry key. See Knowledge Center article, Registry Key Entries Used by Citrix Virtual Apps and Desktops (CTX117446) for more information. Increasing this number might require more CPU and memory resources for the controller.
SettingsCreationFailure	208	The Broker did not construct a set of settings and configurations to send to the VDA. If the Broker is unable to gather the data, registration fails and the VDA becomes unregistered.	Check the event logs on the delivery controller for any errors. Restart the Broker Service if a specific issue is not evident in the logs. Once the Broker Service is restarted, restart the Desktop service on the affected VDAs and verify that they successfully register.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
	208	The Broker did not construct a set of settings and configurations to send to the VDA. If the Broker is unable to gather the data, registration fails and the VDA becomes unregistered.	Restart the Desktop service on the affected VDAs and verify that they successfully register. Contact Citrix support.
SendSettingsFailure	204	The Broker did not send settings and configuration data to the VDA. If the Broker can gather the data but is unable to send it, registration fails.	If limited to a single VDA, restart the Desktop service on the VDA to force reregistration and validate that the VDA registers successfully via the application event log. Troubleshoot any errors seen. Refer to the troubleshooting steps listed in Knowledge center article, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), for common problems that cause communication issues between the controller and the VDA.
AgentRequested	2	An unknown error occurred.	Contact Citrix support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Error Code ID	Issue	Action
DesktopRestart	201	An unknown error occurred.	Contact Citrix support.
DesktopRemoved	202	An unknown error occurred.	Contact Citrix support.
SessionAuditFailure	205	An unknown error occurred.	Contact Citrix support.
UnknownError	300	An unknown error occurred.	Contact Citrix support.
RegistrationStateMismatch	302	An unknown error occurred.	Contact Citrix support.
Unknown	-	An unknown error occurred.	Contact Citrix support.

Secure Private Access integration with Director (Preview)

September 6, 2025

The Secure Private Access integration with Director allows help desk admin or full admin to monitor and troubleshoot all Secure Private Access sessions in Director. To support this feature, you must use the 2402 or later versions of Director, Secure Private Access, Citrix Workspace™ app, and VDA.

Available actions include viewing the details of the following:

- Secure Private Access active sessions for a user under the **Select a Session** popup > **Sessions** tab > **Web SaaS and Client/Server Apps**
- 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
- Session and application details view for failed and blocked enumerations

> **Note:**
>
> The Secure Private Access integration with Director is only supported for Director Forms-based authentication and not supported for Integrated Windows Authentication or Smart Card-based authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

1. To support this feature, you must use the following:
    - Director 2402 or later version
    - Secure Private Access 2402 or later version
    - Citrix Workspace app 2402 or later version
2. Ensure that at least one Citrix Virtual Apps and Desktops™ site is configured on Director.
3. Set up Secure Private Access.
4. Make sure that the Director server has network connectivity to the Secure Private Access server.

    > **Note:**
    >
    > A trusted certificate must be installed on the Secure Private Access server to successfully establish a connection to Citrix Director.

5. Ensure that the Director admin user has the following permissions:
    a) Secure Private Access Full Admin or ReadOnly Admin in the Secure Private Access Admin console.
    b) Citrix Virtual Apps™ or Desktops help desk or Full Admin or ReadOnly Admin in the Citrix Studio console.

Configure Director with Secure Private Access

1. Open a command prompt as admin on the machine where Director is installed.
2. Go to the path of the `DirectorConfig` tool by running the following command:

    ```
    cd c:\inetpub\wwwroot\Director\tools
    ```

3. Run the following command to configure Secure Private Access:

    ```
    DirectorConfig.exe /configspa
    ```

4. Enter the FQDN of the machine where Secure Private Access is installed along with the port number.
5. Make sure that the connection to the Secure Private Access (server or load balancer) is secure and has a trusted certificate applied to it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
PS C:\inetpub\wwwroot\Director\tools> .\DirectorConfig.exe /configspa

 Make sure the SPA server or load balancer is reachable from this Director machine
 Enter SPA server or load balancer FQDN including port [https://spa-server.mydomain.com:4[redacted]3] : https://[redacted]

 Checking connectivity to https://spa1.gwonprem.corp[redacted]

 Spa Server or load balancer: https://s[redacted] is reachable.

 Checking Spa Server or load balancer is valid

 Retry with correct Spa Server FQDN which is reachable

 Director configuration encountered an error

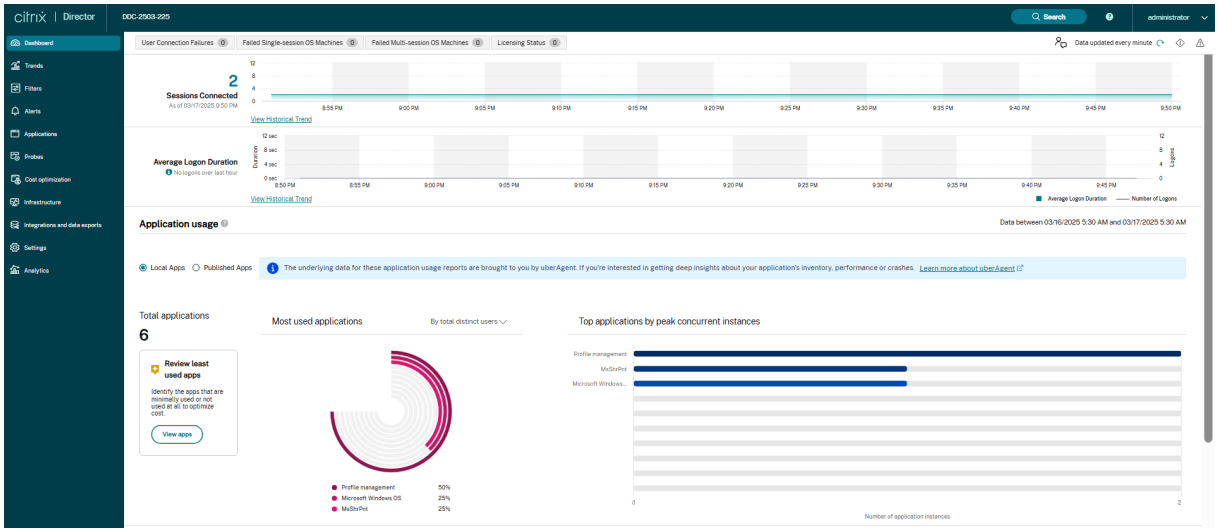

=====================================================
Spa Server or load balancer FQDN https://[redacted] is either invalid or Spa server/load balancer is down
=====================================================
```

> **Note:**
>
> The admins must be added to the Secure Private Access console to view the Secure Private Access session details in Director. For more information, see Manage administrators.

View a Secure Private Access session by user

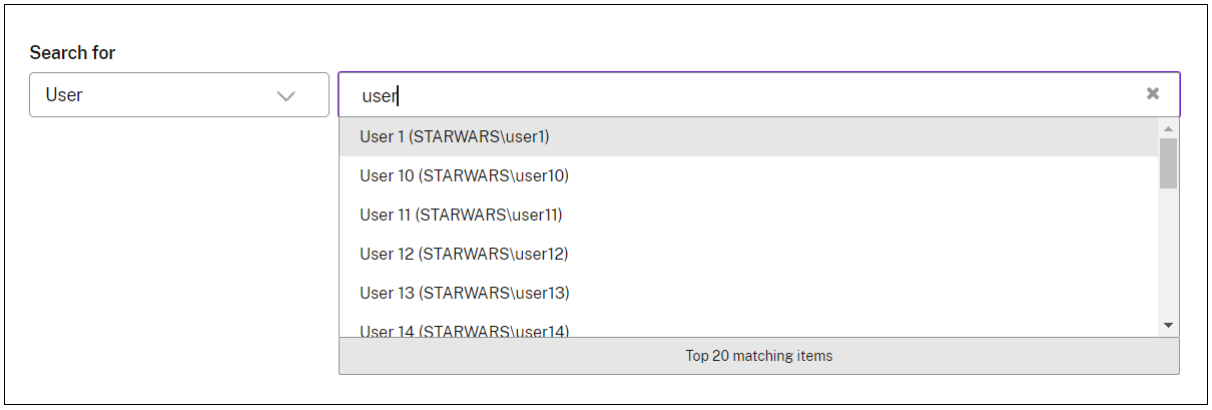
On the Director dashboard, click **Search** and enter the user name. The **Select a session** screen appears.

Full admin:



Help desk admin:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View the Activity Manager for Secure Private Access session

Citrix Director 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. This feature is available from Citrix Virtual Apps and Desktops version 2407 or later.

Prerequisites:

- Director 2407 or later version
- Secure Private Access 2407 or later version

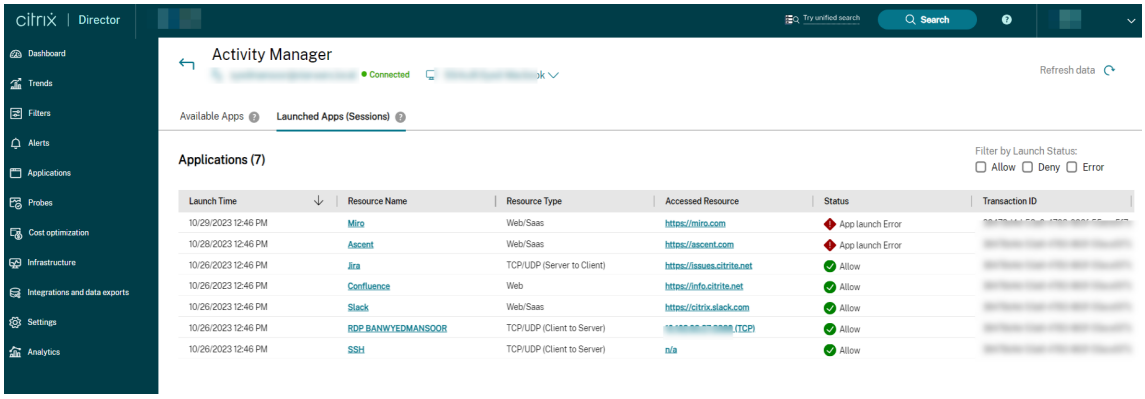
The Activity Manager is displayed with the **Available Apps** and **Launched Apps** details. You can find the following session details:

- Launch time
- Resource name
- Resource type
- Accessed resource
- Status
- Transaction ID

To view the Activity Manager, do the following:

1. On the Director dashboard, click **Search** and enter the user name. The **Select a session** screen appears.
2. Select a session that is opened using the Secure Private Access session. The Activity Manager for the selected session appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 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 filter the resources with the status of the resource set in the Secure Private Access app:

- Allow - Resources that are allowed for a user to access. This status is set using a policy under the Secure Private Access app. This resource is present for the user in the Citrix Workspace app.
- Deny - Resources that are denied for a user to access. This status is set using a policy under the Secure Private Access app. This resource is present for the user in the Citrix Workspace app.
- Error - Resources that are allowed to access for a user under the Secure Private Access app. However, because of some error, the resource isn't available in the Citrix Workspace app. There are two types of errors such as enumeration error and session error.

View available apps

The Web and SaaS apps that are available in the Citrix Workspace app are displayed under the **Available Apps** section. This section shows the last enumeration attempt of the apps and the status of the enumeration attempt.

You can view the following details:

- Resource name
- Status
- Transaction ID

You can also filter the preceding details with the application status such as **Allow**, **Deny**, and **Error**. You also sort the details using the up and down arrow.

> **Note:**
>
> TCP/UDP apps aren't present in the **Available Apps** section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View launched apps

The apps that are opened in the Citrix Workspace app are displayed under the **Launched Apps (sessions)** section. You can view the following details:

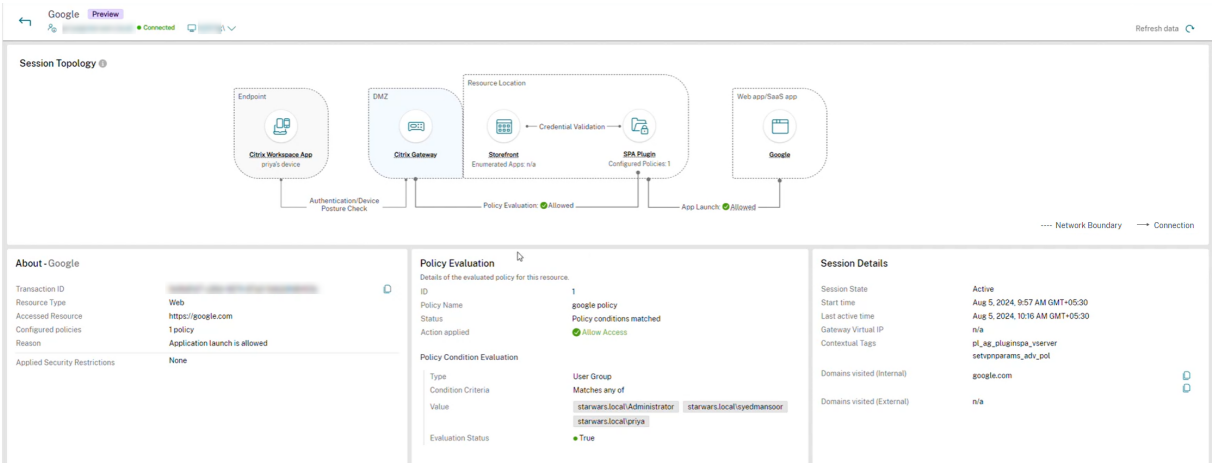
- Launch time
- Resource name
- Resource type
- Accessed resource
- Status
- Transaction ID

You can also filter the preceding details with the application status such as **Allow**, **Deny**, and **Error**. You can also sort the details using the up and down arrow.

Session topology view for Secure Private Access apps

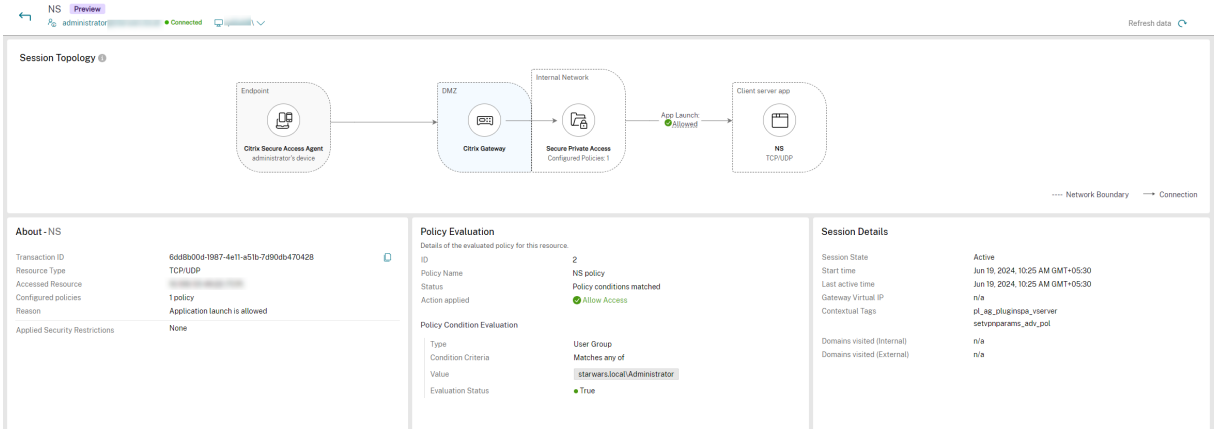
You can view the session topology for the apps opened using Secure Private Access. Click the required app from the **Activity Manager** to view the Session Topology of the selected app.

Web/SaaS apps:



TCP/UDP apps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Session Topology view provides the flow of the app launch process. 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. This feature is available from Citrix Virtual Apps and Desktops version 2407 or later.

Prerequisites:

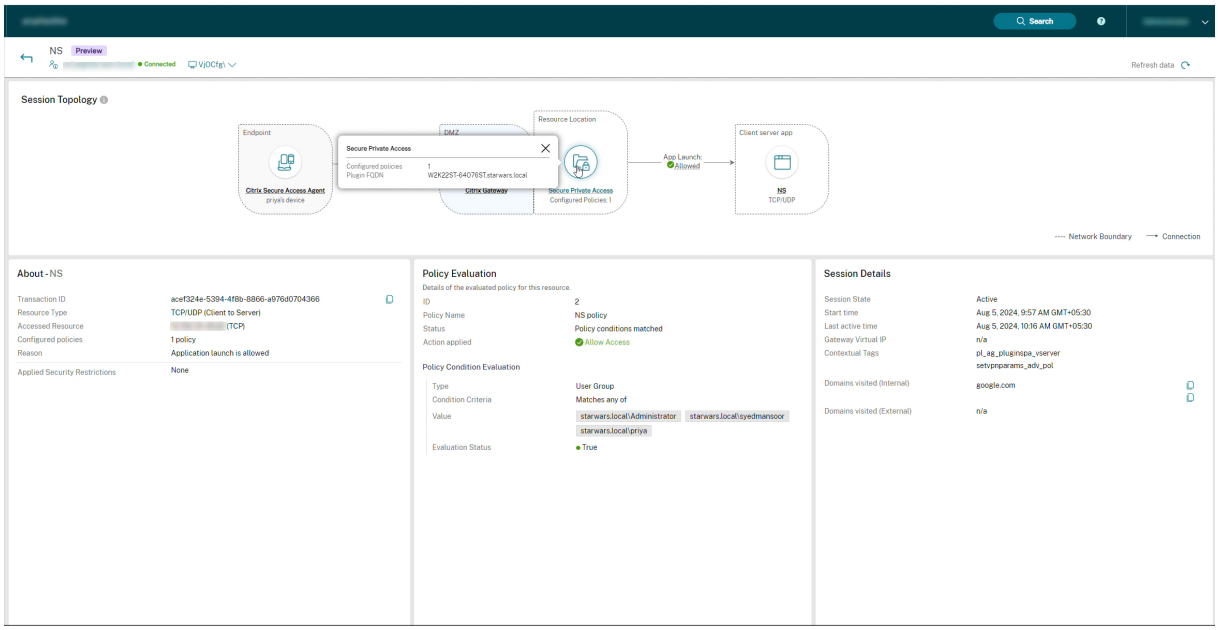
- Director 2407 or later version
- Secure Private Access 2407 or later version
- Citrix Secure Access 24.8.1.x or later version

You can view the following:

- 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.
- Internal network - 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 different values are **Allowed**, **Denied**, **Access allowed with restrictions**, and **Error**. This is applicable only for Web or SaaS apps.
- App launched - Displays the type of apps and the status of app launch. The possible values for app types are Web/SaaS app or TCP/UDP app. Similarly, the possible values for app launch statuses are **Allowed**, **Denied**, **Access allowed with restrictions**, and **Error**.

You can now view the following extra details in the **Session Topology** view for Secure Private Access apps. This change applies to both Web and SaaS apps, in addition to TCP/UDP apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Endpoint:

Click the link within **Endpoint** to view the following:

- **Endpoint type:** This can be either the Secure Access Agent or Citrix Workspace app.
- **Access details:** View how the endpoint is accessed, whether through StoreFront™ or Citrix Workspace app.
- **Endpoint OS:** For example, Windows.
- **Location type:** Indicates whether the location is internal or external.

Resource Location:

Click the link within **Resource Location** to view the following:

> **Note:** This is applicable only for Web and SaaS apps.

- **Number of enumerated applications:** Displays the number of enumerated applications and the store URL.
- **Access method:** Indicates whether the endpoint is accessed through StoreFront or Citrix Workspace app.

Secure Private Access:

- **Configured policies:** Displays the number of configured policies.
- **FQDN plug-in:** Shows the FQDN of the agent that served the request.

Web and SaaS App / Client-Server App (TCP/UDP):

Click the link within **Web and SaaS App / Client-Server App** to view the following:

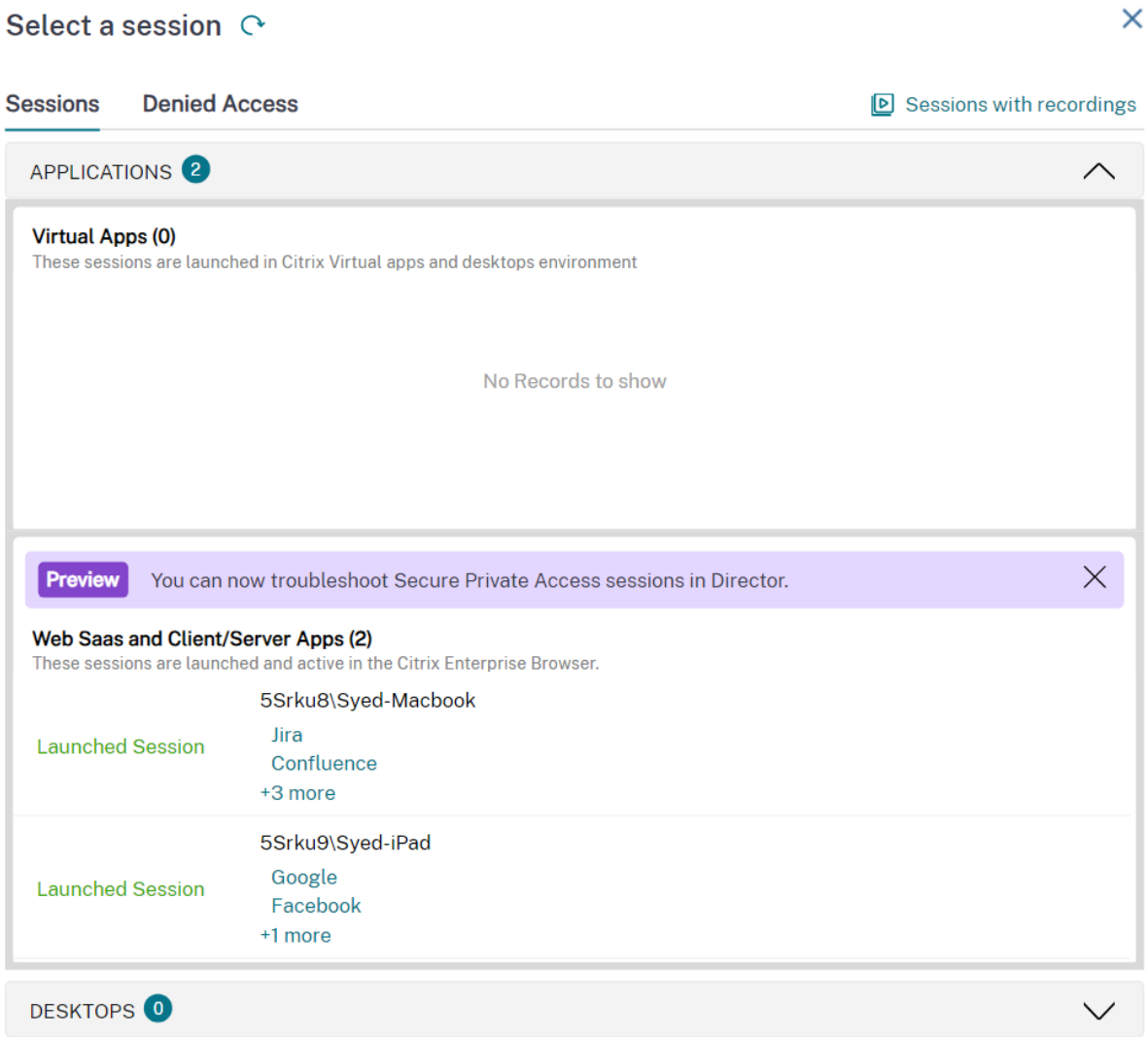
- **App name:** The name of the app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Top level URL:** For Web or SaaS apps, the URL of the published app is displayed. For TCP/UDP apps, the protocol IP address of the app is displayed.
- **App type:** Indicates whether the app is a Web or SaaS app, or a TCP/UDP app.
- **App publishing type:** Indicates whether the app is published externally or internally.

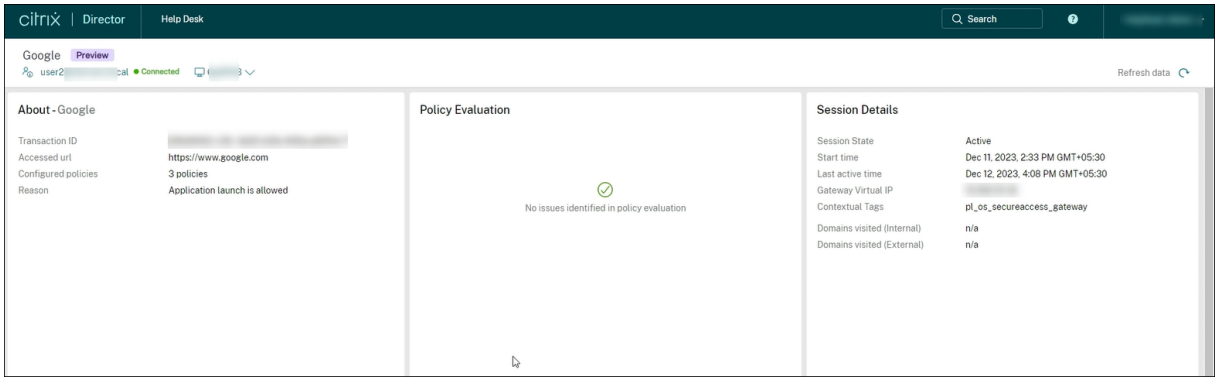
View successfully launched Web apps and SaaS apps

The successfully launched apps are displayed on the **Web SaaS and Client/Server Apps** section.



Click an app from the **Web SaaS and Client/Server Apps** section to view the details.

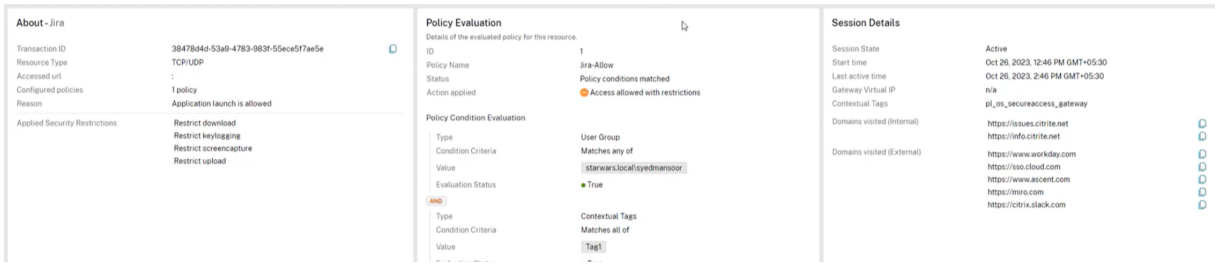
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information on success codes, see Citrix Director related codes.

View details about the access denied apps

Click **Check Access Details** on the **Select a session** screen.



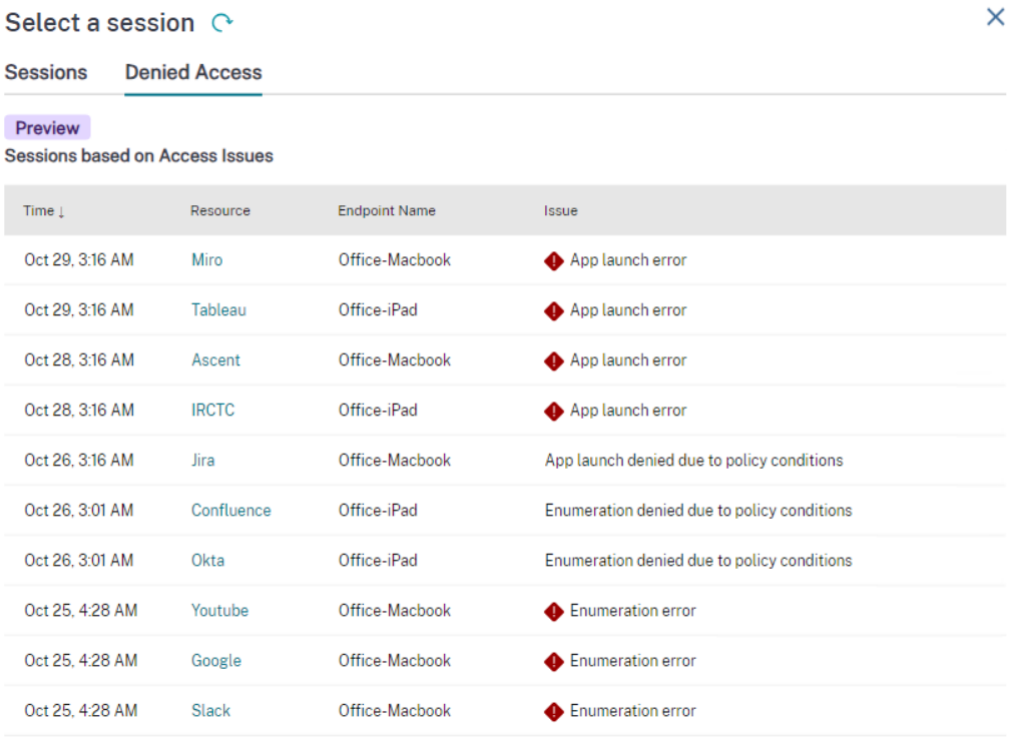
> **Note:**
>
> The **Check Access Details** button appears when there is no active session.

Or,

Click the **Denied Access** tab to view the apps for which the access is denied.

The **Denied Access** tab opens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

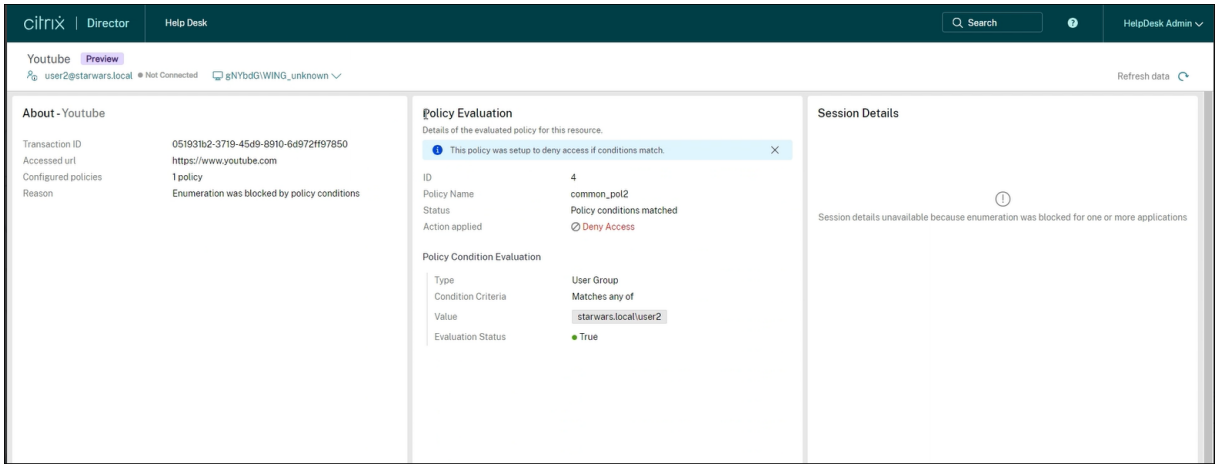


The session details such as time, resource, endpoint name, and reason for failure are displayed. For more information on error codes, see Citrix Director related codes.

Currently, the following issues are identified:

- Enumeration denied due to policy conditions
- App launch error
- Enumeration errors
- App launch denied due to policy conditions

Select an app from the **Denied Access** tab > **Resource** column to view the details:



The following details are displayed for the successful or failed sessions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- About the app
- Policy evaluation
- Session details

About the app

The name of the successful, failed, or denied app is displayed. Along with it, the following details of the app for the success or failure are displayed:

Field	Description
Transaction ID	Citrix Transaction ID 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 Resource	The URL of the accessed resource during the session or enumeration. In the case of a TCP or UDP app, it shows whether the type of accessed resource is TCP or UDP.
Configured policies	The number of policies that are used within a session or enumeration.
Reason	The analysis of the session or enumeration activity.
Applied Security Restrictions	Displays the applied security restrictions which are applied in the Secure Private Access app.

Policy evaluation

Displays that no issues found during evaluation for a successful session. For a failed session or enumeration, the following details of the policies evaluated are displayed:

Field	Description
ID	Citrix Transaction ID.
Policy Name	The name of the policy. If there are multiple policies, the first policy that is matched with the set condition appears.
Status	The status of the policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description
Action applied	The action applied on the policy. For example, deny access.
Policy Condition Evaluation	
Type	The type of the policy condition.
Condition Criteria	The condition criteria of the policy applied in the failed session or enumeration.
Value	The value of the policy.
Evaluation Status	The evaluation status of the policy. The different values are **Allowed**, **Denied**, **Access allowed with restrictions**, and **Error**.

Session details

For a failed session, the reason for session failure is displayed. For a successful session, the following details are displayed:

Field	Description
Session State	Displays the state of the session whether it is active or inactive.
Start time	Displays the session start time.
Last active time	Displays the last active time of the successful session.
Gateway Virtual IP	Displays the virtual IP address of the gateway to which the successful session is connected.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix VDA Upgrade Service (VUS) - Tech Preview

August 21, 2025

Features in Technical Preview

Features in Technical 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 technical preview but welcomes feedback for improving them. Citrix might act on feedback based on its severity, criticality, and importance.

It isn't a commitment, promise, or legal obligation to deliver any material, code, or functionality and must not be relied upon in making Citrix product purchase decisions. The development, release, and timing of any features or functionality remain at our sole discretion and are subject to change without notice or consultation.

Citrix VDA Upgrade Service (VUS)

The Citrix VDA Upgrade Service (VUS) is a component of Citrix Virtual Apps and Desktops™ (CVAD) 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.

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 Web Studio, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pre-requisites for Upgrading VDAs Using VUS

August 21, 2025

To perform VDA upgrades using VUS, the following prerequisites must be met.

Enable the VDA Upgrade Service for your Site

To enable VUS for your 2503 Site, run the following PowerShell cmdlet:

```
Set-VusSite -Enabled $true
```

Once enabled, import the latest VDA versions to your CVAD Site by running the following PowerShell cmdlet:

```
Import-VusVdaReleasesMetadata -Path '[<CVAD-2503-ISO>\Support\VdaUpdateServiceM
\vda_releases.xml]'
```

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 Web Studio, 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`

> **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA Requirements

VDA Version

- For machines created using MCS:
  - 2311 or later
- For machines added using Websocket VDA Enrollment
  - 2311 or later
- For manually provisioned machines
  - 2411 or later

Provisioning Type

- Single or multi-session persistent machines provisioned using non-Citrix provisioning™ services or .
- Single-session MCS-provisioned persistent machines (AD joined, Azure AD joined, and non-domain-joined).
- Remote PC Access machines.

VDA Upgrade Agent

- The VDA Upgrade Agent version 7.44 or later 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

Permissions

You must have the Full Administrator or Machine Catalog Administrator role in CVAD.

VDA State

For upgrades scheduled through VUS to proceed as intended, the VDAs targeted for upgrade must meet the following prerequisites:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

  > **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 Delivery Controllers over HTTPS for VDA upgrades.
  - To verify that the VDA installer is signed by a valid certificate, VDAs must communicate with the following URLs.
    - http://crl3.digicert.com/*
    - http://crl4.digicert.com/*
    - http://ocsp.digicert.com/*
    - http://cacerts.digicert.com/*
- If VDAs do not have access to the internet, configure the VDAs to bypass the certificate revocation list (CRL).
  - Disable the "VDA upgrade certificate revocation list check"Citrix® policy setting, and assign it to the delivery group.
    - Policy description:
      - When enabled, the VDA Upgrade Agent performs certificate revocation list checks during component upgrades.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When disabled, the VDA Upgrade Agent skips these checks. Disable this setting for VDAs without access to the internet.

VDAs with Proxy configurations

- 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 Web Studio or the registry.
  - VDA Upgrade Agent proxy configuration using Web Studio.
    - 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`

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.

Monitoring and Troubleshooting

December 15, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

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.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA Upgrade (Studio)	VDA Upgrade (Powershell)	Description
Available	UpgradeAvailable	The VDA is not on the latest version of the upgrade track. An upgrade is recommended.
Up to date	UpToDate	The VDA is on the latest version of the upgrade track. No action is required.
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**.

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.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA Upgrade State (Studio)	VDA Upgrade State (PowerShell)	Description
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.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**
  - 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
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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**.

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:** `HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent\LogToFile`
- **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
\LogToFile -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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - The log file is created in C:\ProgramData\Citrix\Update Services\Logs folder

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 Connectivity.
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.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Introduction

December 4, 2025

Always On Tracing (AOT) is a modern diagnostic framework from Citrix designed to continuously capture relevant log data across the Citrix Virtual Apps and Desktops (CVAD) environment. AOT is a subset of Citrix Diagnostic Facility (CDF) traces, with additional logs from other components, that can be helpful when troubleshooting common failures (for example, VDA registrations and application/desktop launches etc..).

Unlike traditional tools that require manual intervention, AOT runs in the background by default, ensuring that critical information is available when issues occur, even if the problem cannot be reproduced.

AOT is built to simplify troubleshooting for IT administrators and Citrix support teams to improve the mean-time-to-resolution by:

- Automatically capturing log data for user sessions and system events.
- Eliminating the need to reproduce issues.
- Making logs easily accessible and readable without engineering-level expertise.
- Enabling self-service log data to reduce dependency on Citrix Support.

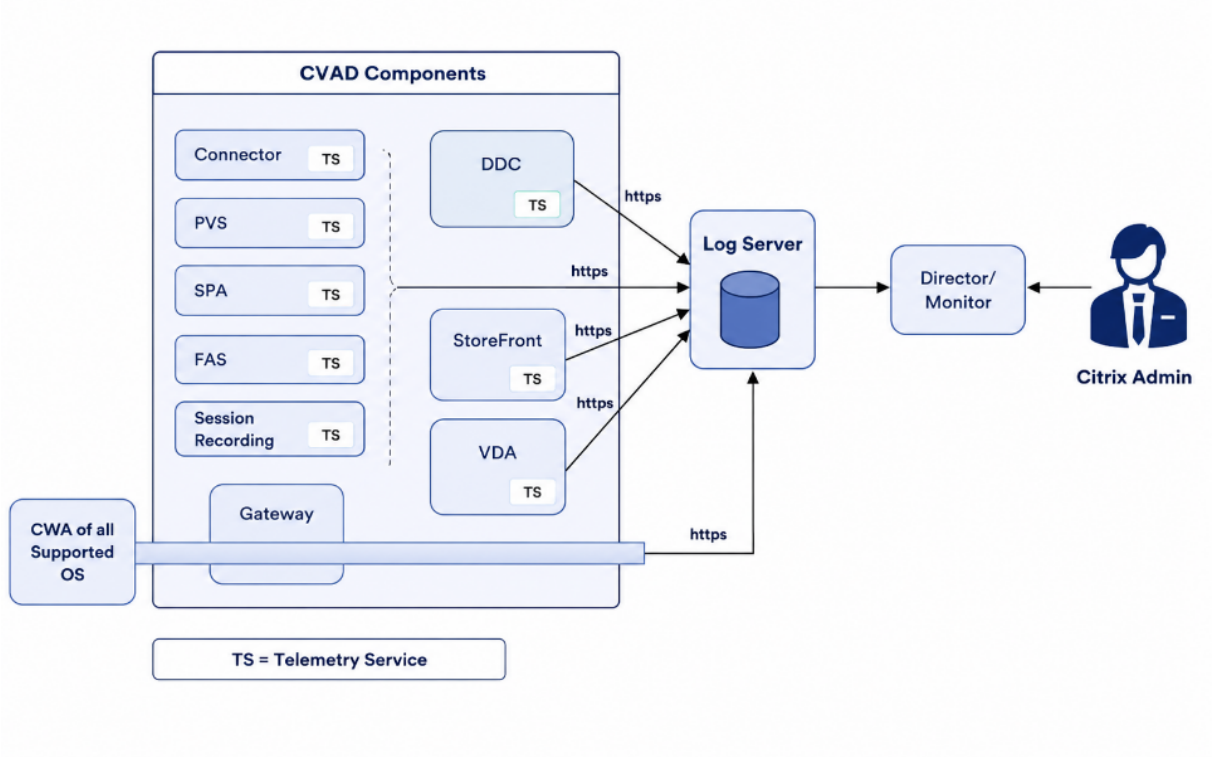
Key Benefits

- Faster MTTR (Mean Time to Resolution)
- Always-on, no manual trace initiation needed
- Self-diagnosis for common issues
- Streamlined escalation to Citrix Support with full context
- Secure, compliant log handling with sensitive data redaction

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Core Concepts

July 5, 2026



The Always on Tracing (AOT) architecture is designed to provide continuous, real-time log collection across the Citrix Virtual Apps and Desktops (CVAD) and DaaS environments. It enables IT administrators and Citrix Support to troubleshoot user and infrastructure issues without requiring manual log initiation or issue reproduction.

The AOT system is built on several integrated components working in sequence to capture, transfer, and store logs from multiple Citrix infrastructure layers into a centralized repository.

Key Components and Workflow

1. **AOT Log Generators (Citrix Core Components)**: Citrix components such as the Virtual Delivery Agent (VDA), Delivery Controller (DDC), StoreFront, and others act as log generators. These components are equipped with the Telemetry Service or a similar service, which uses the AOT API to capture trace data, record pre-defined step traces, and log error events relevant to user sessions and transactions.
2. **Enable Log Collection**: When an administrator initiates a request to collect logs (typically through the web studio settings, instructions are saved in the site database and sent to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the broker, which orchestrates the log collection process across the relevant components, including broker, storefront and VDA. The administrator initiates the request to collect logs through a PowerShell command from other components separately like Session Recording, PVS, FAS etc…

3. **Telemetry Service**: After configuring the Log Server address in the Citrix Web Studio, and when the settings are propagated, the Telemetry Service on each component then activates the new real-time AOT listener, which collects logs based on predefined events, failures, or trigger points.
4. **Log Transfer to Centralized Log Server**: Once the logs are collected, the Telemetry Service or an independent service transfers them securely to a centralized log server directly. In environments where endpoints are connected from external networks through a Citrix Gateway, the transfer typically occurs over a SOCKS tunnel to ensure secure and seamless transfer.
5. **Log Storage and Organization**: The Centralized Log Server receives, parses, and stores the AOT logs in a structured and searchable format using an indexed database backend (OpenSearch by default). Logs are tagged by session, component, and timestamp, enabling easy access and efficient troubleshooting.

Logs in the Citrix AOT system are stored in a structured and searchable format, tagged with various fields to enable easy access and efficient troubleshooting. These tags include:

- **MachineName**: The name of the machine where the log originated.
- **MachineIP**: The IP address of the machine.
- **Role**: The role of the Citrix component (e.g., VDA, DDC, StoreFront).
- **TimeStamp**: The UTC timestamp when the log event occurred.
- **Message**: The actual log message content. Could be searched/filtered by words.
- **Level**: The severity level of the log (e.g., info, warning, error).
- **Module**: The specific software module that generated the log.
- **ProcessName**: The name of the process that generated the log.
- **ProcessId**: The ID of the process.
- **Thread**: The thread ID within the process.
- **Cpu**: Information related to CPU id at the time of the log.
- **SessionId**: The ID of the user session associated with the log.
- **Class**: The class or component within the module.

These detailed tags allow administrators to quickly filter, search, and analyze logs based on specific criteria, facilitating the identification and resolution of issues.

In summary, the AOT workflow begins with Citrix components generating logs. A centralized request is initiated to collect these logs, which the Telemetry Service gathers from the relevant components. The collected logs are then securely transferred to a centralized log server for indexing, storage, and later analysis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How AOT Works

Citrix Always on Tracing (AOT) continuously captures log data from key components in your environment. When triggered, logs are collected automatically, securely transferred to a centralized log server, and retained for analysis. This eliminates the need for manual tracing and simplifies troubleshooting.

Tracing Triggers and Log Collection: Citrix components such as VDA, DDC, StoreFront, and other components are equipped with the AOT API to track critical steps and errors. These components serve as AOT log generators. When an administrator initiates a log collection request from the Delivery Controller:

- The DDC sends instructions to relevant Citrix components. Each component forwards the request to its local Telemetry Service.
- The Telemetry Service starts the real-time AOT listening program to collect AOT logs and forwards the logs to the Centralized Log Server.

Log Storage and Retention: Once the AOT logs are received, the Centralized Log Server formats and indexes them into a structured, searchable database. Logs are retained based on a defined retention policy to optimize storage usage. By default, AOT logs are retained for 7 days, after which they are automatically purged to conserve space.

AOT vs Traditional Logging

Aspect	AOT	Traditional CDF Tracing
Activation	Automatic, continuous	Manual, issue reproduction required
Complexity	User-friendly, readable logs	Engineering-level parsing
Diagnostic Speed	Immediate logs available	Delayed by reproduction effort
Resource Usage	Low overhead with optimized buffers	Moderate to high if used incorrectly

Traditional tracing tools require manual effort and only work if you catch the problem while it's happening. With AOT, logging runs continuously in the background, so issues are captured as they happen —even if you're not watching. This saves time and makes troubleshooting much easier.

AOT Highlights

- **Always On**: Tracing runs all the time, no need to turn it on manually.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Auto Capture**: Logs are collected always when issues occur.
- **Central Log Server**: All logs are stored in one place for easy access.
- **Easier Troubleshooting**: Helps quickly pinpoint common failures.
- **No Reproduction Needed**: No need to recreate the issue; it's already captured.

Centralized AOT Log Server

December 10, 2025

The AOT Log Server acts as a centralized destination for collecting and storing Always on Tracing (AOT) logs from various Citrix components. It is containerized using Docker technology and is preferably deployed on Linux, though it also supports Windows environments via Docker Desktop, and on the Citrix Connector appliance.

Key Features of the AOT Log Server

- **Centralized Log Storage**: Aggregates logs from multiple Citrix components into a unified and searchable location.
- **Retention Policy**: Logs are retained based on a configurable policy (default: 7 days) to optimize storage usage and performance.
- **Deployment**: The Log Server is deployed using packaged installer scripts and Docker containers. The setup requires compatible hardware and a Docker runtime environment or the Cloud Connector appliance (if selected).
- **Secure Log Access**: Logs can be retrieved using CLI tools included with the Log Server. All access requires proper authentication to ensure security and compliance.
- **Integration with Citrix Core Components**: The AOT Telemetry Service is embedded within core Citrix components, enabling them to act as log generators. Telemetry Service ensures seamless and automated log capture across these components, enabling consistent logs visibility throughout the Citrix infrastructure.

AOT Log Server Deployment and Configuration

AOT Prerequisites

The AOT Log Server relies on Docker container technology to function. While Linux is the recommended host operating system, installation on Windows is also possible with Docker Desktop. Alternatively, using a Citrix Connector Appliance provides a packaged solution removing the need to manage hosts and Docker infrastructure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A single Log Server can support **up to 128,000 active component connections** at any moment, and it can process **up to 10,000 log events per second**. Any sizing or deployment recommendation should be based on these two factors:

- **Connection capacity** determines how many components can be connected simultaneously.
- **Log throughput** determines how many logs the system can ingest and index without performance impact.

A single Log Server is suitable as long as your environment stays within these limits.

Citrix Connector Appliance

- Ensure you are running the latest version of Citrix Connector Appliance.
- If you don't have it, download the latest version from Citrix Cloud and install it.

Linux

- **Supported OS**: Ubuntu 24.04 and RHEL 8.10, 9.4
- **Hardware requirements**: 4 cores of CPU, 16 GB RAM, and 500 GB free disk space.
- **Software Requirements**: Install Docker Engine for Linux or Docker Desktop for Linux.
- **User permissions**: Ensure the user can start Docker without requiring root.

Windows

- **Supported OS**: Windows 11, Windows 10, Windows Server 2022 and Windows Server 2025. For Azure VMs see recommendations here.
- **Hardware requirements**: 8 cores of CPU, 24 GB RAM, and 500 GB free disk space.
- **Software requirements**: Install Docker Desktop (subscription may be required) for Windows.
  - **WSL version 2.1.5** or later is required.
  - Enable **Hyper-V** and **Containers** Windows features.
  - Set the memory limit >= 12 GB in docker desktop settings

Log Server Recommendation

June 8, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Daily Log Volume (Storage)

Item	Number of Machines	Sessions per Day/Machine	Avg. Log Size per Session	Total Logs per Day
Persistent VDAs	1000	2	2 MB	4,000 MB (≈4 GB)
Pooled VDAs	1000	50	2 MB	100,000 MB (≈100 GB)
CWA Endpoints	8000	4	1-1.5 MB	48,000 MB (≈48 GB)
Delivery Controllers	4	—	300 MB per DDC	1,200 MB (≈1.2 GB)
StoreFront Servers	4	—	300 MB per server	1,200 MB (≈1.2 GB)
NetScaler Gateway /PVS/Session Recording/ FSA and other servers	4	—	300 MB per server	1,200 MB (≈1.2 GB)
Daily Total Log Size (Post Compression)	—	—	—	**Before compression is ≈156 GB/day** **Post compression is 80 GB to 125 GB/day**

Sizing Assumptions

- This example represents a reference deployment of approximately 10,000 managed endpoints and infrastructure components.
- For sizing purposes, Delivery Controllers, StoreFront servers, Gateway, PVS, FAS, Session Recording, and other infrastructure components are estimated at 300 MB per server per day.
- The 300 MB per server value is a conservative estimate used for storage planning and capacity calculations.

> **Note:**
>
> 1. These values are approximate and can differ widely between deployments. Log volume

© 1997–2026 Citrix Systems, Inc. All rights reserved.

depends on site size, user activity, component mix, and retention needs. Use these numbers only as a baseline to begin planning and adjust the storage allocation based on your environment's actual usage, growth trends, and performance testing.

2. Log server uses the LZ4 compress algorithm by default. The compression percentage could be between 20% to 50%; it means LogServer would take half of the disk space when it does the maximum compression or 80% disk space when it does the minimum compression.
3. A single AOT Log Server can support up to **128,000 active component connections** and process **up to 10,000 log events per second**. The Log Server is designed to continuously collect and store AOT logs around the clock, provided the environment remains within these connection and throughput thresholds.
4. These recommendations are driven not by the size of the virtual machine, but by the capacity of the underlying **search and indexing engine** that ingests, processes, and stores incoming AOT logs. This search layer ultimately determines maximum scale because it handles indexing, querying, and retention operations. As environments grow, this layer must scale horizontally to maintain performance.
5. Today, the Log Server ships as a single combined node that includes both the Log Server service and the search/index engine. This simplifies deployment but limits the ability to scale the search tier independently.
6. In upcoming releases, Citrix will transition to a **separated architecture**, where ingestion and storage/indexing run on independent nodes. This will allow customers to scale the search tier as their environment grows, improve performance across large or multi-site deployments, and remove the scalability ceiling imposed by the current single-node design.
7. Deploy the AOT Log Server on SSD-backed storage. SSDs are strongly recommended to ensure reliable log ingestion, fast search performance, and efficient correlation, especially in high-volume environments.

AOT Log Server Storage Sizing

Sizing storage correctly is one of the most important steps when planning the AOT Log Server. The total storage required depends on how many machines are sending AOT logs, how much data is generated per day, and how long logs must be retained.

Because each Citrix environment behaves differently, customers should begin by estimating their daily log volume using the log generation patterns of their VDAs, Citrix Workspace App endpoints, Delivery Controllers, and StoreFront servers. Once the daily volume is known, the total storage can be calculated using the formulas below.

Storage Calculation Formula

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Total Storage (GB) = Daily Log Volume (GB) × Retention Days

AOT Log Server Storage Sizing Guidance

Use the following table as a reference for estimating daily log volume and storage requirements based on deployment size. These estimates are intended for capacity planning and may vary based on user activity, session density, enabled components, and deployment architecture.

Daily Log Volume Estimate

Deployment Size	Daily Log Volume Before Compression	Daily Log Volume After Compression (LZ4)	Recommended Category
5,000 machines	~78 GB/day	~40–63 GB/day	Small
10,000 machines	~156 GB/day	~80–125 GB/day	Medium
50,000 machines	~780 GB/day	~400–625 GB/day	Large
100,000 machines	~1.56 TB/day	~800 GB–1.25 TB/day	Enterprise

Retention-Based Storage Estimate

Deployment Size	7-Day Retention	10-Day Retention
5,000 machines	~300–450 GB	~400–630 GB
10,000 machines	~600 GB–1 TB	~800 GB–1.25 TB
50,000 machines	~3–5 TB	~4–6.3 TB
100,000 machines	~6–10 TB	~8–12.5 TB

> **Note:**
>
> - These values are approximate estimates intended for capacity planning. Actual storage requirements depend on deployment architecture, user activity, enabled components, retention period, and compression efficiency.
> - Estimates are based on the 10,000-machine reference deployment model and scaled linearly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Minimum supported versions for Always on Tracing (AOT)

July 5, 2026

This table outlines the minimum supported versions of Citrix components required to enable Always On Tracing (AOT) log collection. Version requirements may vary depending on how users access their resources either through **direct access** (for example, directly to StoreFront) or through **Gateway-based access** (Citrix Gateway or Cloud Gateway Services).

Component / Platform	Type	Minimum Version (Direct Access)	Minimum Version (Access via Gateway)
Citrix Workspace App Windows	Client	2511.10 and 2507 CU1 or later	2603 and 2507 CU2 or later
Citrix Workspace App Mac	Client	2603 or later	2603 or later
Citrix Workspace App Linux	Client	Coming soon	Coming soon
Citrix Workspace App HTML5	Client	2511 or later	2603 or later
Citrix Workspace App ChromeOS	Client	2511 or later	2603 or later
Citrix Workspace App Android	Client	2603 or later	2603 or later
Citrix Workspace App iOS	Client	2603 or later	2603 or later
Citrix Virtual Apps and Desktops (Windows VDA, DDC, PVS, FAS, Session Recording, STF, Linux VDA, Mac VDA, WEM, UPM)	Platform	2402 CU4, 2507 CU1, 2511 or later	2402 CU4, 2507 CU1, 2511 or later
Citrix DaaS *	Service	Post February 2026	Post February 2026
Citrix NetScaler	Infrastructure	14.1.60.57	14.1.60.57
Citrix License Server		540000 or later	54000 or later

*For Citrix DaaS deployments, AOT log collection follows the same process. You must configure the DaaS settings to forward logs to the AOT Log Server. All components deployed within the resource location can forward logs to the Log Server once configured. Citrix DaaS control plane components

© 1997–2026 Citrix Systems, Inc. All rights reserved.

do not send logs to the customer-managed Log Server; instead, they continue to forward logs to Citrix-managed cloud telemetry (Splunk). This behaviour applies unless those cloud control plane components are replaced or supplemented with customer-managed CVAD components, such as using StoreFront instead of Workspace Platform or Citrix Gateway instead of Cloud Gateway Services, where applicable.
For more details on log availability across different deployment models, see the **AOT Logs Availability Across Deployment Scenarios** section.

> **Note:**
>
> **Direct Access** refers to scenarios without Gateway involvement (for example, direct StoreFront access).
>
> **Access via Gateway** includes Citrix Gateway and Cloud Gateway Services (CGS).
>
> "Coming soon"indicates planned support in upcoming releases.

Installing and Configuring Log Server

July 5, 2026

The Log Server can be set up on individual Linux or Windows servers or hosted on the Citrix connector appliance and leverage evergreen updates. Refer to the relevant section for installation and configuration steps for each option.

> **Note for Installation**
>
> - For enhanced security, HTTPS is recommended in the deployment.
> - Ensure that the selected port is not already in use.
> - Avoid using privileged ports (0–1023) as they require administrator or system-level permissions.
> - Verify that firewall rules allow traffic on the chosen port.
> - Use a port number within the valid range (0–65535), but avoid ports commonly used by system services to prevent conflicts.
> - If you are using the Citrix Connector Appliance to deploy the Log Server, ensure that only port 443 is configured.
> - The port numbers used in the examples (8080 for HTTP and 8443 for HTTPS) are for reference only. You are not required to use these exact ports. Select appropriate port numbers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> based on your environment and follow the installation guidelines outlined above when configuring the AOT Log Server.

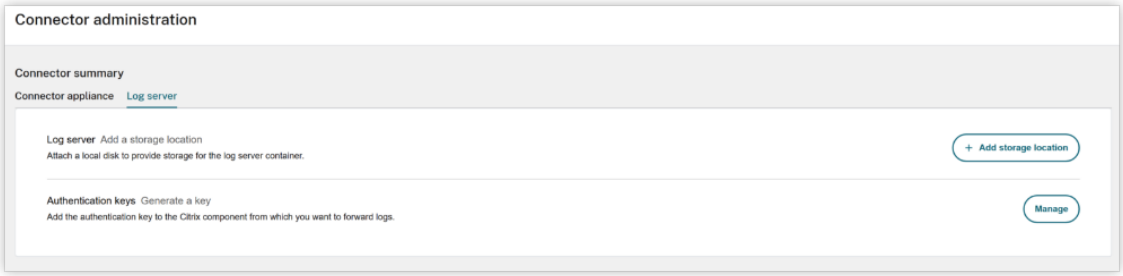
Installing Log Server via Citrix Connector Appliance

The Log Server can be deployed within the Citrix Connector Appliance. This approach eliminates the need to deploy and manage a host VM and manually download images or run container commands. The Log Server is automatically onboarded during Connector Appliance upgrade and remains up to date through ongoing connector updates, ensuring you always have the latest version. For more information, see Connector appliance updates

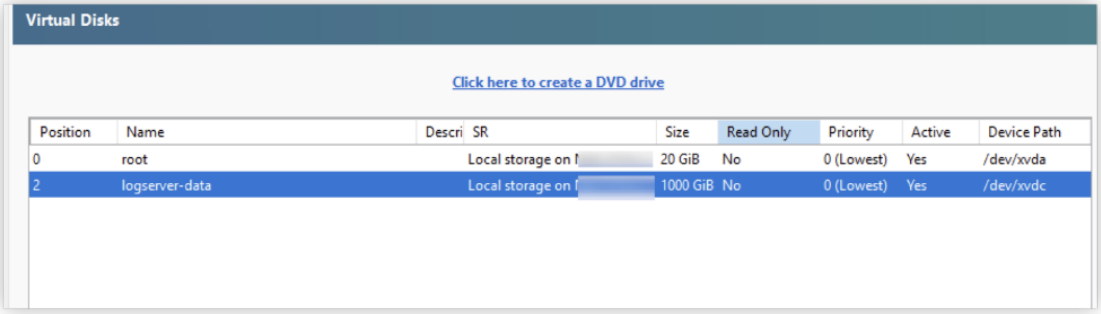
Steps to Deploy Log Server via Citrix Connector Appliance

1. If your environment does not already have a Connector Appliance, deploy the appliance to your hypervisor or from your public cloud marketplace. The minimum required Citrix Connector Appliance is 11.4.1.444. After importing, register the appliance with Citrix Cloud. For more information, see Obtain the connector appliance
2. By default, Connector Appliance has 2 vCPUs and 4GB memory; increase resources to at least 4 vCPUs and 16GB memory to handle log server requests.
3. Create a DNS "A"record for the Connector Appliance FQDN so that supported components can resolve the Log Server hostname. Joining the Connector Appliance to an Active Directory domain is optional.
4. Cloud Monitor retrieves AOT logs through the **Monitor Connector service running on a supported Windows Cloud Connector** in the Resource Location. If the Log Server is deployed on the Citrix Connector Appliance, a supported Windows Cloud Connector must also be present in the same Resource Location. The Connector Appliance alone is not sufficient for Cloud Monitor to retrieve AOT traces. The Cloud Connector must be running version **6.141.0.13739** (or **4.420.0.13739**) or later. Earlier versions will cause the `GetAotTraces` API call to fail, resulting in an HTTP 500 error in Monitor.
5. The Connector Appliance provides a self-signed certificate that is served to a browser that connects to the Connector Appliance administration page. To be able to connect to logserver via HTTPs, you must replace this self-signed certificate with one of your own that is signed by your organization or generated by using your organization's chain of trust, for more details refer to Managing Certificates or Replace Server Certificate.
6. Once the upgrade is complete, log in to the Connector Appliance UI at `https://<connector-appliance-FQDN>/?enable=logserver`, ensure to have the "?enable=logserver"to be able to see the logserver UI. The new Log Server tab now shows storage and authentication key management options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



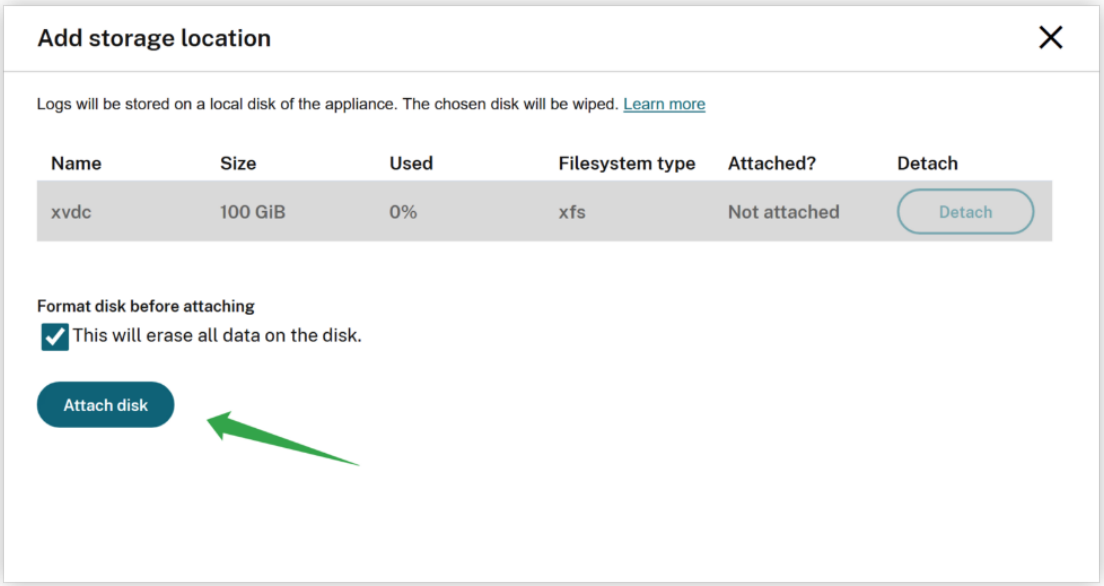
7. The connector appliance boot disk has a capacity of 20GB. To support efficient log storage on the logserver, you should add another virtual disk to the connector appliance using your hypervisor or cloud management platform. This additional disk should have enough space to meet your log storage needs (as explained in the previous section).The XenServer screenshot below shows an example of a connector appliance with an extra disk configured.



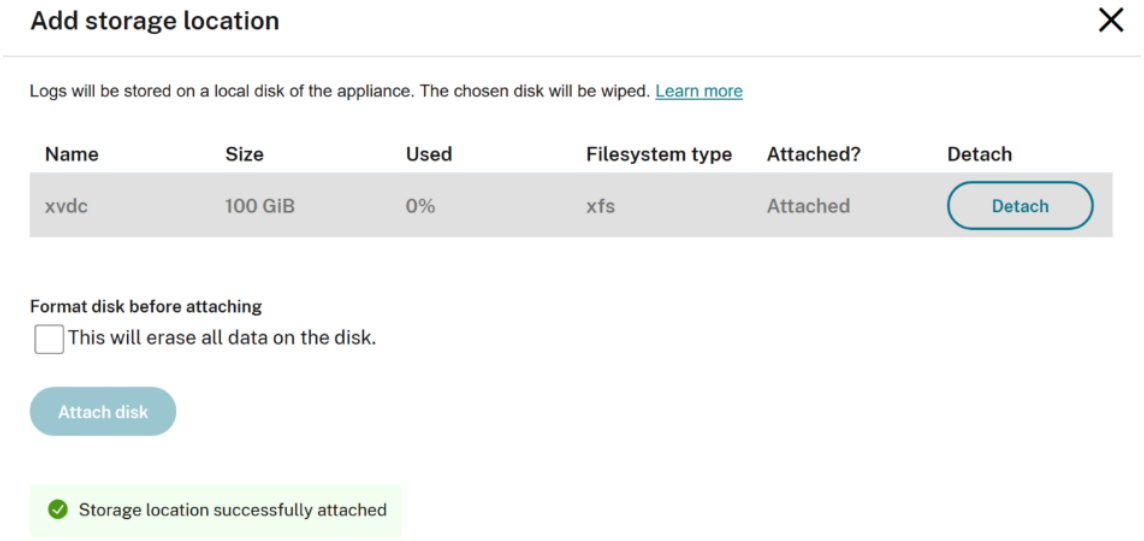
> **Note:**
>
> **A known requirement for VMware ESXi:** Users must attach the additional data disk to a different SCSI controller than the one used by the root disk.

8. After adding the key disk, the logserver UI will automatically detect it, allowing you to format and mount it to the logserver container on the connector appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

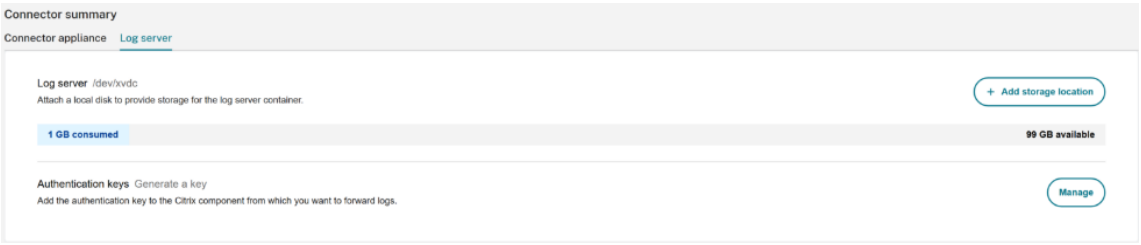


9. Once you click the “Attach disk”button, the disk will be mounted to the logserver container.

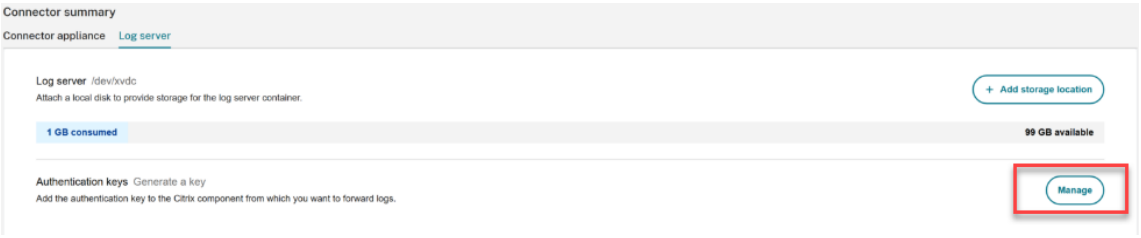


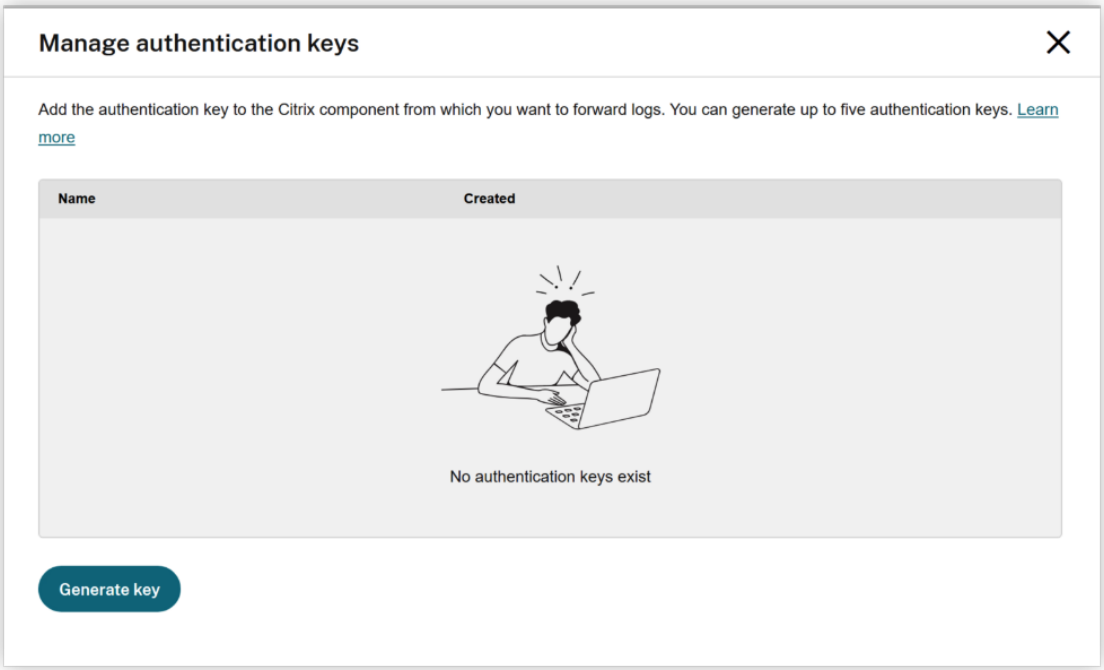
10. The main page will display the disk size along with information about how much space is used and how much remains.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

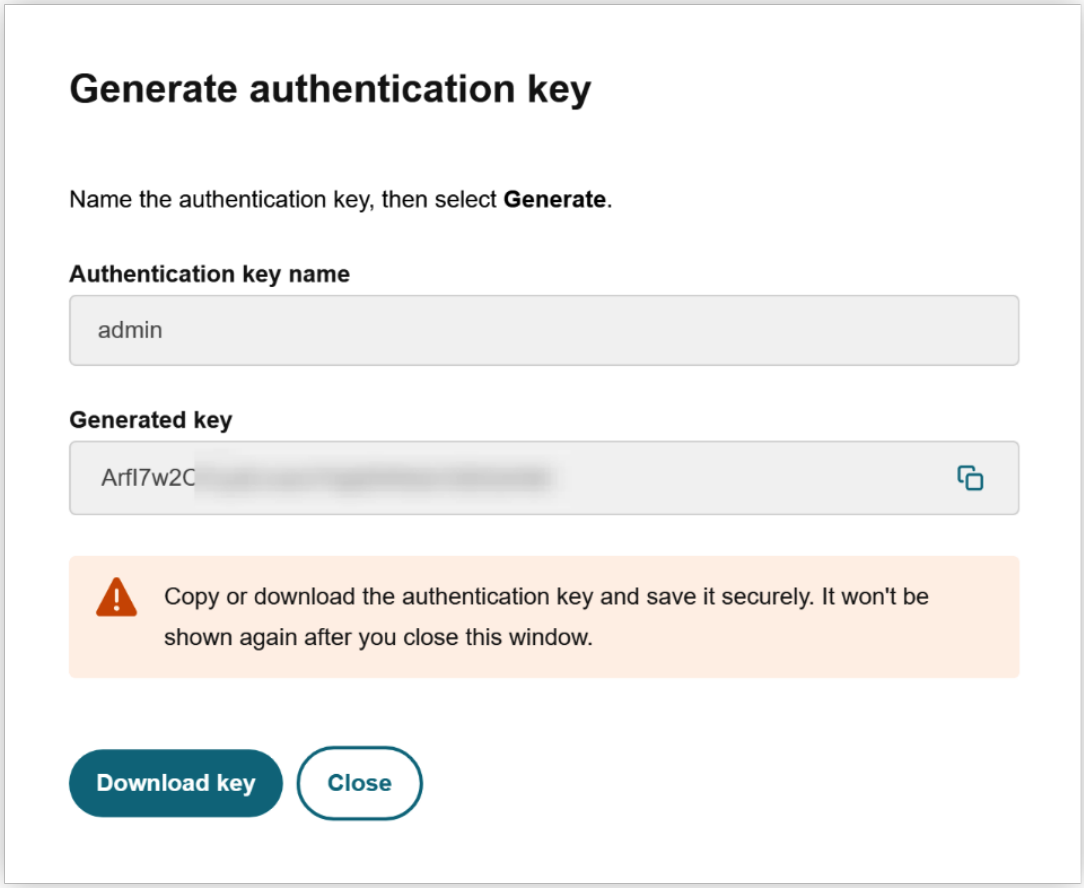


11. After the disk is attached, verify that the Log Server is running by calling the ping endpoint: `https://<connector-appliance-FQDN>/ctxlogserver/Ping`. A pong response confirms that the Log Server has successfully started.
12. Click on Manage button, and click "Generate Key". Now, enter the role name, then copy or download the auth key. The key won't be shown again after you close the window.





© 1997–2026 Citrix Systems, Inc. All rights reserved.



Linux installation

1. Download the log server docker container image from Citrix downloads.
2. Place the downloaded files in the same directory.
3. Run the installer in the directory with terminal (Linux) or command prompt (Windows) and follow the instructions:

```
chmod +x ./InstallLogServer

#Install with https mode with port 8443 with default path
./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port 8443

#Install with http mode, with port 8080 with default path
./InstallLogServer --port 8080

#Command to change the config path and data path of your choice with https mode
./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port 8443 --config /Path/LogServer/Config --database /Path/LogServer
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    /Data
11
12 #Command to change the config path and data path of your choice with
    http mode
13 ./InstallLogServer --port 8080 --config /Path/LogServer/Config --
    database /Path/LogServer/Data
14
15 #To support CWA client uploading AOT logs, some additional parameters
    need to be added after the install log server command.
16 --sta-server http://STA_SERVER_FQDN:port --log-server LOG_SERVER_FQDN:
    PORT
```

Where,

- STA_SERVER_FQDN is the hostname or ip address of the STA server (In on-prem installation, the STA server usually installs along with DDC.)
- LOG_SERVER_FQDN and PORT are the hostname of the log server itself, and the port specified (8080, 8443 or the –port value in the install parameter).
- The log server certificate your_private_cert_key.pfx must be trusted by other Citrix components, where the AOT client will use TLS connection to upload logs.

The **STA_SERVER** address allows the Log Server to issue reconnection STA tickets to Citrix Workspace app (CWA) clients when StoreFront cannot provide them—such as after a session timeout. This enables CWA clients to re-establish the connection directly with the Log Server if a connection break occurs.

The **LOG_SERVER** address is used when the Log Server requests an STA ticket from the configured STA server. The STA server returns a ticket that authorizes connections specifically to the Log Server endpoint.

These parameters are optional if CWA clients don't need reconnection STA tickets or connect to LogServer directly without a gateway.

Post Installation on Linux

After the installation, some useful script files are generated:

```
1 # In Linux, sh scripts will be generated
2 DownloadLogsByTime.sh
3 DownloadLogsByWords.sh
4 GetAuthKey.sh
5 ListMachines.sh
6 StartLogServer.sh
```

Use `./StartLogServer.sh to start the server. Check your configpath/weblogs.txt` to confirm LogServer has started successfully.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the LogServer starts successfully, we can see the below message in the weblogs file. Port 5000 is used by LogServer internally in docker containers with selected http or https protocol.

```
Now listening on https://[::]:5000
```

If the log server was installed in HTTP mode, successful logs should show the below:

```
Now listening on http://[::]:5000
```

If LogServer uses HTTPS, ensure its certificate is trusted on all machines uploading AOT logs

> **Note:**
>
> - The port configured in the installation step (8080 or 8443 or any port specified) should be used when configuring LogServer url in DDC, Storefront, VDA, etc.
> - Usually, it takes 30s to 60s to start on Linux.

Windows Installation

1. Download the log server docker container image from Citrix downloads.
2. Place the downloaded files in the same directory.
3. Run the installer in the directory with terminal (Linux) or command prompt (Windows) and follow the instructions:

Step 1

Install Docker Desktop (subscription may be required) for Windows on the log server VM. Follow the steps below to ensure Docker Desktop installs and starts correctly on Windows systems that rely on WSL 2.

1. Set the memory limit >= 12 GB in docker desktop settings
2. Docker Desktop requires the following Windows features, ensure to verify these features are enabled.
    - Hyper-V
    - Virtual Machine Platform
    - Windows Subsystem for Linux (WSL)
3. If any features are missing, install them and restart the VM to take effect.
4. After the system restarts, open **PowerShell** (Run as Administrator) and update WSL by executing the command `wsl --update`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Docker Desktop requires WSL 2. Configure it as the default by executing the command `wsl --set-default-version 2`
6. Once WSL is updated and the required Windows features are enabled, the Docker Desktop Engine should start successfully.

Step 2

Run the commands below to continue the installation.

> **Note:**
>
> The default location of Config and Database (Data) folders are created under C:\Users<username>\LogServer.You can change them with the commands below

```
#Install with https mode with port 8443 with default path
InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443

#Install with http mode, with port 8080 with default path
InstallLogServer.exe --port 8080

#Command to change the config path and data path of your choice with https mode
InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443 --config C:\LogServer\Config --database C:\LogServer\Datacmd

#Install with specific config path and data path
InstallLogServer.exe --port 8080 --config C:\LogServer\Config --database C:\LogServer\Datacmd

#To support CWA client uploading AOT logs, some additional parameters need to be added after the install log server command.
--sta-server http://STA_SERVER_FQDN:port --log-server LOG_SERVER_FQDN:PORT
```

Where,

- STA_SERVER_FQDN is the hostname or ip address of the STA server (In on-prem installation, the STA server usually installs along with DDC.)
- LOG_SERVER_FQDN and PORT are the hostname of the log server itself, and the port specified (8080, 8443 or the –port value in the install parameter).
- The log server certificate your_private_cert_key.pfx must be trust by other Citrix components, where the AOT client will use TLS connection to upload logs.

The STA_SERVER address enables LogServer to supply reconnection STA tickets to CWA clients when StoreFront cannot provide them due to session timeout. As a result, CWA clients can obtain reconnection tickets directly from LogServer in the event of connection failures.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The LOG_SERVER address is utilised when the logserver requests a STA ticket from the STA_SERVER. The STA_SERVER issues a STA ticket that exclusively authorises connections to the LOG_SERVER address.

These parameters are optional if CWA clients don't need reconnection STA tickets or connect to LogServer directly without a gateway.

Post Installation on Windows

After the installation, a few useful script files are generated in the same directory where you saved the installer files.

> **Note:**
>
> You can move these files to a different location. However, remember the new location, as they will be required again when configuring the Log Server.

```
#In Windows, bat scripts will be generated in the same directory where
   you saved the installer files.
DownloadLogsByTime.bat
DownloadLogsByWords.bat
GetAuthKey.bat
ListMachines.bat
StartLogServer.bat
```

Use `StartLogServer.bat` to start the log server.

Check your `configpath\weblogs.txt` to confirm LogServer started successfully

When the logs show the below, it means to say the Log Server has started successfully. If the LogServer starts successfully you will see the below message in the weblogs file. Port 5000 is used by LogServer internally in docker containers with selected http or https protocol.

```
Now listening on: https://[::]:5000
```

If the log server was installed in HTTP mode, successful logs should show the below:

```
Now listening on: http://[::]:5000
```

If LogServer uses HTTPS, ensure its certificate is trusted on all machines uploading AOT logs.

> **Note:**
>
> - The port configured in the installation step (8080 or 8443 or any port specified) should be used when configuring logserver URL in DDC, Storefront, VDA, etc.
> - Usually, it takes 1~10 minutes depending on the hardware in Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mutual TLS authentication (optional)

Mutual TLS (mTLS) provides an additional layer of security between the Log Server and clients (VDA, DDC, StoreFront, CWA). When mTLS is enabled, both the client and the server authenticate each other using certificates issued by your enterprise PKI.

mTLS is useful in environments where:

- Network segments are untrusted or shared
- There is a requirement to authenticate not only the Log Server but also each AOT log client
- Customers want to prevent unauthorized systems from sending log data
- Regulatory or compliance policies require certificate-based authentication.

Although mTLS is optional, it enhances security by ensuring that only trusted Citrix components can communicate with the Log Server, and that the log server can verify every incoming connection before accepting telemetry data.

Certificate requirements

To configure mTLS, the following certificates must be generated:

- **aotclient.pfx** –Certificate used by AOT log clients (VDA, DDC, StoreFront, CWA)
- **logserver.pfx** –Certificate used by the Log Server
- **enterprise-ca.cer** –The root or intermediate certificate used to sign both .pfx files

> **Note**
>
> - Skip this Mutual TLS section if you use Citrix Connector Appliance, as it isn't supported.
> - The enterprise-ca.cer file must be imported into the Trusted Root Certification Authorities store on both the Log Server and telemetry clients.
> - The aotclient.pfx and logserver.pfx certificates should not be protected by password.
> - The subject of aotclient.pfx must be CitrixAOTClient, allowing the telemetry client to automatically locate the certificate during runtime.

To enable mTLS, include the –ca parameter in the Log Server installation command.
This parameter specifies the path to the enterprise-ca.cer certificate.

```
# with default path
./InstallLogServer --https --cert logserver.pfx --ca enterprise-ca.cer
   --port 8443

# with customized path
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
./InstallLogServer --config /YourPath/LogServer/Config --database /
    YourPath/LogServer/Data --cert /YourPath/logserver.pfx --ca /
    YourPath/enterprise-ca.cer --port 8443

# delete temp certificate logserver.pfx in current install directory
sudo rm -rf /YourPath/logserver.pfx

# keep logserver.pfx accessed only by the container process user '
    ubuntu'.
sudo chmod 400 LogServer/Config/logserver.pfx
sudo chown ubuntu:ubuntu LogServer/Config/logserver.pfx
```

If mutual TLS authentication is required, run the following PowerShell command in DDC, Storefront, VDA and other CVAD components with administrator privileges.

```
# import client cert at the machine aot client
Import-PfxCertificate -CertStoreLocation Cert:\LocalMachine\My\ -
    FilePath c:\aotclient.pfx

# Verify successful import
Get-ChildItem Cert:\LocalMachine\My | Where-Object {
  $_.Subject -like "*AOTclient*"  }


# delete temp certificate aotclient.pfx
Remove-Item -Path "C:\aotclient.pfx" -Force
# Ensure LogServer ' s certificate is trusted on all machines uploading
    AOT logs.
```

> **Note:**
>
> The telemetry service is running in "network service"account, so it is required to manually grant NETWORK SERVICE full control over the private key of the CitrixAOTClient certificate, using the certlm.msc graphical interface.
>
> 1. Press Win + R, type certlm.msc and press Enter to open the Certificates (Local Computer) console.
> 2. Expand Certificates (Local Computer) > Personal > Certificates.
> 3. In the right pane, locate the certificate issued to CitrixAOTClient.
> 4. Open "Manage Private Keys"
> 5. Right-click the certificate and select All Tasks > Manage Private Keys
> 6. In the permissions dialog, select Add, type NETWORK SERVICE, and click Check Names (it should resolve to NT AUTHORITY\NETWORK SERVICE).
> 7. Click OK to apply the permissions.

If customer supplies self-signed certificates, do as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On the logserver side, logserver.pfx and aotclient.cer are installed as previously described. The aotclient.cer serves the role of enterprise-ca.cer.
- On the client side, aotclient.pfx and logserver.cer are imported as previously described. The logserver.cer serves the role of enterprise-ca.cer.
- For more information, seeCreate a new certificate

Verify the Log Server

Open your browser on Log Server or VDA or DDC, visit http://YourLogServerFQDN:8080/Ping

A response string "Pong UTC:08/19/2025 01:03:29 Version: 2511.1.6 will show in the browser. The UTC time should be the LogServer UTC time. The version string contains the release name and builder number.

> **Note:**
>
> Change port 8080 to your configured port if not using the default port, and change http to https if installed with HTTPS mode.

If the log server verification fails, please check the following logs:

- Run docker logs logserver to check docker logs.
- For Linux - `$HOME/LogServer/Config/weblogs.txt` (change $HOME/LogServer to your real installed path if not using default one)
- For Windows - `C:\Users\YourUserName\LogServer\Config\weblogs.txt` (Change YourUserName to real username. Change C:\Users\YourUserName\LogServer to your real installed path if not using default one)

Advanced Configuration of Log Server

On Linux or Windows

Run `docker stop logserver` to stop the logserver

By default, the log server is configured with the below values. To make the changes, edit the `StartLogServer.sh` or `StartLogServer.bat` if installed in windows.

```
-e MAX_RESERVE_DAYS=7
-e MAX_DISK_USAGE_PERCENTAGE=85
-e LOCAL_DOWN_ONLY=true
-e OPENSEARCH_JAVA_OPTS="-Xms2G -Xmx2G"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LogServer Configuration Options	Default Value	Value Range	Desc
LOG_LEVEL	2	0-4	0=Trace, 1=Debug, 2=Info, 3=Warning, 4=Error
CORS_ORIGINS		“Url”or “url1;url2;url3”	Modify this value to allow CWA H5/Chrome client uploading AOT logs. Support multiple urls separated by “;”
MAX_RESERVE_DAYS	7	1~30	Log Server stores log entries max days based on the TimeStamp field. Logs that were inserted 7 days ago will be deleted. Check every 10 minutes.
MAX_DISK_USAGE_PERCENTAGE	85	10~90	Log Server monitors the data storage percentage. If the usage percentage is more than 90%, Log Server will delete old logs day by day until the usage percentage is less than 90%. Check every 10 minutes.
LOCAL_DOWN_ONLY	true	true/false	If true, only the machine installed Log Server can visit the /Download/*APIs. If false, then other machines with AuthKey could visit the /Download/* APIs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LogServer Configuration Options	Default Value	Value Range	Desc
OPENSEARCH_JAVA_OPTS	"-Xms2G -Xmx2G"	2G ~ MaxMem/2	Opensearch memory configurations. Provide more memories if there are a lot of machines that send logs to Log Server. Eg., 0~999 machines: 2GB 1000~1999 machines: 4GB 2000~9999 machines: 6GB

Run `./StartLogServer.sh` on Linux to verify if the changes are updated.

Run `StartLogServer.bat` on Windows to verify if the changes are updated.

On Citrix Connector Appliance

Below are the steps for to configure the advanced settings of log server on Citrix connector appliance via local API.

You can execute this on either Postman or Curl or PowerShell. Below is an example of instructions executed on Postman:

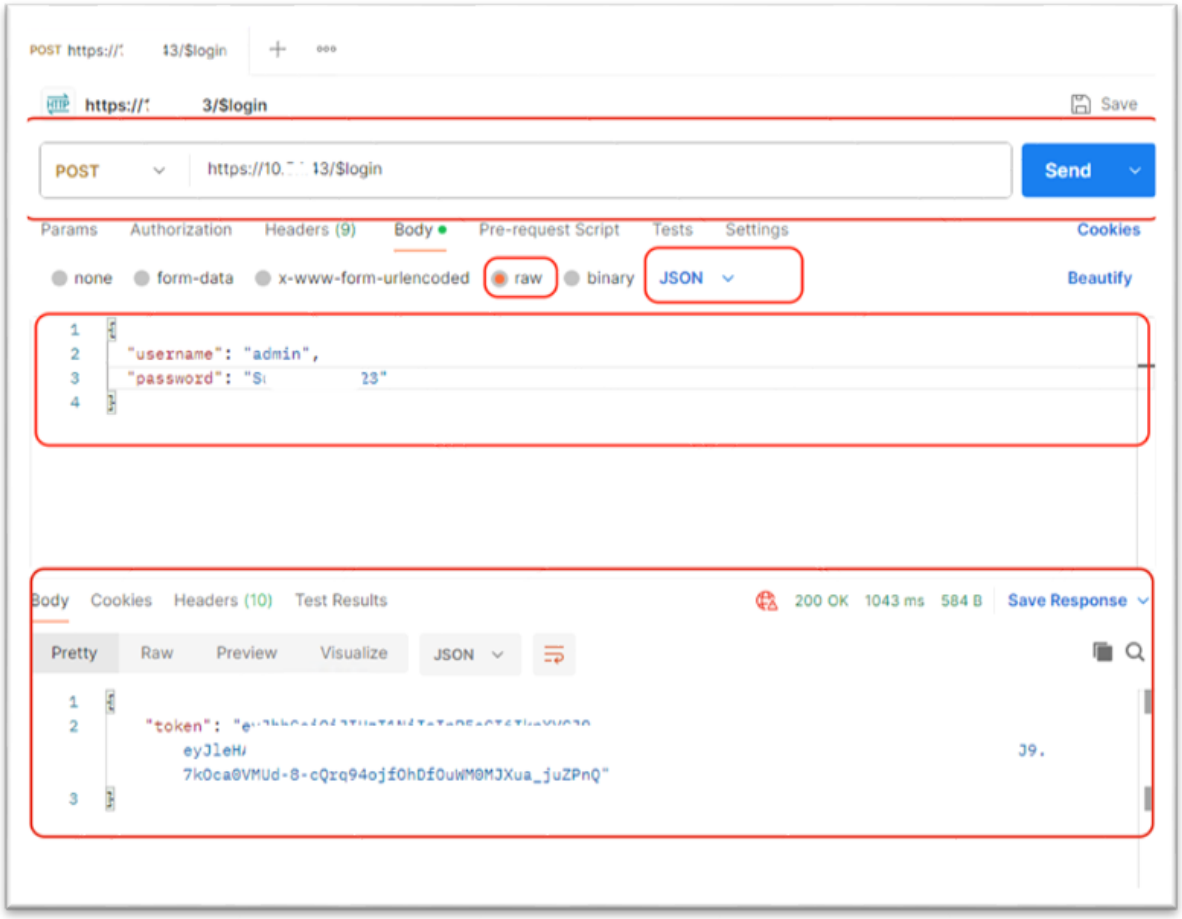
1. **Authentication: Generating a JWT**

All API calls must be authenticated using a JSON Web Token (JWT). You must first generate a token which is then included in the header of subsequent requests.

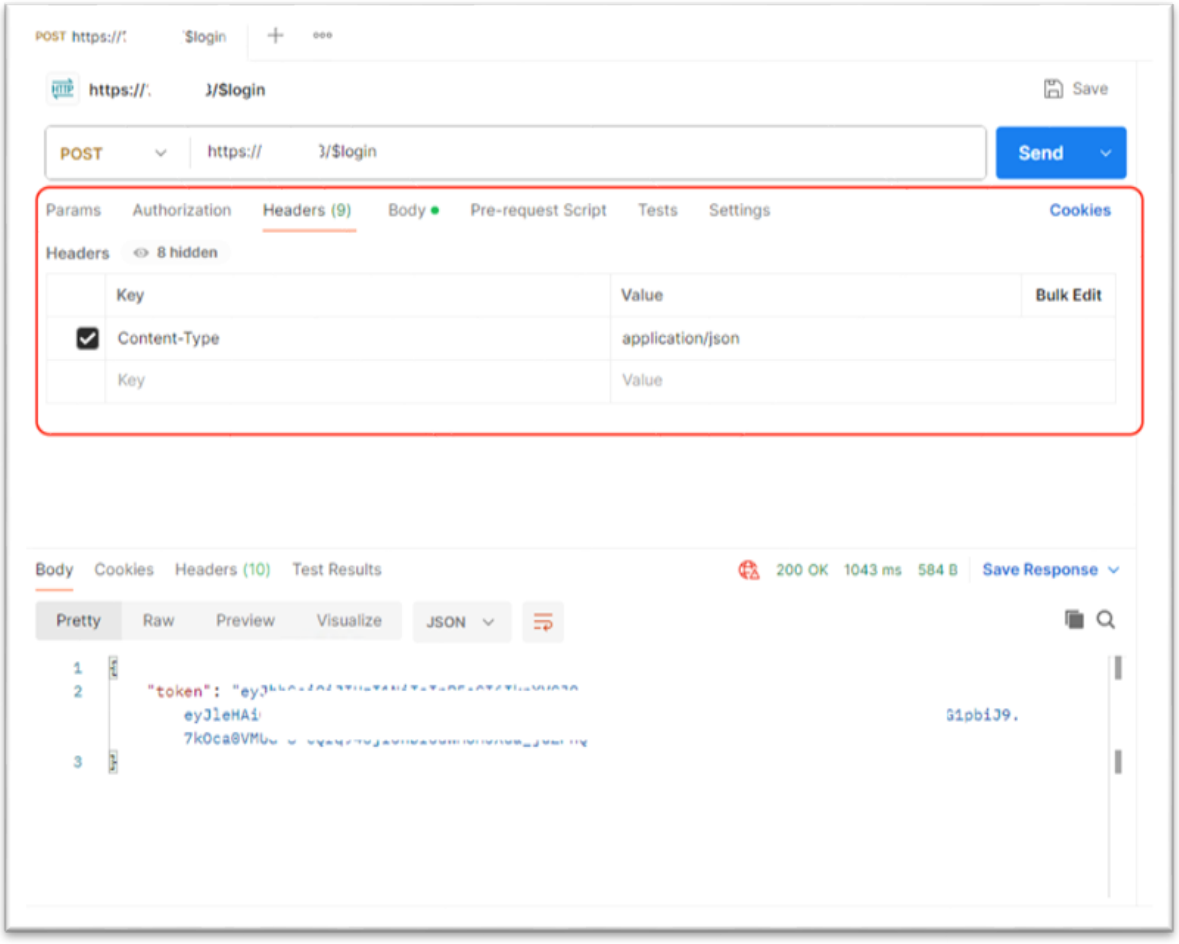
Step 1.1: Generate the Token To generate the token, run a POST request to the $login endpoint.

- Endpoint: POST https://[ip]/$login
- Body: You'll need to include the necessary JSON payload for authentication (e.g., username and password).
  If the credentials are correct, the API will return a token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

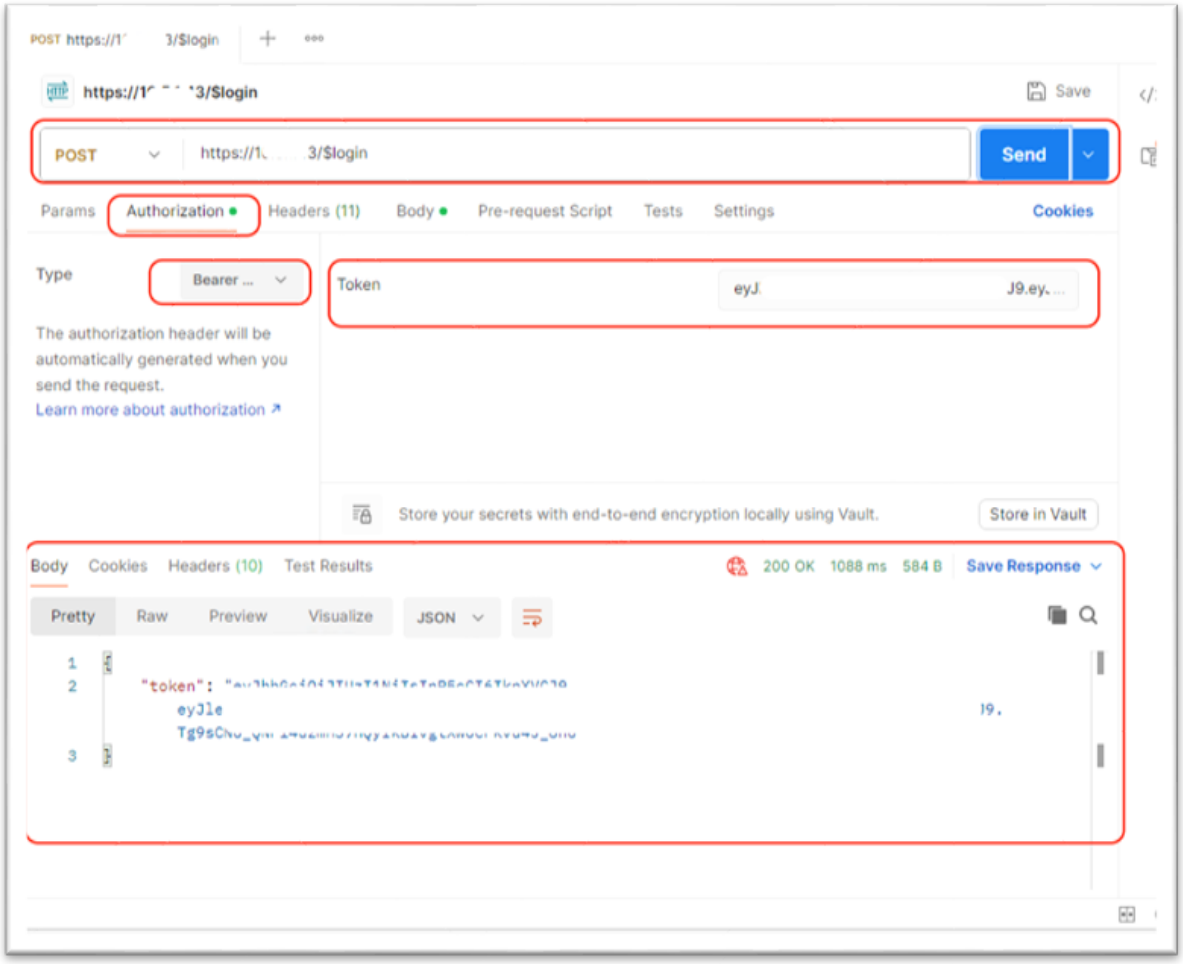


Copy this token value for use in the next steps.

Step 1.2: Authorize API Calls Include the generated token in the Authorization header for all subsequent API calls. The token must be prefixed with Bearer.

Authorization: **Bearer abCD.efGH.ijKL**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A valid token will allow the API call to proceed. An invalid or expired token will be rejected with an error message.

1. **Adding advanced settings**

Once authenticated, you can configure the settings for a target container like logserver **Configure the MAX_RESERVE_DAYS**

This action configures the MAX_RESERVE_DAYS for the logserver.

- Endpoint: https://[ip]/providers/logserver-provider/environment
- Method: PATCH

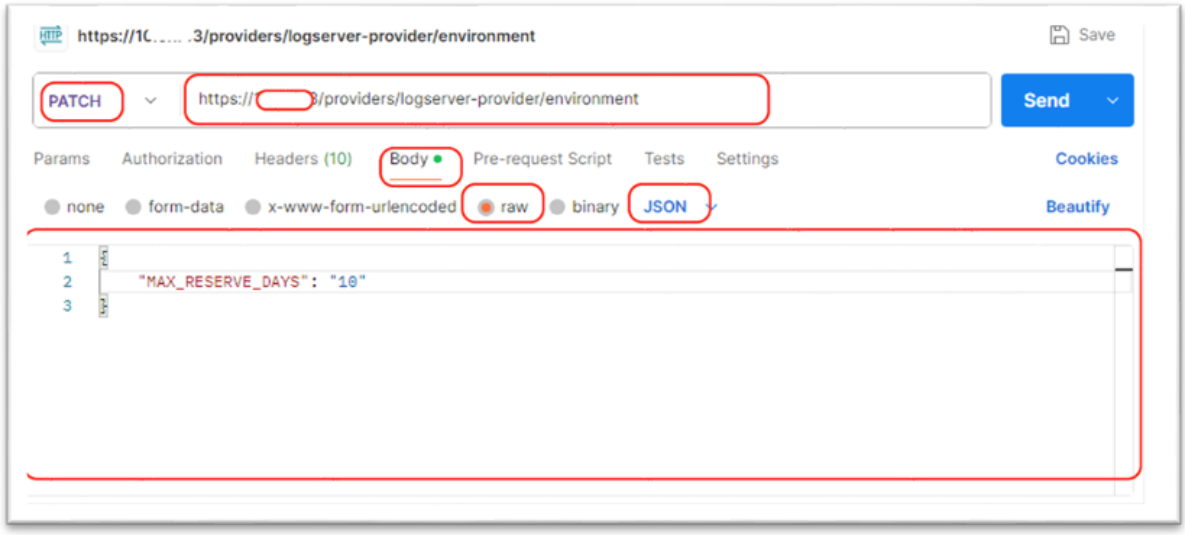
Request Body {
“MAX_RESERVE_DAYS”: “7”
}

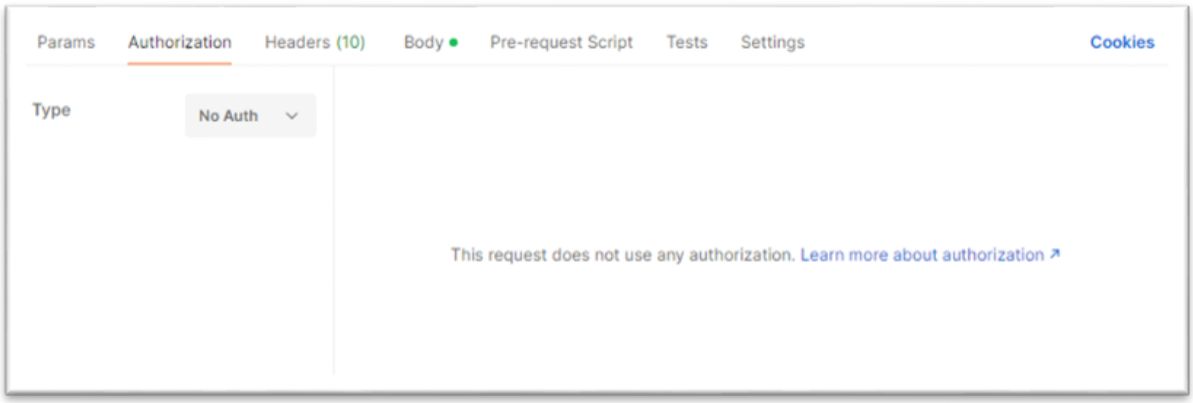
Fields

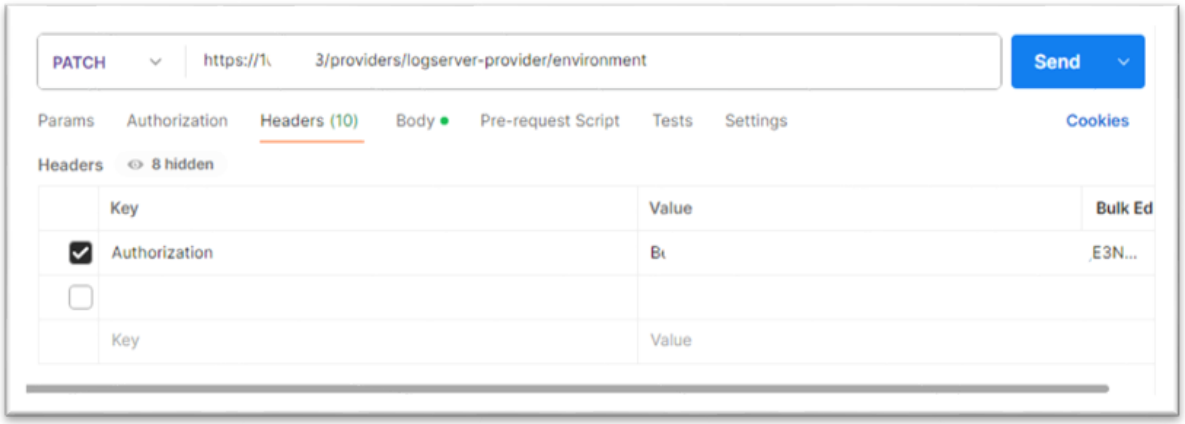
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- MAX_RESERVE_DAYS (string, required): Default value is 7 days. Log Server stores log entries max days based on the TimeStamp field. Logs that were inserted 7 days ago will be deleted. Check every 10 minutes.

In this example, we are changing it to 10 days.

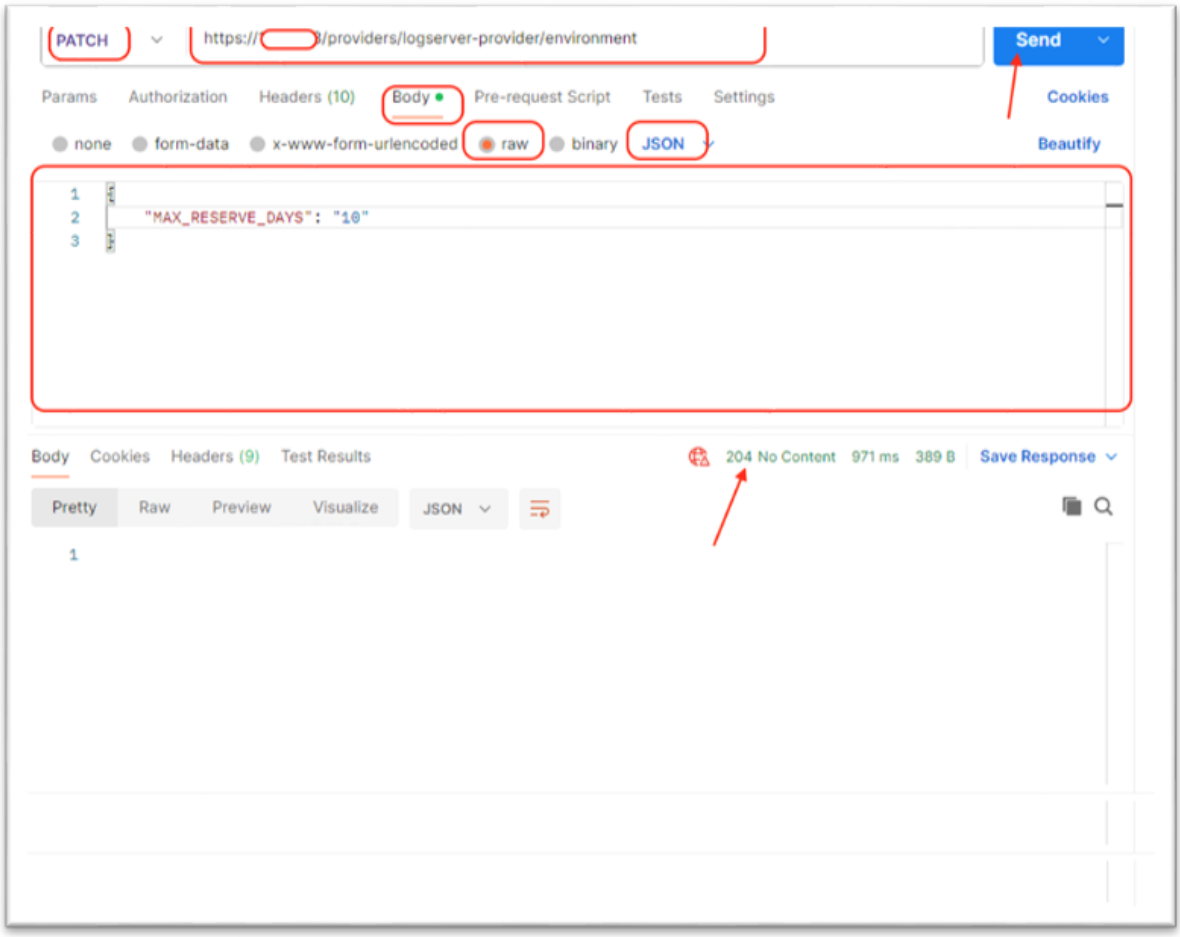






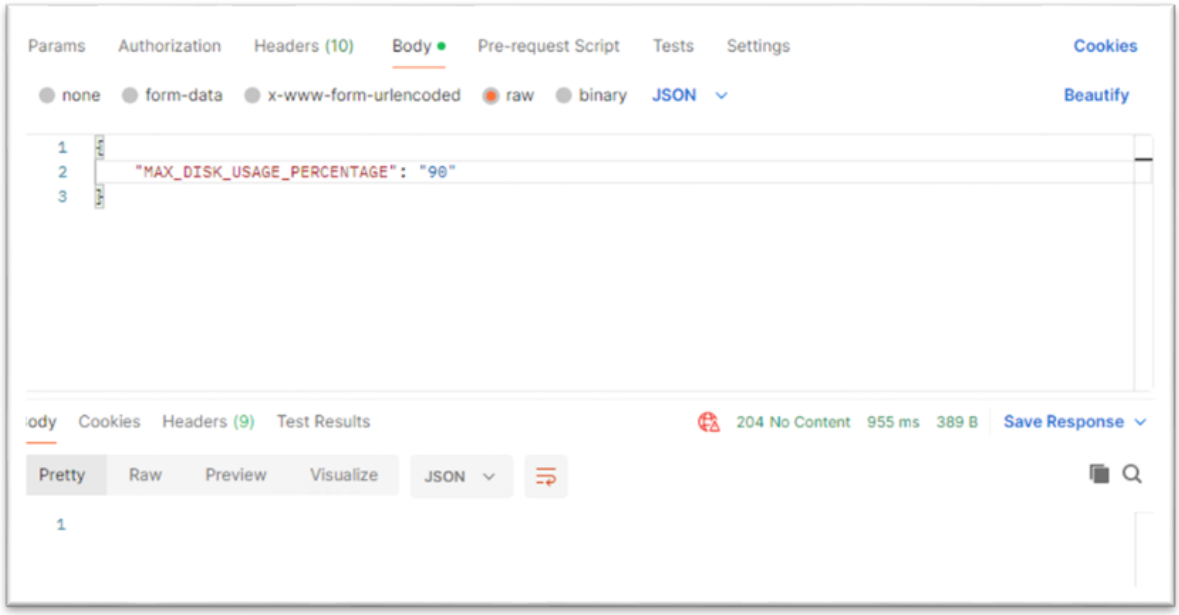
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Responses ☒ Success (204 OK)
Indicates setting is properly configured



Similarly, we can also adjust the Max Disk Usage Percentage from its default of 85. We are changing it to 90 here. When disk usage hits 90%, old logs are deleted to make space for new ones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Response ☒ Success (204 OK)
Indicates setting is properly configured

Upgrade Log Server

December 4, 2025

For a successful upgrade, it is advisable to remove the existing logserver container beforehand by executing `docker rm –f logserver`.

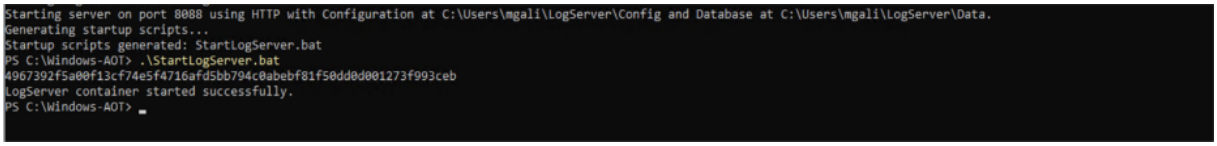
- To upgrade Log Server, download the installation images and new executable log server file, and run the InstallLogServer command with the same arguments.
- The InstallLogServer will prompt whether to delete the current logserver container and images. It is safe to delete the container and images as the log data and configurations are saved separately.

```
PS C:\Windows-AOT>
PS C:\Windows-AOT> .\InstallLogServer.exe
Checking if Docker is available...
Checking for existing logserver container...
Existing logserver container found.
Select action: [R]ename container or [D]elete container:
```

- If you need to keep the old container, you should rename and stop the container (docker stop logserver) before the upgrade process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Don't start the old container and new container at the same time with the same –data path, otherwise the log data will be corrupted.
- After upgrading, the newly generated scripts should be used to start the Log Server.



> **Note:**
>
> This step is not required for Connector Appliance, as updates are managed automatically by Citrix.

Uninstall Log Server

December 4, 2025

1. Uninstall Log Server in Linux

Run the below commands in terminal:

```
docker rm -f logserver
docker rmi logserver

# List containers and images to make sure

docker ps -a
docker images

# Delete Log Server config and data files if not needed any more, change $HOME/LogServer to real installed path if not installed with the default one

rm -r $HOME/LogServer
```

2. Uninstall Log Server in Windows

Run the below commands in powershell:

```
docker rm -f logserver
docker rmi logserver

# List containers and images to make sure
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
5
6  docker ps -a
7  docker images
8
9  # Delete Log Server config and data files if not needed any more,
       change ~/LogServer to real installed path if not installed with the
       default one
10
11 Remove-Item -Recurse -Force ~/LogServer
```

Uploading the AOT logs from CVAD Core Components

July 13, 2026

Beginning with CVAD 2507 CU1 and CVAD 2511, AOT logs are gathered from all applicable components. The supported components include DDC, StoreFront, Citrix Director, Windows VDA, Linux VDA, Mac VDA, License Server, FAS, Cloud Connector, PVS, WEM, Session Recording, Citrix Workspace UI, and Citrix Gateway.

Centralized log forwarding configuration via Citrix Web Studio for CVAD on-prem

Citrix Web Studio provides a centralized location for configuring Always-on Tracing (AOT) log forwarding across the site. This setting defines where AOT logs are sent and automatically propagates the configuration to relevant components in the environment.

When you configure the log server in Web Studio:

- The configuration is written in the **Site database**.
- **Delivery Controllers** retrieve the updated settings and distribute them to the VDAs in the selected delivery groups.
- **VDAs** use the received configuration to forward their AOT logs to the specified log server.
- **StoreFront** that participates in AOT logging receives the necessary details through the same centralized mechanism.
- **Director** uses the provided AuthKey and log server details to query and display AOT logs for monitoring and troubleshooting.

This centralized approach removes the need to configure each component individually. You set up the log server details once in Web Studio, and Citrix automatically propagates the configuration across the site.

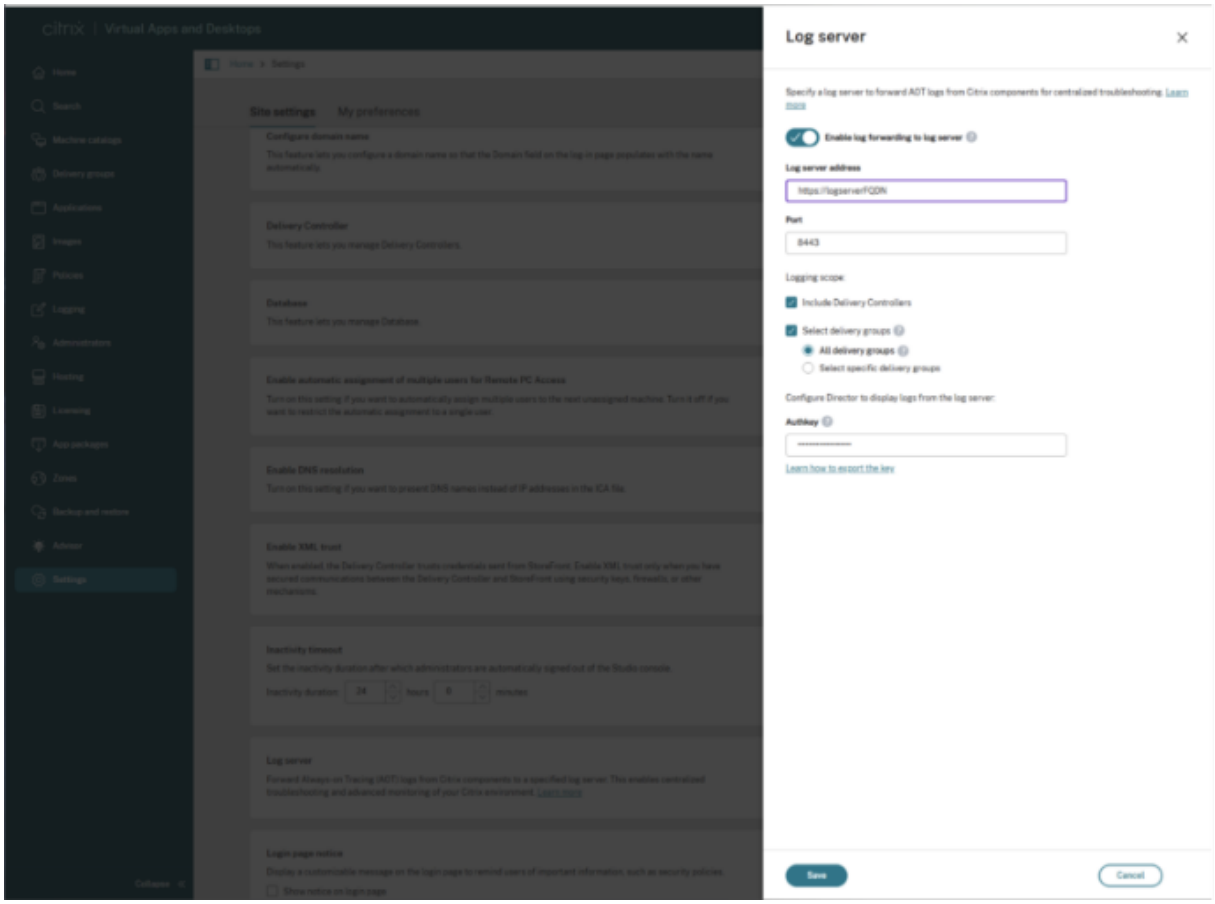
Below is the list of components that will get log server details once it is set on Web Studio:

- Citrix Director/Monitor

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Delivery Controller
- Windows VDA
- Linux VDA
- Mac VDA
- StoreFront
- Session Recording Agent
- CWAs

To configure the log server settings for on-prem environment



1. Sign in to **Web Studio** and select **Settings** in the left pane.
2. In the **Log server** tile, select **Add** if no log server is configured.
3. On the **Log server** page, turn on **Enable log forwarding to log server**.
4. Enter the **Log server address** and **Port**. VDAs and Delivery Controllers use this information to forward AOT logs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> a) If you are using the Citrix Connector Appliance to deploy the Log Server, ensure that only port 443 is configured.
>
> b) Updating the Log Server address and port in Citrix Studio works initially, but if you revisit the settings and modify the Log Server details without re-entering the authentication key, the authentication key placeholder becomes empty after saving, even though the operation appears successful. This results in missing or invalid configuration in Director and Monitor. As a workaround, always re-enter and validate the authentication key whenever modifying Log Server settings until this issue is resolved.

5. Choose which components forward logs:
   a) **Include Delivery Controllers**: Sends AOT logs from all Delivery Controllers.
   b) **Select delivery groups**: Sends logs from VDAs in selected delivery groups.
      - **All delivery groups**: Sends logs from all VDAs.
      - **Select specific delivery groups**: Choose individual delivery groups to include.
6. Enter the AuthKey generated on the log server. The dDirector uses this key to authenticate and retrieve logs.
7. Select **Save** to apply the configuration.

To edit an existing configuration

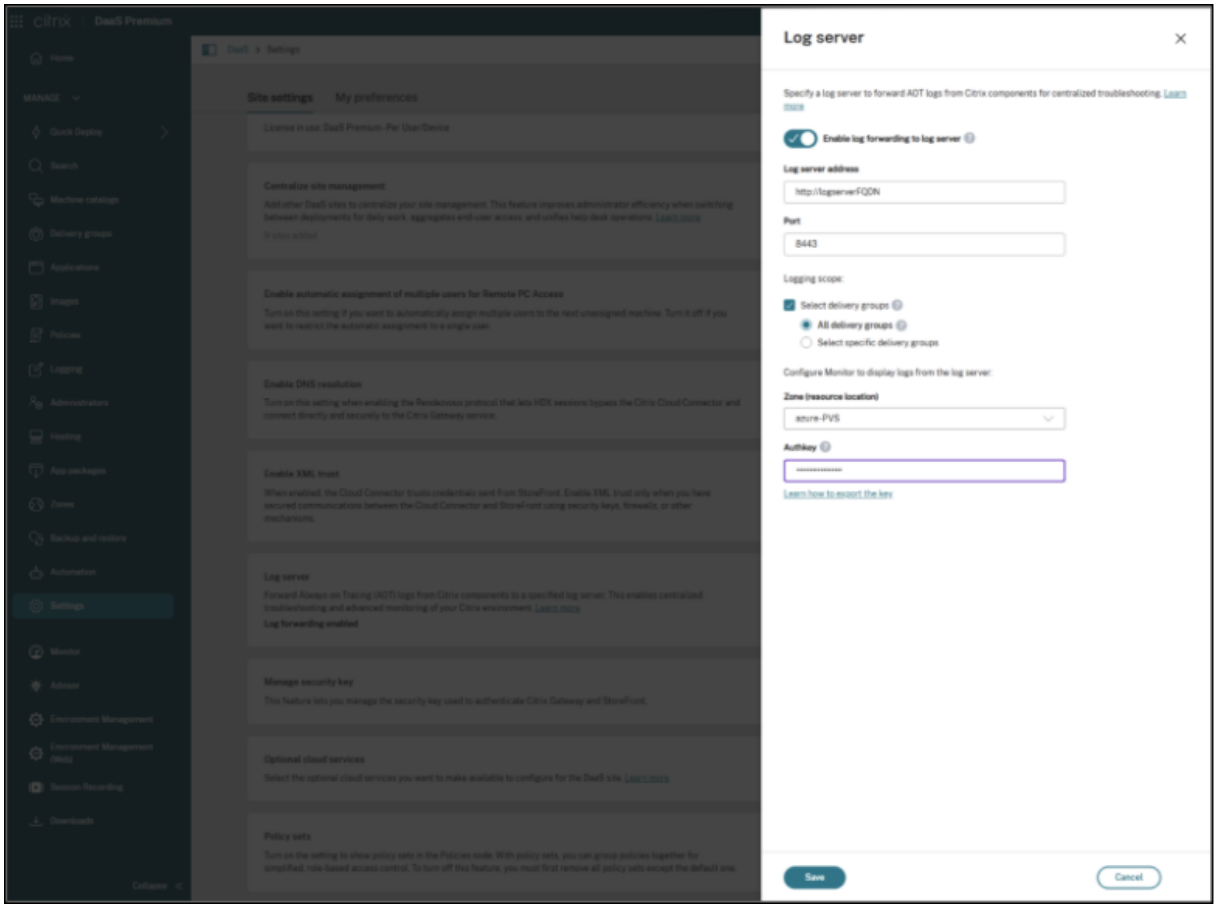
To update the log server or modify the logging scope, go to **Settings > Log server** and select **Edit**.

Configure the log server settings for Citrix DaaS/Cloud environment via DaaS settings

Always On Tracing (AOT) is supported for both on-premises (CVAD) and Citrix DaaS (cloud) deployments. However, log collection behaviour differs based on where the components are hosted.

After installing and configuring the AOT Log Server (on Linux, Windows, or Connector Appliance), complete the following to enable log forwarding to the Log Server in Citrix DaaS settings for Cloud deployments:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix Web Studio for DaaS (DaaS settings) provides a centralized location to configure Always-on Tracing (AOT) log forwarding for cloud-managed sites. This configuration determines where AOT logs are sent and controls which VDAs participate in log forwarding. Monitor uses these settings to retrieve and display logs for troubleshooting.

1. Sign in to **Web Studio** for DaaS (DaaS Settings) and select **Settings** in the left pane.
2. In the **Log server** tile, select **Add** if no log server is currently configured.
3. On the **Log server** page, enter the **Log server address** and **Port**. VDAs use this information to forward AOT logs to the server.
4. Define which VDAs forward logs:
    a) Select **Select delivery groups** to control the scope.
    b) **All delivery groups** (default) forwards logs from all VDAs in the site.
    c) To target specific VDAs, select **Select specific delivery groups**, and choose the delivery groups you want to include.

> **Note:**
>
> If you are using the Citrix Connector Appliance to deploy the Log Server, ensure that only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> port 443 is configured.

5. Select the Zone (resource location) where the log server is deployed.
6. Enter the Authkey generated by the log server. Monitor uses this key to authenticate and retrieve logs for display.
7. Select Save to apply the configuration.

Log forwarding configuration for other components

Configure AOT log upload for StoreFront in Citrix Cloud deployments

For Citrix Cloud (hybrid) deployments, when on-prem storefront is used (instead of Citrix Workspace) with Cloud DDC, StoreFront does not automatically receive the AOT Log Server configuration from the Cloud Connector. Run the following PowerShell command on the StoreFront server to manually configure the AOT Log Server endpoint.

```
# Enable - Run the following command in StoreFront PowerShell

Enable-CitrixAOTUpload -AoTDataStoreEndpoint https://<FQDNofLogServer
    >:<server_port> -Role StoreFront

# Disable - Run the following command in StoreFront PowerShell
Disable-CitrixAOTUpload
```

> **Note:**
>
> Execute this command only for Citrix Cloud (hybrid) deployments that use Cloud DDCs. Do not run this command for on-premises CVAD deployments where StoreFront is paired with on-premises Delivery Controllers, as the Log Server configuration is automatically synchronized and no manual configuration is required.

Configure AOT logs upload for Session Recording Server

You can configure the Session Recording Server to upload AOT logs to a central log server by running the following PowerShell command on the Session Recording Server machine:

```
#Enable - run following command in Session Recording Server PowerShell
Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://FQDNofServer>:<
    server port> -Role SessionRecording

#Disable - run following command in Session Recording Server PowerShell
Disable-CitrixAOTUpload
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure AOT logs upload for FAS

You can configure FAS to upload AOT logs to a central log server by running the following PowerShell command on the FAS Server:

```
#Enable - run following command in FAS PowerShell
Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://FQDNofServer>:<
    server port> -Role FAS

#Disable - run following command in FAS PowerShell
Disable-CitrixAOTUpload
```

> **Note:**
>
> Always-on tracing is not available if you install or upgrade using the FAS installer MSI file - FederatedAuthenticationService_x64.msi.
>
> Always install FAS from the CVAD MetaInstaller or XenDesktopFasSetup.exe or FasSetup_xxxx.exe

Configure AOT logs upload for PVS

You can configure PVS to upload AOT logs to a central log server by running the following PowerShell command on the PVS Server:

```
#Enable - run following command in PVS PowerShell
Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://FQDNofServer>:<
    server port> -Role PVS

#Disable - run following command in PVS PowerShell
Disable-CitrixAOTUpload
```

> **Note:**
>
> If you have multiple PVS servers, run the command to enable or disable AOT log uploads on each one.

Uploading AOT logs for License Server

- The Logserver URL needs to be updated inside SLS config file, which can be find at the location "C:\Program Files (x86)\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml" with XML tag "AotServerURL"

Example:

```
<AotServerURL>https://<FQDNofLogServer:443>//ctxlogserver/
    UploadCitrixLogStream</AotServerURL>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> **When are logs generated in License Server?**
>
> License Server AOT logs are generated only during specific events such as: License Server installation or upgrade, WSL (Citrix Web Services for Licensing) service restart, License activation failure, Dark site activation failures and Clock-related licensing issues
>
> If none of these events occurred recently, the absence of logs does not necessarily indicate a problem.

Quick Checks

1. Confirm whether a qualifying event (restart, upgrade, activation issue, etc.) occurred recently.
2. Restart the Citrix Web Services for Licensing service and allow up to one hour for upload processing.
3. Verify the AOT Log Server URL is configured correctly.
4. Confirm the Citrix Web Services for Licensing service is running.
5. Check: `C:\Program Files (x86)\Citrix\Licensing\LS\resource\aot`
   If the file contains data, logs may be waiting for upload.

> **Note:**
>
> License Server AOT logging is event-driven, not continuous. It is normal to see no logs when no qualifying events have occurred.

- The License Server periodically uploads the logs to AOT server automatically.

Configure AOT logs upload for Citrix Connector

To collect Cloud Connector logs in the AOT Log Server, the following requirements apply:

- Cloud Connector must be on **version 6.169.0.22492 or later**.
- In **Cloud DDC deployments**, Log Server configuration details are automatically synchronized to the registry with **May release**, and no manual configuration is required
- In **hybrid deployments (on-prem DDC)**, manual registry configuration is required to enable log collection. Create the following registry entries on the Cloud Connector machine:

Path:
`HKLM\Software\Citrix\ConfigSyncService`

Entries:

- `LogServerEnabled (REG_DWORD)= 1`
- `LogServerEndpoint (REG_SZ)= <https://<logserver-fqdn>:<port>>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure AOT logs upload for Citrix Workspace apps

Citrix empowers Citrix Workspace app clients to automatically upload diagnostic logs to the centralized log server. This capability enhances troubleshooting efficiency by providing administrators with immediate access to client-side diagnostic information without requiring manual log collection. The client side AOTs will be automatically uploaded, and it triggers when AOT feature is enabled in the whole CVAD environment, and when user launches a resource.

System requirements

- Citrix Virtual Apps and Desktops 2511 or CVAD 2507 CU1 and later versions
- Citrix Workspace app 2511 or CWA 2507.1 CU1 and later versions
- Ensure the required version of the selected Citrix Workspace app (CWA) is installed. For more information, see Supported versions

Prerequisite

Citrix Workspace app web launches **For Citrix Workspace app web** launches (including WebHelper, direct ICA file download, and web browser extension launch methods), StoreFront must be configured to use the modern User Interface (UI Experience).
For instructions on enabling the modern UI experience, see the StoreFront documentation.

> **Note:**
>
> This prerequisite applies only to web-based launches and is not required for native Citrix Workspace app launches.

Configure AOT logs upload for NetScaler

- SSH into NetScaler CLI and then go into the NetScaler shell by running “shell”command.
- Go into /var/analytics_conf directory

```
cd /var/analytics_conf
```

- Generate the schema file by executing an interactive python script “python {auditlog_schema_generator_for_hec_export.py}”. The schema file defines the HTTP headers (Auth-token, User-Agent etc) and Payload attributes (Role, Machine IP etc).

Snippet of the output generated by this script

```
root@Raju-adc2# python auditlog_schema_generator_for_hec_export.py
Schema Builder: Follow the prompts to define your schema.
Include 'Auth-Token'? (Y/n):
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Enter the display name (alias) for 'Auth-Token' (press Enter to keep as is): Authkey
'Auth-Token' can only go in 'header'. Automatically selected.
Include 'HostName'? (Y/n): n
Include 'Content-type'? (Y/n): y
Enter the display name (alias) for 'Content-type' (press Enter to keep as is):
'Content-type' can only go in 'header'. Automatically selected.
Default value for 'Content-type' is 'application/json'.
Do you want to change it? (y/N):
Include 'User-agent'? (Y/n):
Enter the display name (alias) for 'User-agent' (press Enter to keep as is):
'User-agent' can only go in 'header'. Automatically selected.
Default value for 'User-agent' is 'AUDITLOGS/1.0'.
Do you want to change it? (y/N):
Include 'Role'? (Y/n): y
Enter the display name (alias) for 'Role' (press Enter to keep as is):
Where should 'Role' be included? (HEADER/payload): HEADER
Default value for 'Role' is 'GW'.
Do you want to change it? (y/N): y
Enter new default value for 'Role': Gateway
```

Sample schema file generated

```
{

     "Header": {

         "Auth-Token": {

             "name": "AuthKey"
          }
 ,
         "Content-type": {

             "name": "Content-type",
             "value": "application/json"
          }
 ,
         "User-agent": {

             "name": "User-agent",
             "value": "AUDITLOGS/1.0"
          }
 ,
         "Role": {

             "name": "Role",
             "value": "Gateway"
          }
 ,
         "MachineIP": {

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "name": "MachineIP"
          }
,
        "MachineName": {

            "name": "MachineName"
          }

      }
,
    "Payload": {

        "LogLevel": "Level",
        "MessageContent": "Message",
        "ModuleName": "Module",
        "Time": "TimeStamp"
      }
,
    "Format": {

        "delimiter": ""
      }

  }
```

- Exit the shell and come back to the NetScaler CLI
- Create a syslog Action which defines the Syslog Server, Ports and the schema file (created in the previous step) etc

```
add audit syslogAction {
 Action Name }
  {
 AOT Server IP/FQDN }
  -serverPort {
 Destination Port }
  -logLevel {
 Log Level }
  -transport HTTP -httpAuthToken {
 Authentication Token generated on the AOT sever }
  -httpEndpointUrl {
 AOT Server URL where logs will be sent }
  -httpSchemaFile {
 Schema File created in Previous Step }
```

Example:

```
add audit syslogAction act1 10.102.154.196 -serverPort 8088 -logLevel
    ALL -transport HTTP -httpAuthToken
    fbb94d5b234d86a6cb155e3f808dd33c9698a0d1a866e814573b1909e4c9e56896f433da1071e3
     -httpEndpointUrl "/services/collector/event" -httpSchemaFile sample
    .json
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Bind the syslogAction to the Audit Syslog Policy

```
add audit syslogPolicy {
 PolicyName }
  True {
 Name of the Syslog Action }
```

Example:

```
add audit syslogPolicy pol1 true act1
```

Viewing and Using AOT Logs

May 10, 2026

Accessing Logs via Director UI

Step1

Edit the `StartLogServer.bat` file

The `StartLogServer.bat` file contains all configuration parameters used to start the AOT Log Server container, including several environment variables that control log access and behavior. One of the key settings is **LOCAL_DOWN_ONLY**.

- When **LOCAL_DOWN_ONLY=false**, the Log Server accepts remote log-viewing requests. This allows **Citrix Director/Monitor** to connect to the Log Server and display AOT logs directly in the Monitor UI.
- When **LOCAL_DOWN_ONLY=true**, the Log Server restricts log access to local-only connections. In this mode, you must connect directly to the Log Server machine to view logs, and **Citrix Director Monitor will not be able to retrieve or display logs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

File Edit View

```
@echo off
REM Auto-generated startup script for LogServer
docker rm -f logserver 2>nul
docker run -d --restart unless-stopped ^
  -e USE_HTTPS=false ^
  -e STA_SERVER="" ^
  -e LOG_SERVER="Win11-AOTLogSer:8088" ^
  -e LOG_LEVEL="2" ^
  -e MAX_RESERVE_DAYS="7" ^
  -e MAX_DISK_USAGE_PERCENTAGE="85" ^
  -e CORS_ORIGINS="" ^
  -e LOCAL_DOWN_ONLY=false ^
  -e OPENSEARCH_JAVA_OPTS="-Xms2G -Xmx2G" ^
  --name logserver ^
  -p 8088:5000 ^
  -v "C:\Users\mgali\LogServer\Config":/app/Config ^
  -v "C:\Users\mgali\LogServer\Data":/app/indexdb ^
  logserver

if %ERRORLEVEL% NEQ 0 (
  echo Failed to start LogServer container.
  exit /b %ERRORLEVEL%
)
echo LogServer container started successfully.
```

Step 2

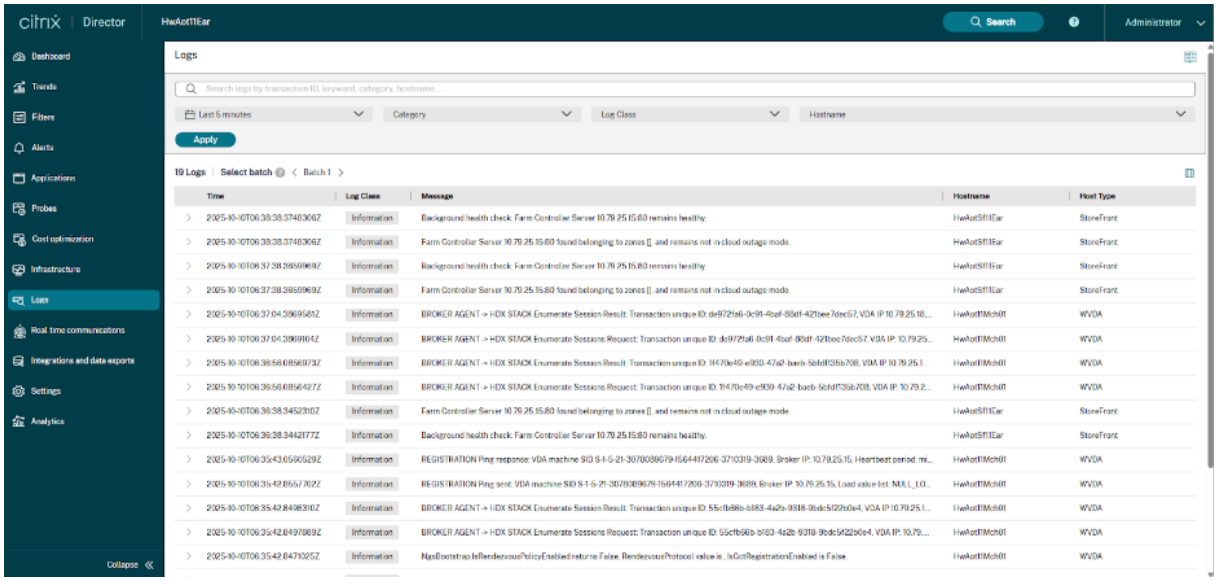
Web Studio provides a dedicated setting that allows **Citrix Director** to connect to the AOT Log Server and display logs in the Monitor console. Once the Web Studio settings are saved, the Delivery Controllers update the site configuration, and Director receives the log server details, including the log server address, port, and authentication key. The director uses these settings to establish a secure connection to the Log Server.

Step 3

After configuration:

1. Open **Citrix Director**.
2. A new **Logs** option appears in the left navigation panel.
3. Select **Logs** and you will see the Get Started page, click on **Close** to skip it, as we have completed these settings earlier.
4. Now, you will see the Director retrieving and displaying AOT logs directly from the Log Server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Logs** page in Director provides a unified view of AOT events from Delivery Controllers, VDAs, StoreFront servers, and other Citrix components. You can search, filter, and inspect logs in real time to troubleshoot issues quickly.

Free-text search: At the top of the Logs page, you'll find a free-text search bar. You can type any keyword to begin narrowing down the results. The search updates the results instantly once you apply filters. Examples include:

- Usernames
- Machine names
- Event keywords (for example, registration, authentication, STA)
- Transaction IDs
- Error messages or partial strings

Time filter: Use the time selector (for example, Last 5 minutes, Last 1 hour, Last 24 hours) to view logs generated within a specific duration. This helps you quickly isolate events around the exact time an issue occurred.

Category filter: The Category field lets you filter logs based on the type of event or subsystem. This helps you focus on logs related to Application launch, Registration, VDA configuration, Graphics, HDX Direct, ICA connection, etc.

Log Class filter: The Log Class filter groups logs by severity or event type. This lets you focus only on errors or important events when troubleshooting. Common classes include:

- Information
- Warning
- Error
- Failure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hostname filter: The Hostname filter lets you select a specific machine —such as a VDA, Delivery Controller, CWA, or StoreFront server. This is useful when you want to drill into logs for a single endpoint or VM instead of searching across the entire deployment.

This centralized access streamlines troubleshooting by allowing for quick log retrieval and analysis from a single console. Learn more about the prerequisites and getting started in Director - Logs.

Accessing Logs via Log Server

The following content is Generate the AuthKey. To enable the access to logs, user needs

1. Modify the `StartLogServer.bat` script **LOCAL_DOWN_ONLY=false**
2. Generate the AuthKey

To keep your logs secure, you'll need an **AuthKey** before downloading them. Here's what to do:

1. **Get your AuthKey** –Use your own role-name/name to generate it.
2. **Run locally** –Scripts can only run on the machine where the Docker container is installed.
3. **Windows users** –Use the `GetAuthKey.bat` scripts instead of shell scripts.
4. **Download logs** –Once authenticated, you can safely retrieve your logs.

Generating and Managing authentication keys for AOT Log Server

You can use the provided .sh (Linux) or .bat (Windows) scripts to quickly generate a new authentication key for a specific role or user. These scripts simplify the process by returning the generated key along with the associated role.

For Linux

```
./GetAuthKey.sh role-name
```

For Windows

```
GetAuthKey.bat role-name
```

The AOT Log Server provides commands to manage authentication keys associated with different roles or users. These commands allow administrators to **add, list, validate**, and **delete** auth keys directly from the container. Use the available docker exec commands directly on the Log Server container.

- **Add a new auth key**: Creates a new auth key for a specified role or user:

```
docker exec logserver /app/authkey add <RoleName>
```

- **List all auth keys**: Displays all existing roles/users for which auth keys are created:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
docker exec logserver /app/authkey list
```

- **Validate an auth key**: Verifies whether a given auth key is valid and identifies the associated role:

```
docker exec logserver /app/authkey validate <key>
```

- **Delete an auth key**: Removes an auth key associated with a specific role:

```
docker exec logserver /app/authkey del <RoleName>
```

- **View command usage**: Displays available options for auth key management:

```
docker exec logserver /app/authkey ??
```

The following example demonstrates how to manage auth keys:

List machine names that have already sent their AOT logs to the logserver

The parameter is the key get from GetAuthKey.sh

For Linux

```
./ListMachines.sh ebac9b7726cb4be597c92c6769134d25
{
 "machines":["MachineName"] }
```

Empty machines means that there has no log

For Windows

```
ListMachines.bat ebac9b7726cb4be597c92c6769134d25
{
 "machines":["MachineName"] }
```

For windows powershell when LogServer starts with "-e LOCAL_DOWN_ONLY=false":

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/
    Download/ListMachine" -Headers @{
  AuthKey = "ebac9b7726cb4be597c92c6769134d25"  }
```

Replace logserver_fqdn with logserver real FQDN, and 8443 with logserver real port. Replace https with http when installed in http mode.

Empty machines means that there has no log

Download logs by Machine name and Time range.

Time is in UTC format:YYYY-mm-ddTHH:MM:SSZ.

```
#Usage: ./DownloadLogsByTime.sh [AuthKey] [MachineName] [StartTime|YYYY
    -mm-ddTHH:MM:SSZ] [EndTime|YYYY-mm-ddTHH:MM:SSZ] [OutputFile]
#Example:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For Linux

```
./DownloadLogsByTime.sh ebac9b7726cb4be597c92c6769134d25 MachineName
    2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
```

For Windows

```
DownloadLogsByTime.bat ebac9b7726cb4be597c92c6769134d25 MachineName
    2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
```

For windows powershell when LogServer starts with "-e LOCAL_DOWN_ONLY=false":

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/
    Download/TimeRange?start=2025-01-01T00:00:00Z&end=2025-01-02T00
    :00:00Z" -Headers @{
  AuthKey = "ebac9b7726cb4be597c92c6769134d25"  }
  -OutFile logs.csv
```

Download logs by keyword/s filter. Time is in UTC format

> **Note:**
>
> - A keyword can be a single word or a combination of words.
> - Keywords can match anywhere within the log message.
> - A **Transaction ID** can also be used as a keyword.

```
#Usage: ./DownloadLogsByWords.sh [AuthKey] [StartTime|YYYY-mm-ddTHH:MM:
    SSZ] [EndTime|YYYY-mm-ddTHH:MM:SSZ] [SearchWords] [OutputFile]
#Example:
```

For Linux

```
./DownloadLogsByWords.sh authkey 2025-01-01T00:00:00.000Z 2025-12-31T23
    :59:59.999Z "session launch" logs.csv
```

For Windows

```
DownloadLogsByWords.bat authkey 2025-01-01T00:00:00.000Z 2025-12-31T23
    :59:59.999Z "failed vda" logs.csv
```

For windows powershell when LogServer starts with "-e LOCAL_DOWN_ONLY=false":

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/
    Download/SearchLog?start=2025-01-01T00:00:00Z&end=2025-01-02T00
    :00:00Z&words=failed vda" -Headers @{
  AuthKey = "ebac9b7726cb4be597c92c6769134d25"  }
  -OutFile logs.csv
```

Words are separated by space

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AOT Logs availability across deployment scenarios

May 29, 2026

This table shows how AOT (Always On Tracing) log collection happens across different deployment scenarios. It highlights which components can send logs to the AOT Log Server based on the architecture used, including **on-prem, Gateway-based, cloud, and hybrid deployments**.

Use Case	Deployment Scenario	CWA	StoreFront (On-Prem)	Citrix Workspace (Cloud)	Gateway (On-Prem)	Citrix Gateway service	DDC (On-Prem)	Cloud DDC	Cloud Connector	VDA	FAS	PVS	Other Components
1	On-Prem Direct Access (StoreFront + on-prem DDC)	Yes	Yes	N/A	N/A	N/A	Yes	N/A	N/A	Yes	Yes	Yes	Yes
2	On-Prem via Gateway (StoreFront + on-prem DDC + Gateway)	Yes	Yes	N/A	Yes	N/A	Yes	N/A	N/A	Yes	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use Case	Deployment Scenario	CWA	StoreFront (On-Prem)	Citrix Workspace (Cloud)	Gateway (On-Prem)	Citrix Gateway service	DDC (On-Prem)	Cloud DDC	Cloud Connector	VDA	FAS	PVS	Other Components
3	Fully Cloud (Citrix Workspace + Cloud DDC + Citrix Gateway service)	Coming Soon	N/A	Yes*	N/A	Yes*	N/A	Yes*	Yes	Yes	Yes	Yes	Yes
4	Hybrid Cloud (Citrix Workspace + Cloud DDC + Gateway)	Coming Soon	N/A	Yes*	Yes	N/A	N/A	Yes*	Yes	Yes	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use Case	Deployment Scenario	CWA	StoreFront (On-Prem)	Citrix Workspace (Cloud)	Gateway (On-Prem)	Citrix Gateway service	DDC (On-Prem)	Cloud DDC	Cloud Connector	VDA	FAS	PVS	Other Components
5	Hybrid Cloud (StoreFront + Cloud DDC + Gateway)	Coming Soon	Yes (Manual Configuration Required)	N/A	Yes	N/A	N/A	Yes*	Yes	Yes	Yes	Yes	Yes

Note:

- **Yes** → Component supports uploading logs to the AOT Log Server
- **Yes*** → Logs are available, but they are handled and stored through Citrix-managed service instead of the customer-managed AOT Log Server
- **Manual Configuration Required** → Manual setup is required for log upload to the Log Server
- **Coming Soon (CWA)** → Indicates current gap in direct log upload from Citrix Workspace app (work in progress)

General Response Code for Log Server API

December 4, 2025

This table outlines the standard HTTP response codes used by the Log Server's API to communicate the result of client requests. These codes help clients understand whether their requests were successful or if errors occurred, and what kind of errors were encountered. Understanding these response codes is crucial for diagnosing issues, debugging API calls, and ensuring smooth integration with the Log Server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error Code	Status	Description
200	OK	The request was successful.
400	Bad request.	The server could not process the request due to missing parameters, malformed syntax, or absence of required HTTP headers. For example, if fields like MachineName or Role are missing in the request headers, this response is triggered.
401	Not Authorized.	The request was denied because the client is not authorized. This usually occurs when the IP address or the authentication key (AuthKey) used is not permitted to access the Log Server.
404	Not found.	The API path requested does not exist. This response is returned when the endpoint is invalid or mistyped.
500	Internal error.	Indicates that the Log Server encountered an unexpected condition preventing it from fulfilling the request. This is commonly caused by server-side issues such as resource exhaustion (e.g., memory or disk space).

Troubleshoot Common Issues with Always On Tracing

August 4, 2026

Applies to: Citrix Virtual Apps and Desktops 2402 CU4, 2507 CU1, 2511, 2603 and later, DaaS

Requires: AOT Log Server deployed; AuthKey configured in Director or Monitor settings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

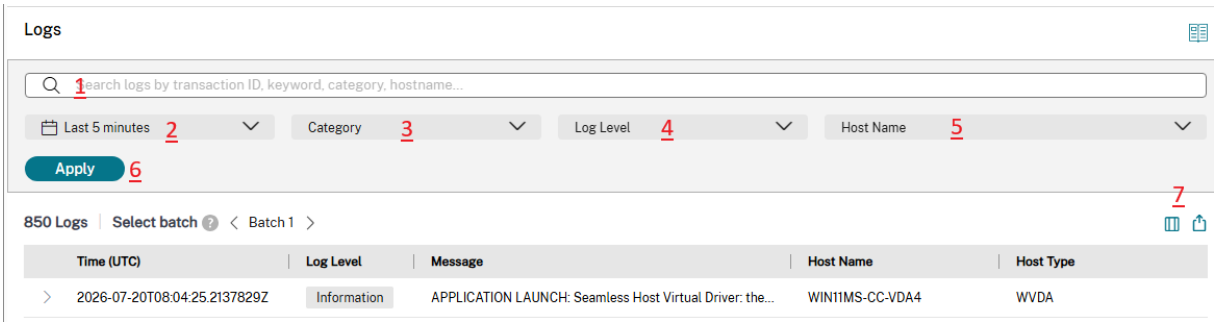
Always On Tracing (AOT) captures logs continuously across all Citrix components —VDAs, Delivery Controllers, StoreFront, License Server, and Citrix Workspace App. When a problem is reported, the data is already there. This article shows how to use the **Logs** node in Citrix Director or Monitor to identify the cause of an issue and how to export logs from Director or Monitor for submission to Citrix Technical Support.

Before you start —collect this for every scenario

- **Affected user or machine** —a specific username, VDA hostname, or delivery group name
- **Time of failure** —even an approximate window helps narrow the default time filter. Adjust the time range to cover the period before the reported failure.
- **Scope** —one user, one machine, or environment-wide? Scope alone often points to the correct failure pattern before you open a log
- **Recent changes** —any CVAD updates, Group Policy changes, power management changes, or network changes in the relevant window

The Logs node in Director and Monitor

The Logs node is available in both **Citrix Director** (on-premises CVAD) and **Citrix Monitor** (DaaS). To access it, select **Logs** from the left navigation panel. The interface is the same in both environments.



1. **Search bar** —keyword, transaction ID, category, or hostname
2. **Time filter** —select the window that covers the failure
3. **Category filter** —filter by event type
4. **Log Level filter** —filter by severity
5. **Host Name filter** —select one or more machines
6. **Apply button** —applies all active filter selections
7. **Export icon** —download logs to submit to Citrix Technical Support

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter bar

The filter bar has four filters and a separate **Apply** button. Set the filters first, then click **Apply** to refresh the log view. The current log count appears below the filter bar —for example, *850 Logs in Batch 1*. Use the batch navigation arrows to page through large result sets.

Filter	What it does	Options
Time	Sets the time window for log retrieval. Set this to a window that starts before the reported failure to capture the events that led up to it.	Last 5 minutes ·Last 1 hour ·Last 24 hours ·Last 48 hours ·Last 7 days ·Custom (UTC) *(CVAD 2603 and later cloud release only)*
Category	Filters by event type. Each category corresponds to a specific part of the Citrix component lifecycle. Includes a Search Category field to quickly find a category by name.	Application Launch ·Clipboard · CWA-PostLaunch · CWA-PreLaunch ·Database · Devices ·and more
Log Level	Filters by severity. Select one or more. When a selection is active, the button label shows the number selected (for example, *1 Log Level Selected*).	Information ·Warning ·Error · Critical
Host Name	Filters to one or more specific machines. Includes a Search Host field and a checkbox list of all machines currently sending logs to the Log Server. When active, shows *N Hostname Selected*.	All machines registered with the Log Server

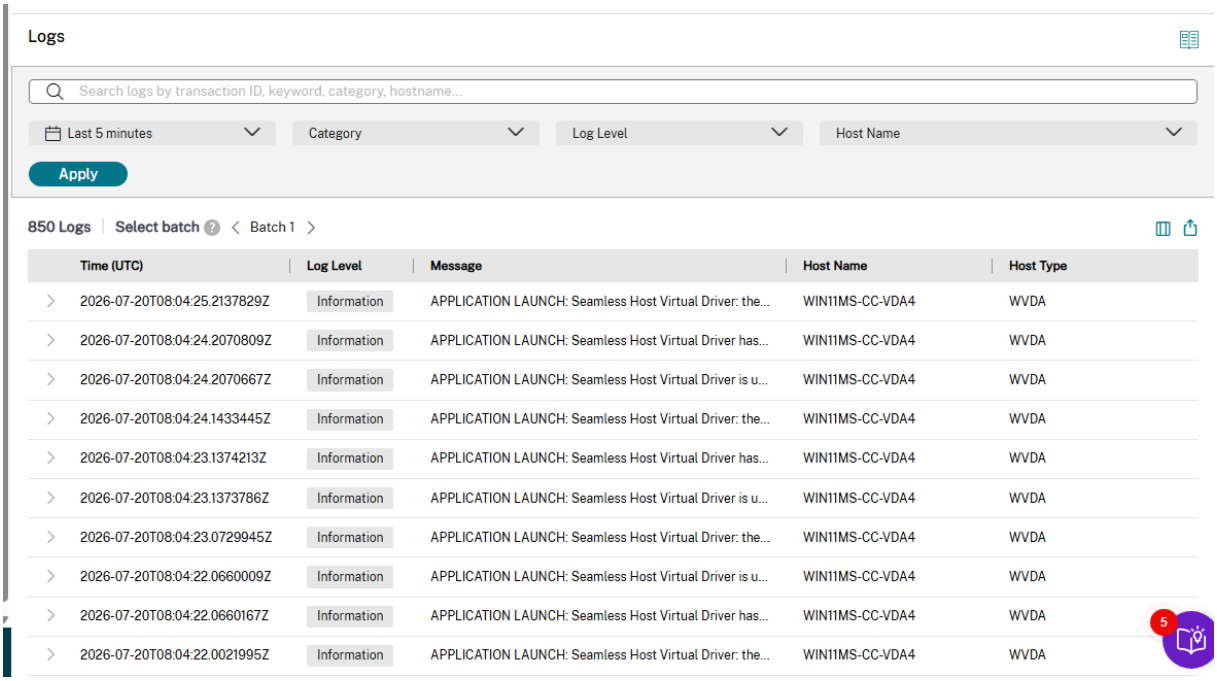
Log Level	When to use it
Information	Standard component events —session started, VDA registered, license checked out. Use to see the full lifecycle sequence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log Level	When to use it
Warning	Non-critical issues that may indicate a problem —session disconnects, idle timeouts, heartbeat warnings. **Start here for disconnect scenarios.**
Error	Failures requiring investigation —launch errors, registration failures, license exhaustion. **Start here for most scenarios.**
Critical	Severe failures affecting service —typically component crashes or unrecoverable states

Log table —columns

The log table shows five columns by default for each entry. New columns can be added by clicking the Column button. Click the **>** expand arrow on any row to see the full log message and additional fields.



*The Logs table with Application Launch category active. The log count and batch navigation appear above the table. Expand any row with the **>** arrow to read the full message.*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	What it shows
Time (UTC)	Timestamp of the event in UTC, with millisecond precision. Sort ascending to read a sequence of events in the order they occurred.
Log Level	Severity badge: Information, Warning, Error, or Critical
Message	The log message from the component. Truncated in the table —click the **>** expand arrow on the row to read the full message. The full message is the primary diagnostic text.
Host Name	The machine that generated the log entry
Host Type	The component type: DDC, StoreFront, WVDA (Windows VDA), CWAWindows, and others depending on what is registered with the Log Server

Exporting logs for Citrix Technical Support

The export icon (**7** in the annotated screenshot above) appears at the top right of the Logs section. Use it to download the current filtered log view as a file. Before exporting:

> **Version availability:**
>
> The export icon is available on DaaS from the Cloud 129 (April–May 2026) release and later, and on Citrix Virtual Apps and Desktops from CVAD 2603 and later. The option is not available on earlier versions.

> **AuthKey required:**
>
> The Logs node only shows data if the AuthKey is configured in Director or Monitor settings. The AuthKey is generated during Log Server setup. Without it, the Logs node shows no entries.

Scenario 1: Session launch failure

A user clicks a published desktop or application and gets a launch error. The session never opens. The error may appear on the Citrix Workspace App screen or the progress bar stalls and times out with no session connecting.

In the Logs node, set **Category** to **Application Launch**, **Log Level** to **Error**, and adjust **Time** to cover the failure window. Click **Apply**. Sort by **Time (UTC)** ascending and read the **Message** and **Host Type**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

columns together —they show which component in the launch path failed and what it reported.

> **Reference only:**
>
> The log messages below are illustrative examples. Actual messages in your environment follow the same format and column structure but may differ in exact wording.

Example: No VDA available in the delivery group

The DDC received the launch request but could not assign a desktop. All VDAs in the delivery group were unregistered or at session capacity.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:14:22.1034Z	Information	APPLICATION LAUNCH: User DOMAIN\jsmith requested Desktop from delivery group 'Windows 11 VDAs'	DDC-01	DDC
2026-07-20T09:14:22.3841Z	Error	APPLICATION LAUNCH: No suitable desktop found —all VDAs in delivery group 'Windows 11 VDAs'are unregistered or at session capacity	DDC-01	DDC
2026-07-20T09:14:22.4102Z	Error	APPLICATION LAUNCH: Launch failed for user DOMAIN\jsmith —no resources available	STF-01	StoreFront

The Error from DDC tells you the broker could not find an available VDA. Check VDA registration in Web Studio → Search Machines. See Scenario 2: VDA registration failure for VDA registration troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example: VDA assigned but session initialization failed

The DDC assigned a VDA but the VDA could not start the session. Common causes: FSLogix or roaming profile container failure, Group Policy processing error, or VDA resource exhaustion.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:22:11.0234Z	Information	APPLICATION LAUNCH: VDA WIN11MS-CC-VDA4 selected for user DOMAIN\jsmith	DDC-01	DDC
2026-07-20T09:22:11.8820Z	Error	APPLICATION LAUNCH: Session initialization failed for user DOMAIN\jsmith —FSLogix profile container could not be mounted at \file-server\profiles\jsmith.vhdx	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:22:12.0011Z	Error	APPLICATION LAUNCH: Launch request failed — VDA WIN11MS-CC-VDA4 reported session preparation error for user DOMAIN\jsmith	DDC-01	DDC

The Error from Host Type WVDA identifies the VDA as the failure point and the Message shows the exact cause. Click the **>** expand arrow on that row to read the full message, which includes the full profile container path and error code.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example: Virtual channel error during CWA post-launch

The session was created on the VDA side but the CWA client could not establish the ICA virtual channel connection. Filter **Host Name** to the CWA machine to see client-side errors.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:31:04.5521Z	Information	APPLICATION LAUNCH: Seamless Host Virtual Driver has been initialized successfully	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:31:05.1204Z	Error	CWA-POSTLAUNCH::VIRTUAL CHANNEL: Failed to load virtual driver —channel negotiation timeout. Check firewall rules for ports 1494 and 2598.	Win22-CC-01	CWAWindows

Host Type CWAWindows with a CWA-POSTLAUNCH error means the VDA was ready but the ICA data path between client and VDA was blocked. Verify ports 1494 and 2598 are open from the client machine to the VDA.

Scenario 2: VDA registration failure

VDAs show as **Unregistered** in Director or Web Studio → Search Machines. Users see "No desktops are available to you at this time."Published desktops appear greyed out in StoreFront or Citrix Workspace.

In the Logs node, set **Category** to **VDA registration**, **Log Level** to **Error**, and set **Host Name** to both the affected VDA and the DDC. Click **Apply**. Reading both sides of the registration handshake together —the VDA row and the DDC row at the same timestamp —shows exactly where the failure occurred.

> **Reference only:**
>
> The log messages below are illustrative examples. Actual messages in your environment follow

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> the same format and column structure but may differ in exact wording.

Example: VDA cannot reach the Delivery Controller

The VDA is attempting to register but the DDC never receives the request. Only VDA-side errors appear —no matching DDC rows at the same timestamps.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T08:30:11.2341Z	Error	REGISTRATION: Failed to contact Delivery Controller DDC-01.domain.com on port 443 — connection timed out	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:30:41.2341Z	Error	REGISTRATION: Failed to contact Delivery Controller DDC-01.domain.com on port 443 — connection timed out	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:31:11.2341Z	Error	REGISTRATION: Failed to contact Delivery Controller DDC-01.domain.com on port 443 — connection timed out	WIN11MS-CC-VDA4	WVDA

The same error repeating at a fixed interval is a retry loop —the VDA is alive but blocked. Verify ports 80 and 443 are open from the VDA to the DDC, and check the `ListOfDDCs` registry key on the VDA for stale or incorrect DDC addresses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example: DDC rejects the registration request

The VDA reached the DDC but the DDC refused to register it. Both VDA and DDC rows appear —read the DDC Message for the rejection reason.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T08:30:11.2341Z	Information	REGISTRATION: VDA WIN11MS-CC-VDA4 attempting to register with DDC-01.domain.com	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:30:11.8820Z	Error	REGISTRATION: Registration rejected — machine account WIN11MS-CC-VDA4$ is disabled or not found in Active Directory	DDC-01	DDC

The Error row comes from Host Type DDC —the DDC is the failure point, not the VDA. Click the **>** expand arrow on the DDC row to read the full rejection reason. Common reasons: disabled machine account in Active Directory, VDA/DDC version mismatch, or license pool exhaustion.

Example: VDA registers then immediately deregisters

Registration succeeds but the DDC initiates deregistration within seconds. This repeats in a loop. A power management drain policy is shutting the VDA down before it can accept sessions.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:01:33.1240Z	Information	REGISTRATION: VDA WIN11MS-CC-VDA4 registered successfully with DDC-01.domain.com	WIN11MS-CC-VDA4	WVDA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:01:47.4421Z	Error	POWER MANAGEMENT: PowerManagementDrain initiated — machine scheduled for shutdown by delivery group power policy	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:01:47.6830Z	Error	REGISTRATION: VDA WIN11MS-CC-VDA4 deregistered — reason: power management drain	DDC-01	DDC

The 14-second gap between registration and deregistration is the tell. Check Web Studio → Delivery Group → Power Management for a drain or shutdown schedule that is applying during business hours.

> **Note:**
>
> The scenarios in this article are examples of how to search and investigate logs in Citrix Director or Monitor. The same methodology applies to any Citrix-related issue you encounter —session failures, authentication errors, connectivity problems, VDA instability, or any other component-level issue. Set the right **Category**, **Log Level**, and **Host Name** filters, read the log sequence in **Time (UTC)** order, and expand individual rows to read the full **Message**. The component that logged the first error and what the Message says will point you to the root cause —regardless of the scenario.

> **Tip —DaaS customers with Citrix Aidrien access:** Copy the error message from the AOT log and paste it directly into Citrix Aidrien. Aidrien will explain the error and provide recommended troubleshooting steps. This may not resolve every issue on its own, but it will narrow down the root cause and in many cases guide you to a fix —before you need to contact Citrix Technical

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Support.

Escalating to Citrix Technical Support

If self-service investigation does not resolve the issue, include the following when opening a support ticket:

- **Exported log file covering the failure window** —use the export icon described in option 7 above. You can export in two ways depending on what you have:
  - **Targeted export** —apply Time, Category, and Host Name filters, then export. This gives Support a focused log set scoped to the failure.
  - **Broad export** —apply only the Time filter and export without any other filters. This gives Support the full log picture for the failure window and is useful when the scope is unclear.

  When the file downloads, the filename is prefixed with **AOT**. Do not remove or rename this prefix. You can edit the portion of the filename that follows —but always retain **AOT** at the beginning.
- The failure pattern identified from the sections above
- CVAD version, component versions (VDA, DDC, StoreFront), and Log Server version
- The transaction ID or session ID of the failed event —searchable in the Logs node search bar using the placeholder: *"Search logs by transaction ID, keyword, category, hostname"*

Because AOT captures logs continuously and every entry includes Host Name, Host Type, and timestamp, Citrix Technical Support can begin analysis immediately without asking you to reproduce the issue or collect new traces.

FAQ

July 13, 2026

1. **How can I check the running log server configurations, like MAX_RESERVE_DAYS?**

   You can check the container environment values using either of the following commands:

   ```
   docker inspect logserver |findstr MAX_RESERVE_DAYS
   ```
   Or by checking the container environment:
   ```
   docker exec -it logserver env |grep MAX_RESERVE_DAYS
   ```

   If nothing is returned, it means the log server is using the default value:
   MAX_RESERVE_DAYS=7

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Do I need to purchase Docker Desktop licenses when installing the log server container image on Windows?**

   Yes. A valid Docker Desktop license is required.

3. **Should I use a new server for log server installation?**

   Yes. It is recommended to use a dedicated server for the log server installation to ensure performance and isolation.

4. **What is the sustained ingest capacity of a single AOT Log Server? What are the maximum and safe Events-Per-Second (EPS) limits?**

   A single AOT Log Server supports a sustained ingest capacity of **10,000 events per second (EPS)**. This value represents both the **maximum** and the **safe operating threshold** for continuous ingestion.

5. **How many components can a single AOT Log Server handle? Is there a maximum limit?**

   A single Log Server can connect up to 128,000 components, but it can only process about 10,000 logs per second. So the number of machines is rarely the issue —the real sizing factor is how many logs your users generate during peak activity.

6. **What is the burst tolerance of the AOT Log Server? How much sudden log spike can it handle without loss or backlog breach?**

   The AOT Log Server can handle short-term bursts of up to **2× the normal event rate** without losing logs. If log volume spikes beyond this (for example, 5×), the system will not be able to persist events reliably, and **OpenSearch will start dropping logs** because it cannot index them fast enough.

7. **Can the AOT Log Server compress logs? What compression ratio should we expect?**

   Yes. The AOT Log Server uses the default **LZ4 compression algorithm** for storing logs in OpenSearch. The typical compression ratio is approximately **2:1**, meaning log data is reduced to less than half its original size while maintaining fast read/write performance.

8. **For each infrastructure type (single-site on-prem, multi-site on-prem, single-region cloud, multi-region cloud, hybrid, MSP/tenant), where should the AOT Log Server be deployed and why?**

   The AOT Log Server should always be deployed **in the same line of sight as the VDAs**. This ensures stable connectivity and helps maintain low latency between the components generating logs and the log server that ingests them. As long as every component (VDAs, DDCs, StoreFront, Gateway, etc.) can reliably reach the log server, the environment will function correctly.

9. **Do we need one log server per region, or can everything be centralized? What about latency and egress?**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can centralize the log server, but customers should evaluate the **latency** and **egress cost** implications for their environment. The **latency between regions may affect log ingestion**, especially during high-volume periods. If the round-trip latency is high, spikes or bursts of logs may cause delays, backlog build-up, or potential loss during peak loads. Egress charges may apply when logs cross regional or cloud boundaries.

10. **Does AOT consume significant network bandwidth or system resources?**

    No. AOT is designed to have minimal impact on endpoint, VDA or any component, and network performance.

    AOT collects logs continuously and uploads them to the AOT Log Server in near real-time over HTTPS. Individual log records are typically very small in size (often only a few kilobytes), which helps minimize network overhead during normal operation.

    The overall bandwidth consumed depends on the number of active sessions, enabled components, and environment activity. In most deployments, AOT log traffic represents a very small percentage of overall network utilization.

    AOT also uses compression to reduce storage requirements and optimize data transfer to the Log Server.

11. **What are the minimum hardware specifications for supporting 1,000 machines with the AOT Log Server?**

    For environments with up to **1,000 machines**, you need: **1 node** (Log Server + OpenSearch combined), **4 vCPUs, 8 GB RAM, 2,000 IOPS** minimum (SSD or NVMe recommended), **1 Gbps NIC**. This setup is suitable for small or single-site deployments with moderate log volume.

12. **How can I troubleshoot if there is a problem with the Log Server?**

    LogServer is running as a docker container, so all docker commands could be used to find the issues:

    ```
    1 docker logs logserver
    2 docker inspect logserver
    ```

    And also, user could attach into the running container and view logs of logserver self:

    ```
    1 docker exec  – it logserver bash
    ```

    In the logserver docker container bash shell, user can verify the health of logserver and opensearch:

    ```
    1 curl http://localhost:5000/Ping
    2 curl http://localhost:9200/_cluster/health?pretty
    ```

    And check logs inside the container:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
tail Config/applogs.txt
tail Config/weblogs.txt
```

If need more logs, user could modify the LOG_LEVEL=0 in StartLogServer.sh/StartLogServer.bat and restart the logserver by these script files. Then the detailed logs will include TRACE, DEBUG, INFO, WARN, ERROR all levels.

13. **Recover from an improperly detached Log Server storage disk**

    If you remove or detach the Log Server storage disk directly from the **hypervisor** or **cloud provider** without first detaching it from the Citrix Connector Appliance administration UI, the Connector Appliance retains the storage configuration and assumes that the disk is still attached. As a result, the previously attached disk remains configured in the Connector Appliance, attaching a new disk fails, and you may see an error similar to: **A local disk is already mounted to the provider**.

    Option 1 (Recommended): If the original disk is still available:

    a) Reattach the original disk to the Connector Appliance VM from the hypervisor or cloud provider.

    b) Reboot the Connector Appliance.

    c) After the appliance starts successfully, detach the disk using the Connector Appliance administration UI.

    d) You can now attach a new disk if required.

    Option 2: If the original disk is no longer available, manually remove the stale storage configuration by executing the following API request. Retrieve an Authorization token and run the appropriate command:

    Linux:

    ```
    curl -X POST "https://<connector-fqdn>/storage/$detach" \
    -H "Content-Type: application/json" \
    -H "Authorization: Bearer <token>" \
    -d '{
     "targetProvider":"logserver-provider","storageType":"local" }
     '
    ```

    Windows:

    ```
    curl -X POST "https://<connector-fqdn>/storage/$detach" ^
    -H "Content-Type: application/json" ^
    -H "Authorization: Bearer <token>" ^
    -d "{
     \"targetProvider\":\"logserver-provider\",\"storageType\":\"local
        \" }
     "
    ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The API may return an error even though the stale storage configuration is successfully removed. Verify the storage configuration before retrying the disk attachment.

As a best practice, always detach the Log Server storage disk from the Connector Appliance administration UI before removing or detaching the disk from the hypervisor or cloud provider. This ensures that the Connector Appliance cleans up its storage configuration and prevents stale storage references.

Known Issues and Limitations

July 13, 2026

- **Only One Log Server Is Supported Per Environment**

  The current architecture supports only a single AOT Log Server per environment, and both Web Studio and Director/Monitor are designed to work with only one Log Server configuration. All components must point to this same Log Server; configuring or distributing workloads across multiple Log Servers is not supported today. This single Log Server can handle up to 128,000 active component connections and process up to 10,000 log events per second, which is sufficient for most deployments. Since these limits are based on connection capacity and log-throughput, not on the number of components, even very large environments can operate with one Log Server as long as they remain within throughput thresholds.
  However, customers with extremely high log volumes during peak activity may reach ingestion or indexing limits due to the absence of horizontal scaling. Support for multiple Log Servers and broader scaling options will be introduced in future releases as part of the evolving architecture.

- Running the AOT Log Server on a **Windows VM hosted on XenServer** is **not supported.**
  XenServer does not support nested virtualization, which prevents Docker from running inside the guest VM. As a result, the Log Server container cannot be deployed in this configuration.

- **Docker Desktop on Windows requires an active user session for AOT Log Server**

  When the AOT Log Server is deployed on a Windows VM using Docker Desktop, the container runs within the context of the user session that started Docker Desktop. Docker Desktop is designed as a user-session-based application and does not run as a system-level service on Windows. As a result, if the user logs out, Docker Desktop stops, which causes the AOT Log Server container to stop. Because of this behaviour: The AOT Log Server stops when the user logs out as the deployment depends on a specific user session. Other administrators cannot access or manage the running containers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workaround: Keep the user session active or in a disconnected state (do not log out) to ensure that Docker Desktop and the AOT Log Server container continue running.

Recommendation For production deployments, use one of the following:

- Deploy the AOT Log Server on a Linux VM using Docker Engine
- Use the Citrix Connector Appliance (CCA)-based deployment where supported

These options allow the Log Server to run independently of user sessions and provide a more reliable, always-on deployment model.

> **Note:**
>
> This approach may not be reliable in environments with session timeouts or strict security policies.
>
> This behaviour is a known limitation of Docker Desktop on Windows and is not specific to the AOT Log Server.

- **License Server logs appear with incorrect Host Type in Director/Monitor**

  When viewing AOT logs from the License Server in Director, the **Host Type** column may incorrectly display the value as **DDC** instead of **License Server**, even though the hostname is correct.

  This issue is limited to how the Host Type is represented in Director and does not impact log collection or functionality. This issue has been resolved in the latest License Server release and is fixed starting from **License Server version: 55000 or later**.

- **Citrix Cloud Connector is required to view AOT logs in Monitor**

  Customers using **Citrix Monitor** to view AOT logs must have at least one **Citrix Cloud Connector** deployed in their environment. This requirement applies regardless of where the AOT Log Server is hosted, including Linux VM or Windows VM or Citrix Connector Appliance

  Citrix Monitor relies on the **Monitor service running on the Cloud Connector** to retrieve logs from the configured Log Server and display them in the UI.

  Without a Windows Cloud Connector, AOT logs cannot be fetched or displayed in Monitor.

- **ADC Gateway logs display incorrectly in Citrix Director**

  Symptoms: When viewing Always On Tracing (AOT) logs for Citrix ADC Gateway in Citrix Director, you might observe:

  - Log Level displayed as **Error** instead of **Debug** or **Info**.
  - The **Message** column shows the entire raw log entry.
  - The displayed timestamp differs from the original event timestamp.
  - Only malformed JSON log records are affected. Valid log records display correctly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Affected versions: Citrix ADC earlier than **14.1-73.x** and Citrix ADC earlier than **15.1-8.x**.

Cause: Citrix ADC Gateway uploads malformed JSON log records that cannot be parsed by the AOT Log Server. As a result, the Log Server stores the raw log entry and classifies it as an error.

Resolution: Upgrade Citrix ADC to one of the following versions or later:

- 14.1-73.x
- 15.1-8.x

Fixed in: Citrix ADC **14.1-73.x** and Citrix ADC **15.1-8.x**.

- The AOT Log Server does not currently support **FIPS-compliant deployments**. Customers with mandatory FIPS requirements should defer production deployment until FIPS support becomes available.

  Customers who do not require FIPS compliance may continue to deploy and evaluate the AOT Log Server in supported environments.

Third party notice

December 4, 2025

This release of Citrix AOT Log Server may include third-party software licensed under the terms defined in the following documents:

- Citrix Centralized Log Server Third Party Notices

Introduction

December 4, 2025

Always On Tracing (AOT) is a modern diagnostic framework from Citrix designed to continuously capture relevant log data across the Citrix Virtual Apps and Desktops (CVAD) environment. Always on Tracing (AOT) is a subset of CDF traces that can be helpful when troubleshooting common failures (for example, VDA registrations and application/desktop launches).
Unlike traditional tools that require manual intervention, AOT runs in the background by default, ensuring that critical information is available when issues occur, even if the problem cannot be reproduced.

AOT is built to simplify troubleshooting for IT administrators and Citrix® support teams to improve the mean-time-to-resolution by:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

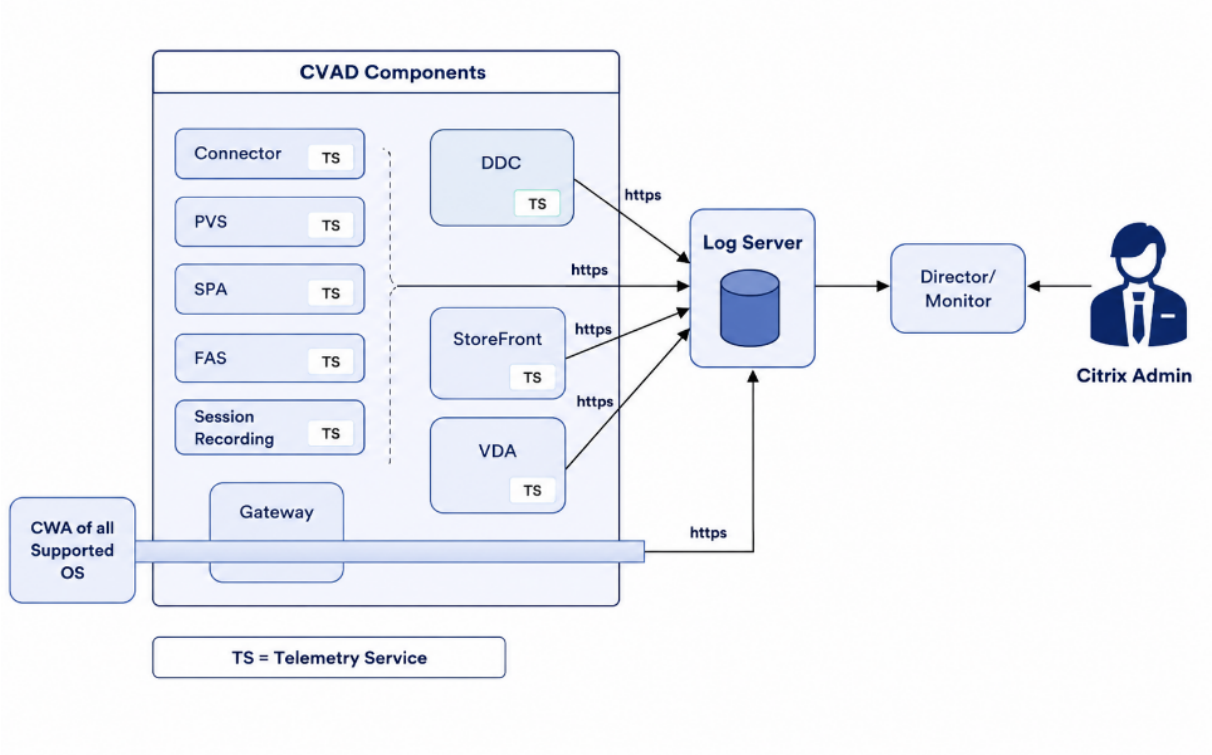
- Automatically capturing log data for user sessions and system events.
- Eliminating the need to reproduce issues.
- Making logs easily accessible and readable without engineering-level expertise.
- Enabling self-service diagnostics to reduce dependency on Citrix Support.

Key Benefits

- Faster MTTR (Mean Time to Resolution)
- Always-on, no manual trace initiation needed
- Self-diagnosis for common issues
- Streamlined escalation to Citrix Support with full context
- Secure, compliant log handling with sensitive data redaction

Architecture Overview

December 4, 2025



The Always On Tracing (AOT) architecture is designed to provide continuous, real-time trace collection across the Citrix Virtual Apps and Desktops™ (CVAD) environment. It enables IT administrators and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Support to troubleshoot user and infrastructure issues without requiring manual trace initiation or issue reproduction.

The AOT system is built on several integrated components working in sequence to capture, transfer, and store telemetry logs from multiple Citrix infrastructure layers into a centralized repository.

Key Components and Workflow

1. **AOT Log Generators (Citrix Core Components):** Citrix components such as the Virtual Delivery Agent (VDA), Delivery Controller™ (DDC), StoreFront, and others act as log generators. These components are equipped with the Telemetry Service, which uses the AOT API to capture trace data, record pre-defined step traces, and log error events relevant to user sessions and transactions.
2. **Enable Log Collection:** When an administrator initiates a request to collect logs (typically through a powershell command), instructions are sent to the broker, which orchestrates the log collection process across the relevant components, including broker and VDA; the administrator initiates the request to collect logs (through a powershell command) from Storefront™ Server separately.
3. **Telemetry Service:** After configuring the Log Server address and port in Storefront and DDC, the Telemetry Service then activates the new real-time AOT listener, which collects logs based on predefined events, failures, or trigger points.
4. **Log Transfer to Centralized Log Server:** Once the logs are collected, the Telemetry Service transfers them securely to a centralized log server directly. In environments where endpoints are connected from external networks through a Citrix Gateway, the transfer typically occurs over a SOCKS tunnel to ensure secure and seamless transfer.
5. **Log Storage and Organization:** The Centralized Log Server receives, parses, and stores the AOT logs in a structured and searchable format using an indexed database backend (OpenSearch by default). Logs are tagged by session, component, and timestamp, enabling easy access and efficient troubleshooting.

Logs in the Citrix AOT system are stored in a structured and searchable format, tagged with various fields to enable easy access and efficient troubleshooting. These tags include:

- **MachineName:** The name of the machine where the log originated.
- **MachineIP:** The IP address of the machine.
- **Role:** The role of the Citrix component (e.g., VDA, DDC, StoreFront).
- **TimeStamp:** The UTC timestamp when the log event occurred.
- **Message:** The actual log message content. Could be searched/filtered by words.
- **Level:** The severity level of the log (e.g., info, warning, error).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Module:** The specific software module that generated the log.
- **ProcessName:** The name of the process that generated the log.
- **ProcessId:** The ID of the process.
- **Thread:** The thread ID within the process.
- **Cpu:** Information related to CPU id at the time of the log.
- **SessionId:** The ID of the user session associated with the log.
- **Class:** The class or component within the module.

These detailed tags allow administrators to quickly filter, search, and analyze logs based on specific criteria, facilitating the identification and resolution of issues.

In summary, the AOT workflow begins with Citrix components generating diagnostic logs. A centralized request is initiated to collect these logs, which the Telemetry Service gathers from the relevant components. The collected logs are then securely transferred to a centralized log server for indexing, storage, and later analysis.

How AOT Works

Citrix Always On Tracing (AOT) continuously captures diagnostic data from key components in your environment. When triggered, logs are collected automatically, securely transferred to a centralized log server, and retained for analysis. This eliminates the need for manual tracing and simplifies troubleshooting.

Tracing Triggers and Log Collection: Citrix components such as VDA, DDC, StoreFront and other components are equipped with the AOT API to track critical steps and errors. These components serve as AOT log generators. When an administrator initiates a log collection request from the Delivery Controller:

The DDC sends the instruction to relevant Citrix components. Each component forwards the request to its local Telemetry Service.

The Telemetry Service starts the real-time AOT listening program to collectAOT logs, and forwards the logs to the Centralized Log Server.

Log Storage and Retention: Once the AOT logs are received, the Centralized Log Server formats and indexes them into a structured, searchable database. Logs are retained based on a defined retention policy to optimize storage usage. By default, AOT logs are retained for 7 days, after which they are automatically purged to conserve space.

AOT vs Traditional Logging

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Aspect	AOT	Traditional CDF Tracing
Activation	Automatic, continuous	Manual, issue reproduction required
Complexity	User-friendly, readable logs	Engineering-level parsing
Diagnostic Speed	Immediate logs available	Delayed by reproduction effort
Resource Usage	Low overhead with optimized buffers	Moderate to high if used incorrectly

Traditional tracing tools require manual effort and only work if you catch the problem while it's happening. With Always On Tracing (AOT), logging runs continuously in the background, so issues are captured as they happen —even if you're not watching. This saves time and makes troubleshooting much easier.

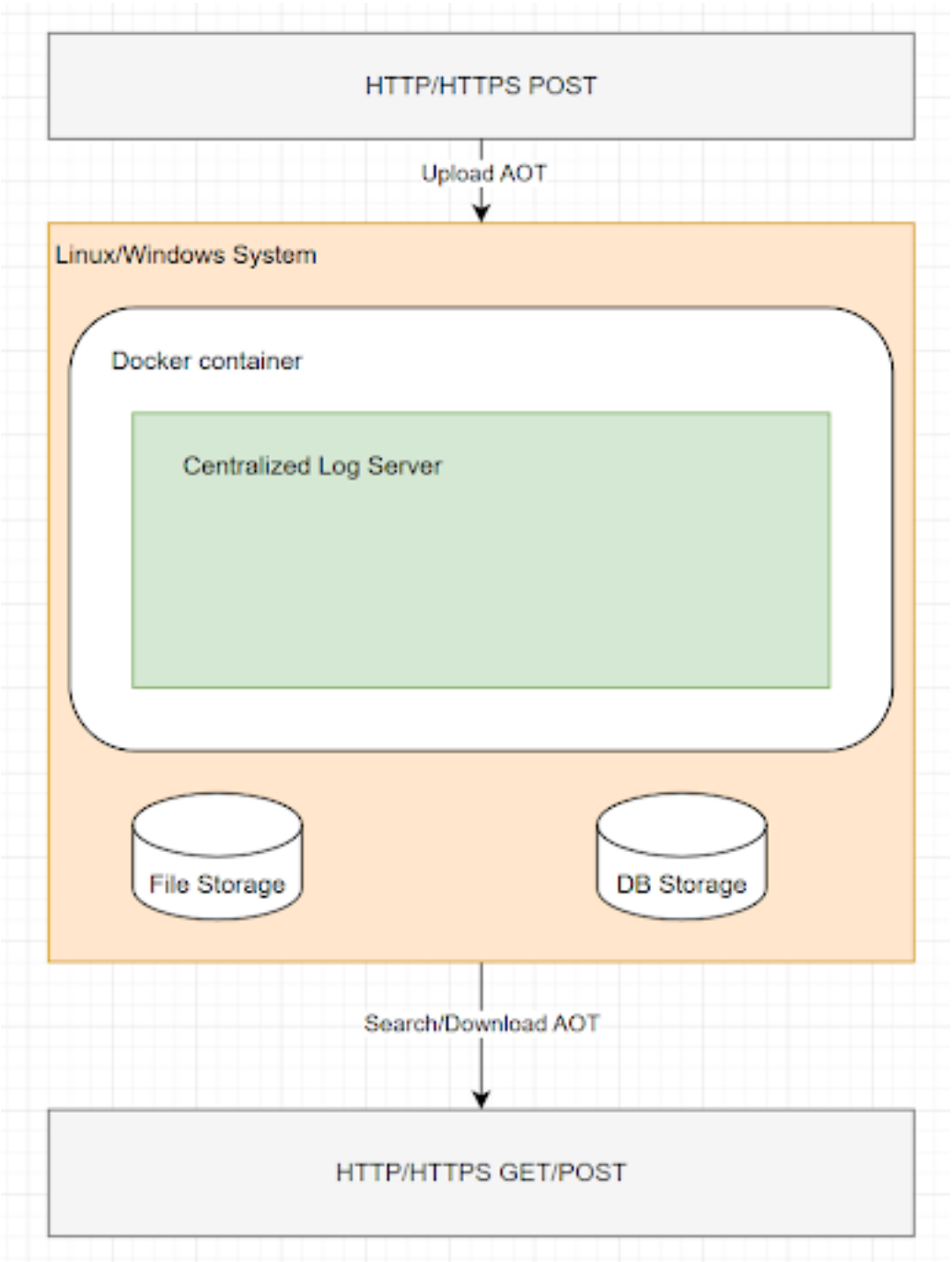
AOT Highlights

- **Always On:** Tracing runs all the time, no need to turn it on manually.
- **Auto Capture:** Logs are collected always when issues occur.
- **Central Log Server:** All logs are stored in one place for easy access.
- **Easier Troubleshooting:** Helps quickly pinpoint common failures.
- **No Reproduction Needed:** No need to recreate the issue, it's already captured.

Centralized AOT Log Server

December 4, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The AOT Log Server acts as a centralized destination for collecting and storing Always On Tracing (AOT) logs from various Citrix® components. It is containerized using Docker technology and is preferably deployed on Linux, though it also supports Windows environments via Docker Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key Features of the AOT Log Server

- **Centralized Log Storage:** Aggregates diagnostic logs from multiple Citrix components into a unified and searchable location.
- **Retention Policy:** Logs are retained based on a configurable policy (default: 7 days) to optimize storage usage and performance.
- **Deployment:** The Log Server is deployed using packaged installer scripts and Docker containers. The setup requires compatible hardware and a Docker runtime environment.
- **Secure Log Access:** Logs can be retrieved using CLI tools included with the Log Server. All access requires proper authentication to ensure security and compliance.
- **Integration with Citrix Core Components:** The AOT Telemetry Service is embedded within core Citrix components, enabling them to act as log generators. Telemetry Service ensures seamless and automated log capture across these components, enabling consistent diagnostic visibility throughout the Citrix infrastructure.

AOT Log Server Deployment and Configuration

AOT Prerequisites

The AOT Log Server is deployed using Docker container technology. Linux is the preferred operating system, though it can also be installed on Windows using Docker Desktop.

Linux

- **Supported OS:** Ubuntu 24.04, Ubuntu 22.04 and RHEL 8.10, 9.4 with Docker installed.
- **Hardware requirements:** Minimum 4 cores CPU, 16 GB RAM, and 500 GB free disk space.
- **Software Requirements:** Install Docker Engine for Linux or Docker Desktop for Linux.
- **User permissions:** Ensure the user can start Docker without requiring root.

Windows

- **Supported OS:** Windows 11, Windows 10, Windows Server 2022 and Windows Server 2025. For Azure VMs see recommendations here.
- **Hardware requirements:** Minimum 8 cores, 24 GB RAM, and 500 GB free disk space.
- **Software requirements:** Install Docker Desktop (subscription may be required) for Windows.
    - **WSL version 2.1.5** or later is required.
    - Enable **Hyper-V** and **Containers** Windows features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Installing and Configuring Log Server

December 4, 2025

1. Download the log server docker container image from Citrix downloads.
2. Place the downloaded files in the same directory.
3. Run the installer in the directory with terminal (Linux) or command prompt (Windows) and follow the instructions:

> **Note:**
>
> - For secure deployment, HTTPS is strongly recommended as it ensures encrypted communication between clients and servers. The use of HTTP is at the customer's discretion.
> - Ensure the selected port is not already in use.
> - Avoid using privileged ports (0–1023) as they require administrator or system-level permissions.
> - Verify that firewall rules allow traffic on the chosen port.
> - Use a port number within the valid range (0–65535), but avoid ports commonly used by system services to prevent conflicts.

Linux Installation

```
chmod +x ./InstallLogServer

# Install with https mode with port 8443 with default path
./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port 8443

# Install with http mode, with port 8080 with default path
./InstallLogServer --port 8080

# Command to change the config path and data path of your choice with https mode
./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port 8443 --config /Path/LogServer/Config --database /Path/LogServer/Data

# Command to change the config path and data path of your choice with http mode
./InstallLogServer --port 8080 --config /Path/LogServer/Config --database /Path/LogServer/Data
```

After the installation, some useful script files are generated:

```
# In Linux, sh scripts will be generated

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
DownloadLogsByTime.sh
DownloadLogsByWords.sh
GetAuthKey.sh
ListMachines.sh
StartLogServer.sh
```

Use ./StartLogServer.sh to start the server.
Check your configpath/weblogs.txt to confirm LogServer started successfully.

If the LogServer starts successfully you will see the below message in the weblogs file. Port 5000 is used by LogServer internally in docker containers with selected http or https protocol.

```
Now listening on: https://[::]:5000
```

If the log server was installed in HTTP mode, successful logs should show the below:

```
Now listening on: http://[::]:5000
```

> **Note:**
>
> - The port configured in the installation step (8080 or 8443 or any port specified) should be used when configuring LogServer url in DDC, Storefront™, VDA, etc.
> - Usually it takes 30s to 60s to start on Linux.

Windows Installation

Step 1: Install Docker Desktop (subscription may be required) for Windows on the log server VM.

Step 2: Run the below commands to continue the installation.

> **Note:**
>
> The default location of Config and Database (Data) folders are created under C:\Users<username>\LogServer.You can change them with the commands below:

```
#Install with https mode with port 8443 with default path
InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443

#Install with http mode, with port 8080 with default path
InstallLogServer.exe --port 8080
#Command to change the config path and data path of your choice with
    https mode
InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443 --
    config C:\LogServer\Config --database C:\LogServer\Datacmd

#Install with specific config path and data path
InstallLogServer.exe --port 8080 --config C:\LogServer\Config --
    database C:\LogServer\Datacmd
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After the installation, a few useful script files are generated in the same directory where you saved the installer files.

> **Note:**
>
> You may move these files to a different location. However, remember the new location, as they will be required again when configuring the Log Server.

```
#In Windows, bat scripts will be generated in the same directory where
    you saved the installer files.

DownloadLogsByTime.bat
DownloadLogsByWords.bat
GetAuthKey.bat
ListMachines.bat
StartLogServer.bat
```

Use `StartLogServer.bat` to start the log server.

Check your **configpath\weblogs.txt** to confirm LogServer started successfully

When the logs show the below, it means to say the Log Server has started successfully.

If the LogServer starts successfully you will see the below message in the weblogs file. Port 5000 is used by LogServer internally in docker containers with selected http or https protocol.

```
Now listening on: https://[::]:5000
```

If the log server was installed in HTTP mode, successful logs should show the below:

```
Now listening on: http://[::]:5000
```

> **Note:**
>
> - The port configured in the installation step (8080 or 8443 or any port specified) should be used when configuring LogServer url in DDC, Storefront, VDA, etc.
> - Usually it takes 1~10 minutes depending upon the hardware in Windows.

Verify the Log Server

Open your browser on Log Server or VDA or DDC, visit http://YourLogServerFQDN:8080/Ping
A response string “Pong UTC:08/19/2025 01:03:29“will show in the browser.

> **Note:**
>
> Change port 8080 to your configured port if not using the default port, and change http to https if installed with HTTPS mode:
>
> If the log server verification fail, please check the following logs:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Run `docker logs logserver` to check docker logs.
> For Linux – `$HOME/LogServer/Config/weblogs.txt`
> (change $HOME/LogServer to your real installed path if not using default one)
>
> For Windows - `C:\Users\YourUserName\LogServer\Config\weblogs.txt`
> (Change YourUserName to real username. Change C:\Users\YourUserName\LogServer to your real installed path if not using default one)

Advanced Configuration of Log Server

Run `docker stop logserver` to stop the logserver

By default, the log server is configured with the below values. To make the changes, edit the `StartLogServer.sh` or `StartLogServer.bat` if installed in windows.

-e MAX_RESERVE_DAYS=7
-e MAX_DISK_USAGE_PERCENTAGE=90
-e LOCAL_DOWN_ONLY=true
-e OPENSEARCH_JAVA_OPTS="-Xms2G -Xmx2G"

LogServer Configuration Options	Default Value	Value Range	Description
MAX_RESERVE_DAYS	7	1~30	Log Server stores log entries max days based on the TimeStamp field. Logs that were inserted 7 days ago will be deleted. Check every 10 minutes.
MAX_DISK_USAGE_PERCENTAGE	90	10~90	Log Server monitors the data storage percentage. If the usage percentage is more than 90%, Log Server will delete old logs day by day until the usage percentage is less than 90%. Check every 10 minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LogServer Configuration Options	Default Value	Value Range	Description
LOCAL_DOWN_ONLY	true	true/false	If true, only the machine installed Log Server can visit the `/Download/*` APIs. If false, then other machines with AuthKey could visit the `/Download/*` APIs.
OPENSEARCH_JAVA_OPTS	”-Xms2G -Xmx2G”	2G ~ MaxMem/2	Opensearch memory configurations. Provide more memory if there are a lot of machines that would send logs to Log Server.

Start the log server, using `./StartLogServer.sh` on Linux
Start the log server using `StartLogServer.bat` on Windows.

To check if the changes are considered

Uninstall Log Server

December 4, 2025

1. Uninstall Log Server in Linux

Run the below commands in terminal:

```
docker rm -f logserver
docker rmi logserver

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
# List containers and images to make sure

docker ps -a
docker images

# Delete Log Server config and data files if not needed any more, change $HOME/LogServer to real installed path if not installed with the default one

rm -r $HOME/LogServer
```

2. Uninstall Log Server in Windows

Run the below commands in powershell:

```
docker rm -f logserver
docker rmi logserver

# List containers and images to make sure

docker ps -a
docker images

# Delete Log Server config and data files if not needed any more, change ~/LogServer to real installed path if not installed with the default one

Remove-Item -Recurse -Force ~/LogServer
```

Uploading the AOT logs from CVAD Core Components

December 4, 2025

If you have configured the log server in HTTPS mode `https://<LogServerFQDN>:port`, make sure the necessary certificate is properly installed and trusted on your system.

1. **Uploading AOT logs from Storefront™**

```
#Enable uploading in HTTP

Set-STFDiagnosticsLogServer -Server LogServerFQDN:8080

#Or to use HTTPS

Set-STFDiagnosticsLogServer -Server https://LogServerFQDN:8443

#Disable
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
10
11 Clear-STFDiagnosticsLogServer
12
13 #The configuration will take effect in one hour. To apply the
       changes immediately, restart the Citrix Telemetry Service.
```

2. **Uploading AOT logs from DDC:**

```
1 #Enable uploadng in HTTP
2 Set-ConfigSite -LogServerEnabled $true -LogServerName
      LogServerFQDN -LogServerPort 8080
3
4 #Or enable HTTPS
5 Set-ConfigSite -LogServerEnabled $true -LogServerName https://
      LogServerFQDN -LogServerPort 8443
6 #Disable HTTP
7 Set-ConfigSite -LogServerEnabled $false -LogServerName
      LogServerFQDN -LogServerPort 8080
8 #Disable HTTPS
9 Set-ConfigSite -LogServerEnabled $false -LogServerName https://
      LogServerFQDN -LogServerPort 8443
```

3. **Enable AOT on Windows VDA:**

From the machine where you installed DDC, run the below commands and after this you need to restart Citrix Desktop Service to make it take effect immediately.

```
1 ```bash
2 #Initiate, run following commands in DDC powershell
3 $configSlot = New-BrokerConfigurationSlot -Name VdaAotTracing -
      Description VdaAotTracing -SettingsGroup G=Telemetry
4
5
6 #If using HTTPS, parameter of -Endpoint should be "https://
      logserverFQDN:8443"
7 $policy = New-BrokerLogServerAddress -Enabled $true -Endpoint "
      logserverFQDN:8080"
8 $mc = New-BrokerMachineConfiguration -ConfigurationSlotUid $configSlot.
      Uid -LeafName VdaAotTracing -Policy $policy
9
10
11 # Using the real DeliverygroupName of your VDA.
12 $dg = Get-BrokerDesktopGroup -Name "DeliverygroupName"
13 Add-BrokerMachineConfiguration -InputObject $mc -DesktopGroup $dg
14
15
16 #Restart Citrix Desktop Service in your VDA to make it take effect
      immediately.
17 ```
```

Update when the log server address or port changed:

```
1 ```bash
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
#Update, run following commands in DDC powershell
#If using HTTPS, parameter of -Endpoint should be "https://
    NewLogServerFQDN:8443"


$policy = New-BrokerLogServerAddress -Enabled $true -Endpoint "
    NewLogServerFQDN:8443"
Set-BrokerMachineConfiguration -Name "VdaAotTracing\VdaAotTracing" -
    Policy $policy
$mc=Get-BrokerMachineConfiguration -Name "VdaAotTracing\VdaAotTracing"

# Using the real DeliverygroupName of your VDA.
$dg = Get-BrokerDesktopGroup -Name "DeliverygroupName"
Add-BrokerMachineConfiguration -InputObject $mc -DesktopGroup $dg
#Restart Citrix Desktop Service in your VDA to make it take effect
    immediately.
```

How to disable:

```bash
#Disable, run following commands in DDC powershell


#If using HTTPS, parameter of -Endpoint should be "https://
    LogServerFQDn:8443"
$policy = New-BrokerLogServerAddress -Enabled $false -Endpoint "
    LogServerFQDN:8080"
Set-BrokerMachineConfiguration -Name "VdaAotTracing\VdaAotTracing" -
    Policy $policy
$mc=Get-BrokerMachineConfiguration -Name "VdaAotTracing\VdaAotTracing"

# Using the real DeliverygroupName of your VDA.
$dg = Get-BrokerDesktopGroup -Name "DeliverygroupName"
Add-BrokerMachineConfiguration -InputObject $mc -DesktopGroup $dg

#Restart Citrix Desktop Service in your VDA to make it take effect
    immediately.

```

1. **Enable AOT on WindowsVDA directly:**

Run the command directly on the machine(WindowsVDA) where you want to upload AOT. This will only take effect on the machine where the command is applied.

```bash
# Enable AOT uploading for Windows VDA
#If using HTTPS, parameter of -AotDataStoreEndpoint should be "https://
    LogServerFQDN:8443"

Enable-CitrixAOTUpload -AotDataStoreEndpoint LogServerFQDN:8443 -Role
    WVDA
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
6
7  # Disable AOT uploading
8  Disable-CitrixAOTUpload
9  ```
```

Viewing and Using AOT Logs

Accessing Logs via Log Server

To keep your logs secure, you will need an **AuthKey before** downloading them. Here is what to do:

1. Get your AuthKey –Use your own role-name/name to generate it.
2. Run locally –Scripts can only run on the machine where the Docker container is installed.
3. Windows users –Use the GetAuthKey.bat scripts instead of shell scripts.
4. Download logs –Once authenticated, you can safely retrieve your logs.

```
1  For Linux
2  ./GetAuthKey.sh role-name
3  {
4   "key":"ebac9b7726cb4be597c92c6769134d25","role":"role-name","
       status":"DONE" }
5
6
7  For Windows
8  GetAuthKey.bat role-name
9  {
10  "key":"ebac9b7726cb4be597c92c6769134d25","role":"role-name","
       status":"DONE" }
11
12
13 #Save the key: ebac9b7726cb4be597c92c6769134d25 by yourself. It's
       the only way to get the key.
```

List machine names that have already sent their AOT logs to the logserver:

```
1  ```bash
2  #The parameter is the key get from GetAuthKey.sh
3  For linux:
4  ./ListMachines.sh ebac9b7726cb4be597c92c6769134d25
5  {
6   "machines":["MachineName"] }
7
8  #Empty machines means that there has no log
9
10 For Windows:
11 ListMachines.bat ebac9b7726cb4be597c92c6769134d25
12 {
13  "machines":["MachineName"] }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
14
15 #Empty machines means that there has no log
16 ```
```

Download logs by Machine name and Time range. Time is in UTC format.

```
1  ```bash
2  #Usage: ./DownloadLogsByTime.sh [AuthKey] [MachineName] [StartTime] [
       EndTime] [OutputFile]
3  #Example:
4
5  For Linux
6  ./DownloadLogsByTime.sh ebac9b7726cb4be597c92c6769134d25 MachineName
       2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
7
8  For Windows
9  DownloadLogsByTime.bat ebac9b7726cb4be597c92c6769134d25 MachineName
       2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
10 ```
```

Download logs by keyword/s filter. Time is in UTC format:

> **Note:**
>
> - A keyword can be a single word or a combination of words.
> - Keywords can match anywhere within the log message.
> - A **Transaction ID** can also be used as a keyword.

```
1  ```bash
2  #Usage: ./DownloadLogsByWords.sh [AuthKey] [StartTime] [EndTime] [
       SearchWords] [OutputFile]
3
4  #Example:
5  For Linux:
6  ./DownloadLogsByWords.sh authkey 2025-01-01T00:00:00.000Z 2025-12-31T23
       :59:59.999Z "session launch" logs.csv
7
8  For Windows:
9  DownloadLogsByWords.bat authkey 2025-01-01T00:00:00.000Z 2025-12-31T23
       :59:59.999Z "failed vda" logs.csv
10 ```
```

General Response Code for Log Server API

December 4, 2025

This table outlines the standard HTTP response codes used by the Log Server's API to communicate the result of client requests. These codes help clients understand whether their requests were success-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ful or if errors occurred, and what kind of errors were encountered. Understanding these response codes is crucial for diagnosing issues, debugging API calls, and ensuring smooth integration with the Log Server.

Error	Status	Description
200	OK	The request was successful.
400	Bad request.	The server could not process the request due to missing parameters, malformed syntax, or absence of required HTTP headers. For example, if fields like MachineName or Role are missing in the request headers, this response is triggered.
401	Not Authorized.	The request was denied because the client is not authorized. This usually occurs when the IP address or the authentication key (AuthKey) used is not permitted to access the Log Server.
404	Not found.	The API path requested does not exist. This response is returned when the endpoint is invalid or mistyped.
500	Internal error.	Indicates that the Log Server encountered an unexpected condition preventing it from fulfilling the request. This is commonly caused by server-side issues such as resource exhaustion (e.g., memory or disk space).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting with AOT and Log Server

December 4, 2025

Top challenges addressed by AOT

1. Availability of AOT logs from a centralized log server for DDC, StoreFront™ and VDA components.
2. Improve log collection time and reduce repetitive log iterations.
3. Increase customer self-troubleshooting capabilities.
4. Accelerate issue resolution time (MTTR)
5. Quick search for logs based on various parameters/keywords.

Ways to download AOT logs

1. When the Timestamp is Known:
    - Use the /Download/TimeRange interface within the powershell script to download logs for the timeframe when the issue occurred.
    - Collect logs from all relevant components (DDC, StoreFront, VDA) involved in the issue.
    - Review the logs to identify failures or anomalies and take corrective action based on log details.
2. When the Problem Description is known:
    - Use the /Download/SearchLog interface with relevant keywords (error messages, components, events).
    - Identify specific log entries related to the issue.
    - Further refine the search by time or component as necessary.
3. When the logs have to shared with Citrix Tech Support with further troubleshooting
    - If the logs do not clearly indicate the root cause, or if the available information is insufficient to resolve the issue.
    - Package the logs and share them with Citrix Support for further analysis.

Best Practices for Using AOT

December 4, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Time-Based Log Analysis: Download logs based on the estimated timeframe of the issue using /Download/TimeRange. Analyze the logs to identify failures or anomalies tied to that timeframe.

Keyword-Based Log Search: Use /Download/SearchLog with relevant **keywords or transaction ID** to locate specific error messages, events, or patterns. This is effective for known issues or symptoms.

Combine Time and Keyword Search: For complex issues, start with a time-based search and refine results using keywords within the identified timeframe.

FAQ

December 4, 2025

1. **How can I check the running log server configurations, like MAX_RESERVE_DAYS?**
   You can check the container environment values using either of the following commands:

```
docker inspect logserver |findstr MAX_RESERVE_DAYS
```

Or by checking the container environment:

```
docker exec -it logserver env |grep MAX_RESERVE_DAYS
```

If nothing is returned, it means the log server is using the default value:
MAX_RESERVE_DAYS=7

1. **Do I need to purchase Docker Desktop licenses when installing the log server container image on Windows?**

Yes. A valid Docker Desktop license is required.

1. **Should I use a new server for log server installation?**

Yes. It is recommended to use a dedicated server for the log server installation to ensure performance and isolation.

Known Issues and Limitations

December 4, 2025

In the CVAD 2507 LTSR release, Always On Tracing (AOT) is designed to capture logs from the following three primary components: Delivery Controllers (DDCs), StoreFront™ and Virtual Delivery Agents (VDAs)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This initial scope targets a subset of the most common and recurring issues. The current implementation helps reduce the need for issue reproduction in a few scenarios but not all, specifically for problems related to DDCs, StoreFront, and VDAs.

All remaining components and their corresponding AOT logs will be introduced in future iterations.

Third party notice

December 4, 2025

This release of Citrix AOT Log Server may include third-party software licensed under the terms defined in the following documents:

- Citrix Centralized Log Server Third Party Notices

Third party notices

September 6, 2025

This release of Citrix Virtual Apps and Desktops™ may include third-party software licensed under the terms defined in the following documents:

- Citrix Virtual Apps and Desktops Third Party Notices (PDF Download)
- Citrix Assistant App Third Party Notices - Preview (PDF Download)
- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0) (PDF Download)
- FlexNet Publisher Documentation Supplement Third Party and Open Source Software used in FlexNet Publisher 11.15.0 (PDF Download)

SDKs and APIs

September 13, 2025

Several SDKs and APIs are available with this release. To access the SDKs and APIs, go to Build anything with Citrix. From there, select **Citrix Workspace** to access programming information for Citrix Virtual Apps and Desktops and its related components.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The Citrix Virtual Apps and Desktops™ SDK and the Citrix Group Policy SDK can be installed as a module or a snap-in. Several component SDKs (such as Citrix Licensing, Citrix Provisioning, and StoreFront) install using only a snap-in.

This product supports PowerShell versions 3 through 5.

Citrix Virtual Apps and Desktops SDK

This SDK installs automatically as a PowerShell module when you install a Delivery Controller™ or Studio. This enables you to use this SDK's cmdlets without having to add snap-ins. (Instructions are provided below if you choose to install this SDK as a snap-in.)

Permissions

You must run the shell or script using an identity that has Citrix administration rights. Although members of the local administrators group on the Controller automatically have full administrative privileges to allow Citrix Virtual Apps or Citrix Virtual Desktops™ to be installed, Citrix recommends that for normal operation, you create Citrix administrators with the appropriate rights, rather than use the local administrators account.

Access and run the cmdlets

1. Start a shell in PowerShell: Open Studio, select the **PowerShell** tab, and then click **Launch PowerShell**.
2. To use SDK cmdlets within scripts, set the execution policy in PowerShell. For information about PowerShell execution policy, see the Microsoft documentation.
3. If you want to use the snap-in (rather than the module), add the snap-in using the `Add-PSSnapin` (or `asnp`) cmdlet.

   V1 and V2 denote the version of the snap-in. XenDesktop 5 snap-ins are version 1. Citrix Virtual Apps and Desktops, and earlier XenDesktop 7 version snap-ins are version 2. For example, to install Citrix Virtual Apps and Desktops snap-in, type `Add-PSSnapin Citrix.ADIdentity.Admin.V2`. To import all the cmdlets, type: `Add-PSSnapin Citrix.*.Admin.V*`

You can now use the cmdlets and help files.

- To access the help files for this SDK, select the product or component in the Categories list, and then select **Citrix Virtual Apps and Desktops SDK**.
- For PowerShell guidance, see Windows PowerShell Integrated Scripting Environment (ISE).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Group Policy SDK

The Citrix Group Policy SDK enables you to display and configure Group Policy settings and filters. This SDK uses a PowerShell provider to create a virtual drive that corresponds to the machine and user settings and filters. The provider appears as an extension to `New-PSDrive`.

To use the Group Policy SDK, either Studio or the Citrix Virtual Apps and Desktops SDK must be installed.

The Citrix Group Policy PowerShell provider is available as a module or a snap-in.

- To use the module, no additional work is needed.
- To add the snap-in, type `Add-PSSnapin citrix.common.grouppolicy`.

To access help, type: `help New-PSDrive -path localgpo:/`.

To create a virtual drive and load it with settings, type `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` where the Controller string is the fully qualified domain name of a Controller in the site you want to connect to and load settings from.

Citrix Virtual Apps and Desktops REST APIs

With Citrix Virtual Apps and Desktops REST APIs, you can automate the management of resources within a Citrix Virtual Apps and Desktops deployment.

The Citrix Virtual Apps and Desktops REST APIs are available at https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis. APIs not applicable to Citrix Virtual Apps and Desktops are marked accordingly. Follow the guidance there to configure access to the API service and use the APIs to manage and optimize your resources.

Monitor Service OData

The Monitor API allows access to the Monitor Service data using Version 3 or 4 of the OData API. You can create customized monitoring and reporting dashboards based on data queried from the Monitor Service data. OData V.4 is based on the ASP.NET Web API and supports aggregation queries.

For more information, see the Monitor Service OData API.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.