Workspace Environment Management™ 2603

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

Contents

Workspace Environment Management™ 2603 22
Technical overview 22
What's new 25
What's new in 2603 25
Run scripted tasks as a logged-on user 25
Create multiple scripted tasks from a single script 25
Microsoft User State Virtualization (USV) settings 25
Add local Citrix applications to Citrix Environment Tool Hub 26
VHD Expansion Tool 26
Pre-migration permission validation for profile migration 26
Support for LDAPS communication with Active Directory 26
LAS enforcement 26
Profile Management 26
Fixed issues 27
Known issues 27
Third party notices 27
Deprecation 27
Deprecations and removals 28
Quick-start guide 32
Overview 32
Prerequisites 32
Installation and configuration 32
Step 1: Install the infrastructure services 33
Step 2: Create a WEM database 34
Step 3: Configure infrastructure services 44
Step 4: Install the administration console 49

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

Step 5: Configure configuration sets 50
Step 6: Add the group policy template (optional) 60
Step 7: Install the agent 63
Step 8: Add the agent to the configuration set you created 67
System requirements 69
Software prerequisites 69
Operating system prerequisites 71
Infrastructure services 71
Administration console 71
Web console 71
Agent 72
SQL Server Always On 72
Hardware prerequisites 73
Service dependencies 74
Antivirus exclusions 74
In the infrastructure services installation folder 74
In the agent installation folder 74
Install and configure 76
Download the installer 76
Infrastructure services 77
Install the infrastructure services 77
Create a service principal name 78
Group Managed Service Account 79
Configure load balancing 81
Create a Workspace Environment Management database 82
Configure the infrastructure service 88
Administration console 96
Install the administration console 96

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

Create an infrastructure server connection 97
Configure the database with a license server 98
Import quickstart settings 98
Enforce LDAPS to encrypt Active Directory connections 99
Web console service 100
Install the web console service 100
Configure the Web console service 101
Prerequisites 101
Configure and start the Web console service 101
Set up licensing 113
Prerequisites 114
Configure licensing for the infrastructure services 114
Configure the license server globally for WEM infrastructure services 114
Configure the license server for a single WEM infrastructure server 115
Configure licensing for the web console 116
Re-accept the license server certificate 118
Verify that WEM LAS is working 118
Verify LAS for the infrastructure service and legacy console 118
Check license server information in the web console 119
Troubleshoot license issues 120
Agent 120
Install and configure the agent 120
Step 1: Configure group policies (optional) 121
Step 2: Install the agent 124
Step 3: Restart the machine to complete the installation 129
Prerequisites and recommendations 129
Prerequisites 129
Recommendations 130

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

Agent startup behaviors 130
Agent cache utility options 130
Good to know 131
Agent settings 131
System settings 132
Examples 133
Scale and size considerations for deployments 134
Upgrade a deployment 136
Introduction 136
Step 1: Upgrade the infrastructure services 137
Upgrade the operating system of an infrastructure server 137
Step 2: Upgrade the database 138
Step 3: Reconfigure the infrastructure services 140
Step 4: Upgrade the administration console 140
Step 5: Upgrade and reconfigure the web console service 140
Step 6: Upgrade the agent 141
Home page 142
Overview 142
Quick access 142
Global configurations 143
Highlights 144
Preview features 144
Home page 145
Overview 145
Quick access 145
Global configurations 146
Highlights 147
Preview features 147

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

Configuration Sets 147
Add a configuration set 148
Edit or delete a configuration set 148
Add configuration sets to favorites 149
Configure settings for a configuration set 149
Back up and restore 149
Upload a configuration file 150
Manage automatic backup 151
Back up a configuration set 151
Back up Profile Management settings 153
Actions 153
Group Policy settings 154
Applications 164
External tasks 170
Printers 176
Network drives 179
Virtual drives 182
Registry Entries 185
Environment variables 188
More information 191
File System Operations 195
File Type Associations 196
JSON files 199
INI Files 204
Ports 205
User DSNs 207
Security 209
Application security 209

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

Privilege elevation 212

Process hierarchy control 214

Assignments 219

Assignment targets 219

Filters 222

More information 232

Triggers 234

Create a trigger 235

Edit a trigger 238

Clone a trigger 238

Manage associations 239

Delete a trigger 239

Supportability matrix for triggers 240

Profiles 240

Citrix Profile Management Settings 241

Microsoft USV Settings 258

Scripted Tasks 260

Create a scripted task 260

View reports for a scripted task 264

App package delivery 264

Configure storage location 264

Add app package 265

Create a WEM agent upgrade task 266

Create a custom task 267

Advanced Settings 268

Agent settings 268

Action settings 274

UI Agent Personalization 277

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

Monitoring preferences 280
File shares 282
System Optimization 284
CPU management 285
Memory management 293
I/O management 296
Fast logoff 297
Citrix Optimizer 297
Multi-session optimization 300
Directory Objects 301
Add a machine or machine group 302
Add machines in an OU 302
Edit machine, machine group, or OU details 303
Delete objects 303
Advanced settings 304
Unbound agents 304
Active Directory connection security 304
Monitoring 304
Administration 305
User statistics 305
Agents 307
Configure Profile Management health check 317
Insights 317
Optimization insights 317
Usage insights 318
Profile container insights 319
Reports 321
Introduction 321

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

Columns to display and filters 325
View more details of a report 326
Export reports 326
Export to third-party platform 327
Scripts for scripted tasks 328
Introduction 328
Add a custom script 328
Before you begin 328
Workflow 329
Manage scripts 330
Edit a script 331
Delete a script 331
Clone a script 331
Configure tasks from a script 332
Built-in scripts 332
Cloud Health Check 332
Windows Service Management 333
Server Reboot 336
CDF Tracing Management 337
AOT Log Collection 340
Check DNS Settings 340
Check RDS License 341
Diagnose VDA Unregistration 342
Run Profile Management Health Check 342
Set Profile Reset Trigger 343
More information 344
Files 344
Manage Basic Deployment agents 346

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

Configuring the basic deployment agent settings 346
Switching the agent deployment type 353
Using the WEM Logon duration feature 353
User experience 355
Start the administration console 355
Configure your installation 355
Manage (legacy console) 356
Ribbon 356
Home tab 356
About tab 360
Actions 361
Action Groups 362
Action group list 362
Example scenario 366
Group Policy Settings 374
Group Policy settings 375
Import Group Policy settings 376
Import Group Policy settings from registry files 376
Edit Group Policy settings 377
Contextualize Group Policy settings 379
Template-based settings 381
Create a GPO with a template 382
Scripted Task Settings 385
Configure a scripted task 385
View reports for a scripted task 388
Applications 388
Application list 389
Start menu view 391

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

Editing application settings using Citrix Studio 391
Printers 393
Network printer list 393
Network Drives 394
Network drive list 394
Virtual Drives 395
Virtual drive list 395
Registry Entries 396
Registry value list 396
To add a registry entry 397
Import registry files 397
Environment Variables 398
Environment variable list 399
Ports 399
Ports list 400
Ini Files 401
Ini files operation list 401
External Tasks 402
External task list 402
Troubleshooting 407
External task examples 407
File System Operations 407
File system operations list 408
User DSN 409
User DSN list 409
File Associations 410
File association list 410
Good to know 413

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

Filters 414
Rules 414
Filter rule list 414
Fields and controls 415
Conditions 415
Filter condition list 415
Fields and controls 416
Assignments 416
Action assignment 417
Users 417
Assignments 417
Modeling wizard 418
Fields and controls 418
System Optimization 418
CPU Management 419
CPU management settings 419
CPU priority 424
CPU affinity 425
CPU clamping 425
Memory Management 426
Memory management 426
Memory usage limit 428
I/O Management 429
I/O priority 429
Fast Logoff 430
Settings 430
Citrix Optimizer 430
Settings 430

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

Fields and controls 432
Multi-session Optimization 433
Settings 433
Policies and Profiles 433
Environmental Settings 434
Start menu 434
Desktop 434
Windows Explorer 434
Control Panel 435
Known folders management 435
SBC/HVD tuning 435
Microsoft USV Settings 436
Roaming profiles configuration 436
Roaming profiles advanced configuration 436
Folder redirection 437
Citrix Profile Management Settings 438
Main Citrix Profile Management settings 438
Profile container settings 439
Profile handling 440
Advanced settings 441
Log settings 446
Registry 446
File system 446
Synchronization 448
Streamed user profiles 448
File deduplication 449
Cross-platform settings 449
App access control 450

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

Folder redirection 450
Security 451
Application security 452
Application security 452
Rule collections 453
To import AppLocker rules 454
To add a rule 454
To assign rules to users 455
To add default rules 456
To edit rules 456
To delete rules 456
To back up application security rules 456
To restore application security rules 456
Process management 457
Process management 457
Process block list 457
Process allow list 457
Privilege elevation 458
Privilege elevation 458
Supported rules 458
Self-elevation 463
Process hierarchy control 464
Considerations 465
Prerequisites 466
Process hierarchy control 466
Active Directory Objects 469
Users 470
To add a user 470

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

To add multiple users 470
Machines 470
To add a computer or computer group to the current configuration set 471
To add computers in an organizational unit to the configuration set 471
To edit computer, computer group, or OU details 471
Advanced 472
Active Directory search timeout 472
Unbound agent site settings 472
Enforce LDAPS to encrypt Active Directory connections 472
Transformer settings 472
General 472
General settings 472
Site settings 473
Tool settings 473
Advanced 474
Process launcher 474
Advanced & administration settings 474
Logon/logoff and power settings 476
Advanced settings 476
Configuration 477
Main configuration 477
Cleanup actions 478
Agent options 479
Advanced options 481
Reconnection actions 481
Advanced processing 481
Service options 481
Console settings 482

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

StoreFront™ 482
Agent switch 483
Wake on LAN 484
UI agent personalization 485
UI agent options 485
Helpdesk options 487
Power saving 488
Administration 488
Administrators 489
Configured administrators list 489
Users 490
Statistics 491
Agents 491
Statistics 491
Registrations 494
Logging 495
Administrative 495
Agent 496
Monitoring 496
Daily reports 496
User trends 496
User & device reports 497
Profile container insights 497
Summary 497
Profile container status 498
Configuration 498
Report options 498
Back up and restore 498

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

Upload a configuration file 499
Manage automatic backup 500
Back up a configuration set 500
Back up Profile Management settings 502
Reference 503
Agent event logs 503
WEM configuration set 504
WEM agent connection to infrastructure services 504
Agent configuration refresh events 505
Directory service events 505
Machine policy events 506
User policy events 506
Cache sync events 507
Optimization events 509
CPU optimization 509
Memory optimization 511
Agent Insights 511
WEM Administrators: Enable and configure Agent Insights in the WEM console 512
Users: Enable and open Agent Insights on machines 513
Reference 513
Session tab 514
Profile tab 515
Logon tab 515
Agent in CMD and UI mode 516
Differences between CMD mode and UI mode 516
Citrix Environment Tool Hub 518
Download and launch the tool hub 519
Application Assistant 519

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

Workspace resources 519
Icons 520
Start Menu Configurator for Windows 11 520
Add applications 520
Windows Logon analysis 521
Process activity and details 549
User Store Creation Tool 550
Errors 550
File Info Viewer 551
File Type Association Assistant 551
Printer Assistant 552
Profile Migration Tool 552
Rule Generator for App Access Control 554
About the rules 554
Create rules 554
Generate raw data for rules 557
Validate rules 558
Import FSLogix rule sets 558
Assign app access rules to AAD users/groups and NDJ machines 559
Profile Cleanup Tool 560
Scripted Task Validator 562
Validate and export a scripted task 562
VHD Expansion Tool 563
Add local applications for quick access 563
Common Control Panel applets 564
Dynamic tokens 567
Dynamic token support for Group Policy settings 567
Applications 568

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

Printers 568
Network drives 568
Virtual drives 568
Registries 568
Environment variables 569
Ports 569
Ini files 569
External tasks 569
File system operations 569
Certain filter conditions 569
String operations 569
Hashtags 571
Active Directory attributes 574
Registries 576
XML files 576
INI files 576
More information 577
Supportability matrix for filter conditions 577
Environmental Settings registry values 578
Filter conditions 605
FIPS support 621
Upgrade considerations 625
Agent considerations 625
Load balancing with Citrix ADC 625
Log parser 627
Port information 628
View log files 630
Logs related to the agent 630

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

Logs related to the infrastructure service 632
Logs related to the administration console 633
Logs related to the WEM database 633
Logs related to the WEM web console 633
Windows Communication Foundation traces 634
Troubleshoot communications between the agent and the infrastructure service 634
Troubleshoot communications related to the WEM infrastructure service 636
Troubleshoot communications between the WEM administration console and the WEM database 637
Troubleshoot WEM LAS issues 639
Check connectivity to the license server 640
Test connectivity 641
Troubleshoot license server certificate issues 641
Certificate expired or not yet valid 641
License server hostname mismatch 642
The certificate acceptance dialog box does not appear 645
Force the certificate acceptance dialog box to appear 646
Collect verbose LAS logs 647
WEM health check tool 648
Launch the tool 648
Home page 648
Infrastructure server 649
WEM Integrity Condition List Manager 650
XML printer list configuration 666
XML printer list file structure 666
VUEMUserAssignedPrinter tag syntax 668
Example printer object 669
Glossary 674

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

Workspace Environment Management™ Document History 679

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

Workspace Environment Management™ 2603

Workspace Environment Management uses intelligent resource management and profile management technologies to deliver the best possible performance, desktop logon, and application response times for Citrix Virtual Apps and Desktops™ deployments. It is a software-only, driver-free solution.

Resource management - To provide the best experience for users, Workspace Environment Management monitors and analyzes user and application behavior in real time, then intelligently adjusts RAM, CPU, and I/O in the user workspace environment.

Profile Management - To deliver the best possible logon performance, Workspace Environment Management replaces commonly used Windows Group Policy Objects, logon scripts, and preferences with an agent which is deployed on each virtual machine or server. The agent is multi-threaded and applies changes to user environments only when required, ensuring users always have access to their desktop as fast as possible.

For information about upgrading, see Upgrade a deployment.

For information about installing the current release, see Install and configure.

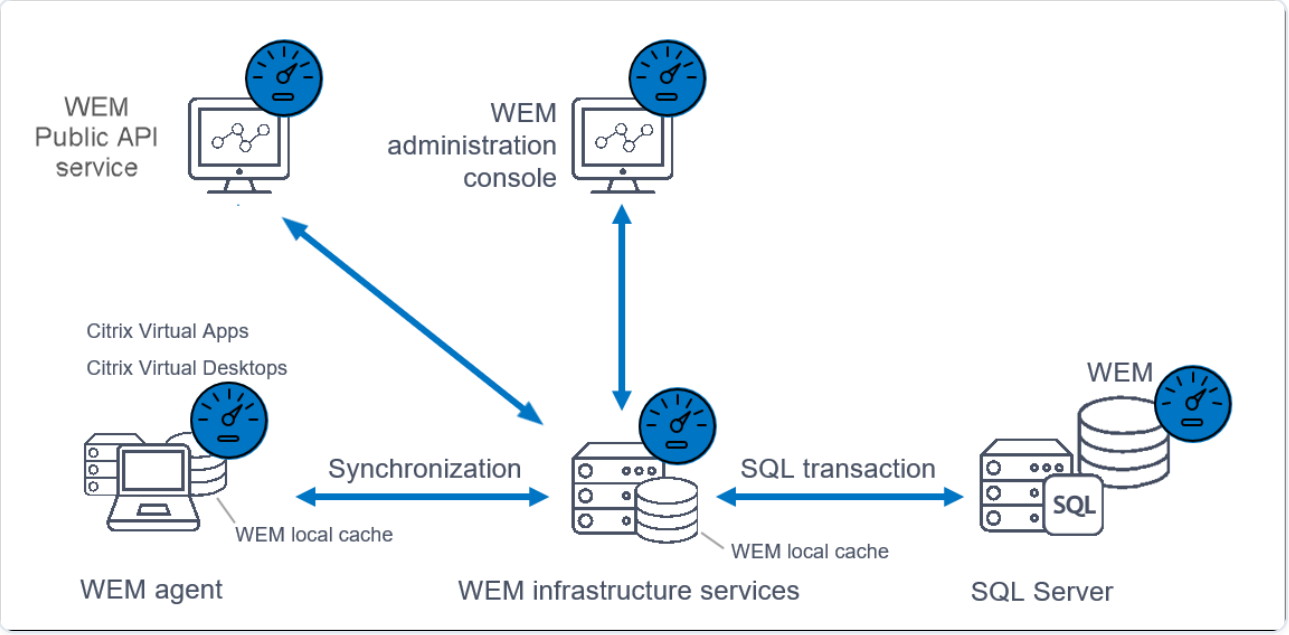
NOTE:

Workspace Environment Management is covered by the Current Releases (CR) lifecycle of Citrix Virtual Apps and Desktops. For more information, see Product Matrix.

Technical overview

Workspace Environment Management (WEM) has the following architecture:

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



Infrastructure services. The infrastructure services are installed on a multi-session OS. They synchronize various back-end components (SQL Server and Active Directory) with front-end components (administration console and agent).

NOTE:

Infrastructure services cannot be installed on a domain controller. Kerberos authentication issues prevent the infrastructure service from working in this scenario.

Administration console. The Workspace Environment Management administration console is installed on a single-session or multi-session OS. It connects to the infrastructure services. You use the administration console to manage your Workspace Environment Management installation. For example, you create and assign resources, manage policies, authorize users, and so on.

WEM Public API service. The Workspace Environment Management Public API service provides HTTPS services to support the WEM web console and communicate with the WEM infrastructure service.

Agent. The Workspace Environment Management agent connects to the Workspace Environment Management infrastructure services and enforces settings you configure in the administration console. You can deploy the agent on a Virtual Delivery Agent (VDA). Doing so lets you manage single-session or multi-session environments. You can also deploy the agent on a physical Windows endpoint.

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

NOTE:

- The agent cannot be installed on the infrastructure server. The agent installer fails in this scenario.
- The Transformer feature is not supported on multi-session OSs.

SQL Server Database. Workspace Environment Management requires an SQL Server database to store its settings. The database can be hosted in an SQL Server Always On availability group if necessary. (For more information, see System requirements.)

Microsoft Active Directory Server. Workspace Environment Management requires access to your Active Directory to push settings to your users.

TIP:

You can download the latest Workspace Environment Management installer from the Citrix Virtual Apps and Desktops downloads page `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/>`. On that page, access the installer under **Components** of the latest version of Citrix Virtual Apps and Desktops.

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

What's new

What's new in 2603

TIP:

You can download the latest Workspace Environment Management installer from the Citrix Virtual Apps and Desktops downloads page `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/>`. On that page, access the installer under **Components** of the latest version of Citrix Virtual Apps and Desktops.

This release includes the following new features and addresses issues to improve the user experience:

Run scripted tasks as a logged-on user

You can now run scripted tasks on demand directly in a logged-on user's session. By specifying a user name or session ID, you can trigger tasks to run with that user's permissions. This feature enables seamless interaction with user-specific actions and environments in real-time. For more information about how to enable this feature, see Add a custom script.

Create multiple scripted tasks from a single script

You can now use a single script to create multiple scripted tasks. This feature reduces duplicate tasks, speeds rollout, and lowers maintenance effort and error risk. Faster navigation from task definitions to settings further streamlines management and improves admin productivity across environments. For more information, see Scripted Tasks.

Microsoft User State Virtualization (USV) settings

You can now configure Microsoft User State Virtualization (USV) settings directly through the web console. For more information, see Microsoft User State Virtualization (USV) settings.

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

Add local Citrix applications to Citrix Environment Tool Hub

You can now automatically add local Citrix-related applications to Citrix Environment Tool Hub for quick access. This enhancement streamlines application discovery and availability, making it easier to launch and manage Citrix applications from a single location. For more information, see Add local applications for quick access.

VHD Expansion Tool

You can now seamlessly scale user profile storage with the new VHD Expansion Tool in Citrix Environment Tool Hub. This tool provides a guided workflow with path selection and one-click expansion, reducing the need for manual resizing steps. For more information, see VHD Expansion Tool.

Pre-migration permission validation for profile migration

Profile Migration Tool now validates user store permissions before migration starts. This pre-migration check helps ensure successful migrations by identifying and remediating permission issues early, reducing setup errors, and failures. For more information, see Profile Migration Tool.

Support for LDAPS communication with Active Directory

You can now secure communication between WEM and Active Directory using LDAPS. This feature ensures encrypted directory traffic, helps meet enterprise security and compliance requirements, and reduces exposure in regulated environments. For more information about how to enable LDAPS communication, see Install and configure Infrastructure services, Install and configure Administration console, and Manage Active Directory objects.

LAS enforcement

You can now activate WEM using the License Activation Service (LAS) from the on-premises WEM web console. LAS is a cloud-based alternative to legacy Citrix licensing that simplifies license management. For more information, see Set up licensing.

Profile Management

Workspace Environment Management™ now supports all supported versions of Profile Management through 2603:

- **Enable multi-session support for machine hibernation.** If enabled, VHDX disks used by a hibernated session are not reassigned to other sessions. This behavior allows the user profile to be resumed after the machine recovers from hibernation, ensuring session continuity.

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

The feature is available under each configuration set in **Profiles > Profile Management Settings > Advanced settings > VHD settings**. For more information, see Citrix Profile Management Settings.

Fixed issues

Workspace Environment Management™ 2603 contains the following fixed issues:

- The VUEMUIAgent process might crash on Windows 11 when the location services feature is disabled in the system settings.
- Restoring the default recommended settings (VUEMAgentSettings.xml) might fail in FIPS-enabled environments.

Known issues

Workspace Environment Management™ 2603 has the following known issues:

- WEM license authentication through the Citrix Licensing Activation Service (LAS) fails when the debug mode is disabled (the default). As a result, license activation does not complete.

  Workaround: Enable debug mode on both the infrastructure service and the web console, then retry activation:

  a. Open the **WEM Infrastructure Service Configuration** utility, go to the **Advanced Settings** tab, select the **Enable debug mode** check box, and click **Apply**.

  b. Open the **Citrix Workspace Environment Management Web Console Configuration** utility, select the **Enable console logging** check box, and **Save**.

Third party notices

The current release of Workspace Environment Management™ might include third-party software licensed under the terms defined in the following document:

Workspace Environment Management Third Party Notices

Deprecation

The announcements in this article are intended to give you advanced notice of platforms and Workspace Environment Management™ features that are being phased out so that you can make timely business decisions. Citrix® monitors customer use and feedback to determine when they

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

are withdrawn. Announcements might change in subsequent releases and might not include every deprecated feature or functionality.

For more information about product lifecycle support, see Product Lifecycle Support Policy.

Deprecations and removals

The following table shows the platforms and Workspace Environment Management (WEM) features that are deprecated or removed.

Deprecated items are not removed immediately. Citrix continues to support them in this release but they will be removed in a future Current Release. Items marked with an asterisk (*) are supported up to and including the next Citrix Virtual Apps and Desktops Long Term Service Release (LTSR) release.

Removed items are either removed—or are no longer supported—in Workspace Environment Management.

ITEM	ANNOUNCED IN	REMOVED IN	ALTERNATIVE
File-based licensing	2507	April 2026	License Activation Service (LAS) is the next-generation technology for product activations across Citrix products. If you are using file-based licensing, you must upgrade to a LAS-compatible release and complete the transition before April 15, 2026. After that date, LAS will be the only method to activate and license Citrix on-premises components. For more information, see File-based

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

ITEM	ANNOUNCED IN	REMOVED IN	ALTERNATIVE
			licensing system EOL notification.
Support for cache synchronization port (applicable to Workspace Environment Management 1909 and earlier; replaced by Cached data synchronization port in Workspace Environment Management 1912 and later).	2012	**2103**	Upgrade to Workspace Environment Management 1912 or later. Note: If you use Workspace Environment Management 2103 or later, be sure to upgrade your Workspace Environment Management agent to 1912 or later.
Support for VMware Persona settings.	1906	**1909**	
Support for WEM infrastructure services on the following OS platforms: Windows Server 2008 R2 SP1, and Windows Server 2012.	4.7	**1808**	
Support for the WEM administration console on the following OS platforms: Windows Vista SP2 32-bit and 64-bit, Windows 7 SP1 32-bit and 64-bit, Windows 8.x 32-bit and 64-bit, Windows Server	4.7	**1808**	

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

ITEM	ANNOUNCED IN	REMOVED IN	ALTERNATIVE
2008 SP2, Windows Server 2008 R2 SP1, and Windows Server 2012.			
Support for the WEM agent on the following OS platforms: Windows Vista SP2 32-bit and 64-bit, and Windows Server 2008 SP2.	4.7	**1808**	
In-place upgrade from WEM 3.0, 3.1, 3.5, 3.5.1 to WEM 4.x.*	4.5	Upgrade to WEM 3.5.2, then upgrade to WEM 4.x.	
Support for all WEM components on Windows XP SP3 32-bit and 64-bit.	4.5	4.5	Use a supported OS platform.
Support for WEM agent on the following OS platforms: Windows XP SP3 32-bit and 64-bit, Windows Server 2003 32-bit and 64-bit, Windows Server 2003 R2 32-bit and 64-bit	4.5	4.5	Use a supported OS platform.
Support for assigning and binding existing (pre-version 4.3) agents to sites via GPO.	4.3		Upgrade agents to Workspace Environment Management 4.3 or later.

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

ITEM	ANNOUNCED IN	REMOVED IN	ALTERNATIVE
Support for WEM administration console on the following OS platforms: Windows XP SP3 32-bit and 64-bit, Windows Server 2003 32-bit and 64-bit, Windows Server 2003 R2 32-bit and 64-bit	4.2	4.5	Use a supported OS platform.
Support for WEM administration console on the following OS platforms: Windows Vista SP1 32-bit and 64-bit, Windows Server 2008, Windows Server 2008 R2	4.2	4.5	
Support for all WEM components on Microsoft .NET Framework 4.0, 4.5.0, or 4.5.1.	4.2	4.5	Upgrade to Microsoft .NET Framework 4.5.2.

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

Quick-start guide

This guide describes how to install and configure Workspace Environment Management™ (WEM). It provides step-by-step installation and configuration instructions, and suggested best practices.

Overview

WEM is a user environment management solution designed to let you deliver the best possible workspace experience to users. It is a software-only, driver-free solution.

Prerequisites

Before you install WEM in your environment, verify that you meet all system requirements. For more information, see System requirements.

Installation and configuration

Citrix® recommends that you install the latest version of WEM. Deploying WEM consists of installing and configuring three core components: Infrastructure services, Administration console, and Agent. The following procedures detail how to install and configure these components:

- Infrastructure services
- Administration console
- Web console
- Agent

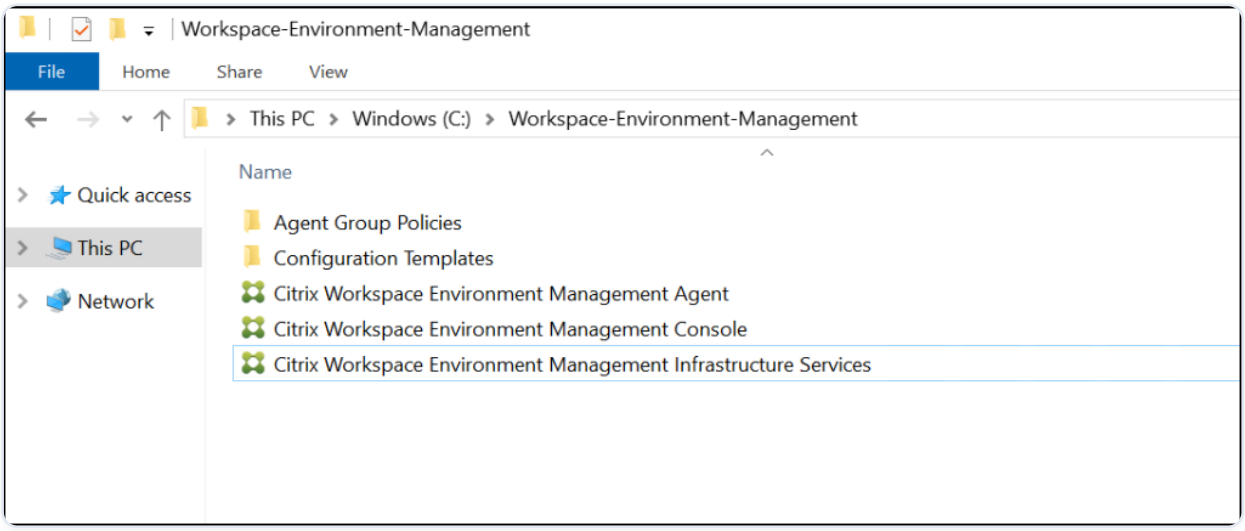
NOTE:

- Do not install any of the components above on a domain controller.
- Do not install the infrastructure services on the server where the Delivery Controller™ is installed.

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

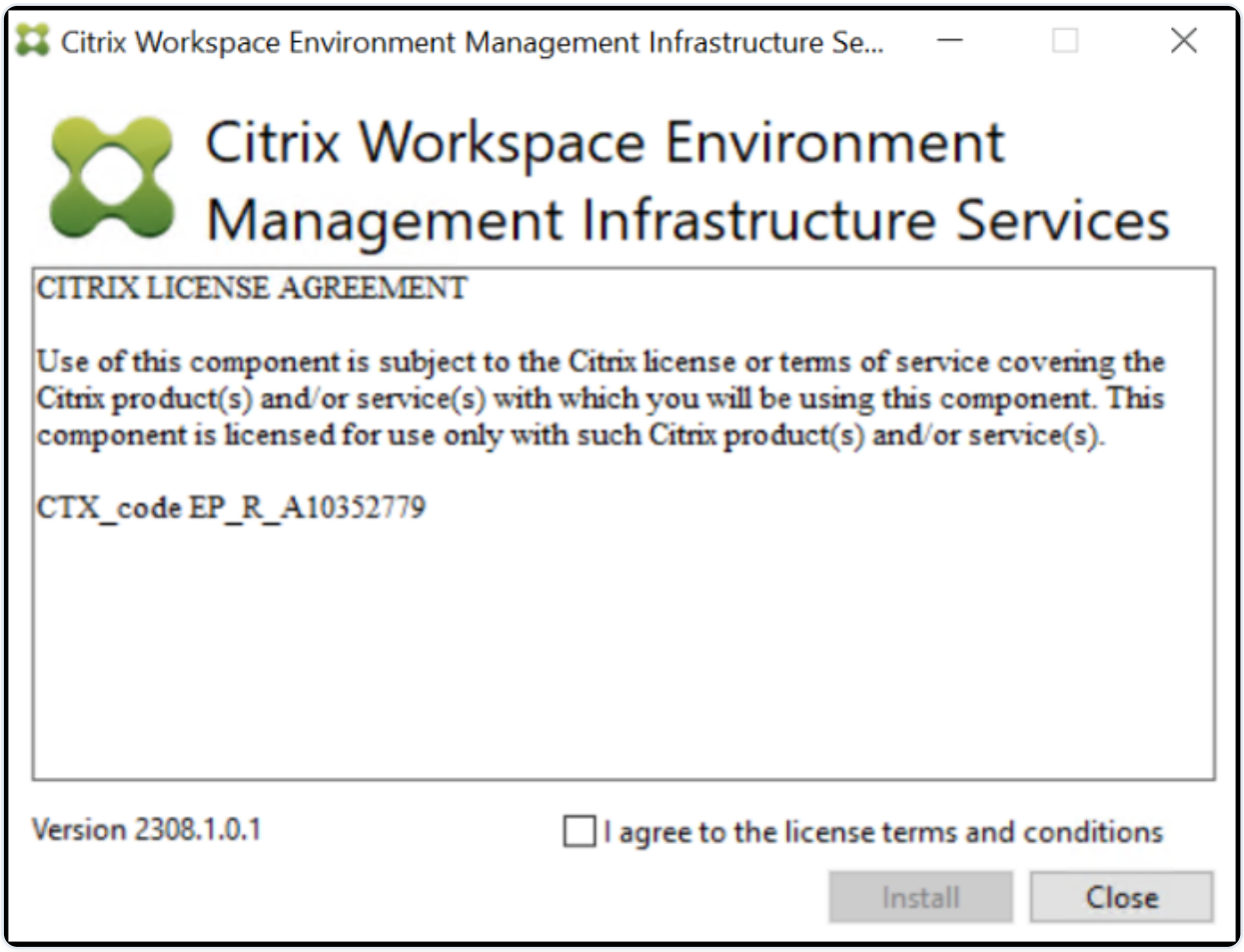
Step 1: Install the infrastructure services

1. Download the latest WEM installer from the Citrix Virtual Apps and Desktops Advanced or Premium Edition Components downloads page `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/>`. Extract the zip file to a convenient folder.



2. Run **Citrix Workspace Environment Management Infrastructure Services.exe** on your infrastructure server.
3. Click **Install**.
4. Click **Next**.
5. Select “I agree to the license terms and conditions" in the license agreement.

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



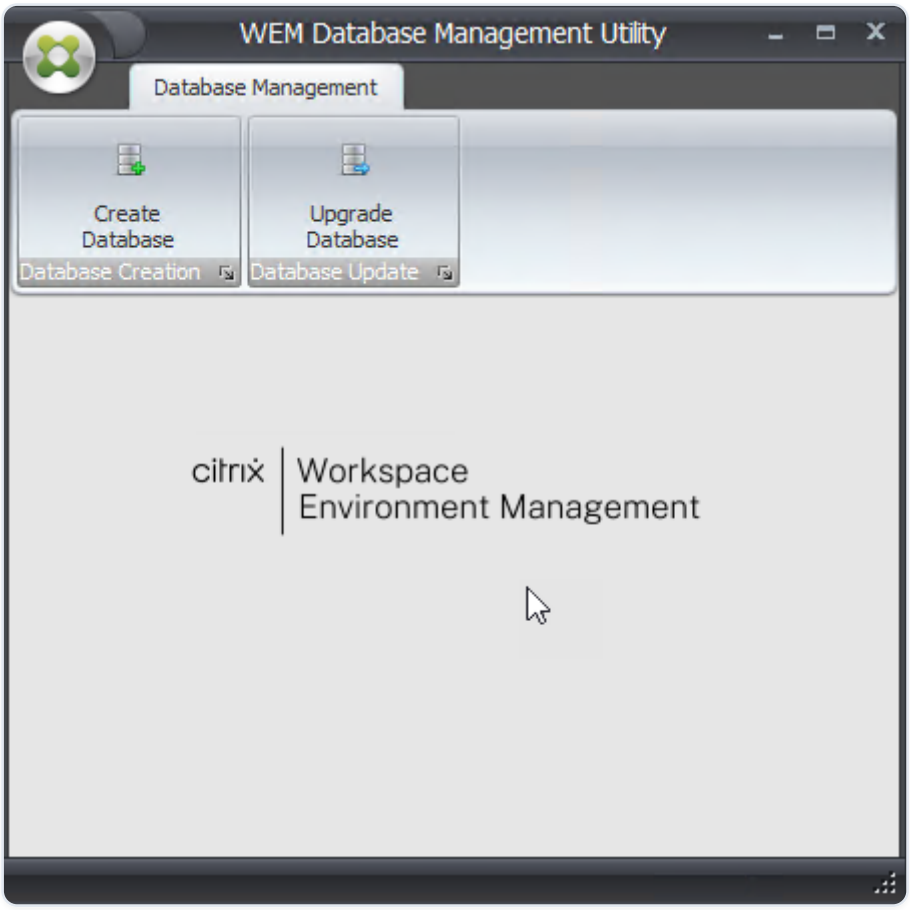
6. Follow the wizard instructions to complete the steps.

Step 2: Create a WEM database

1. In the database management utility, click **Create Database** to create a WEM database for your deployment. The database creation wizard appears.

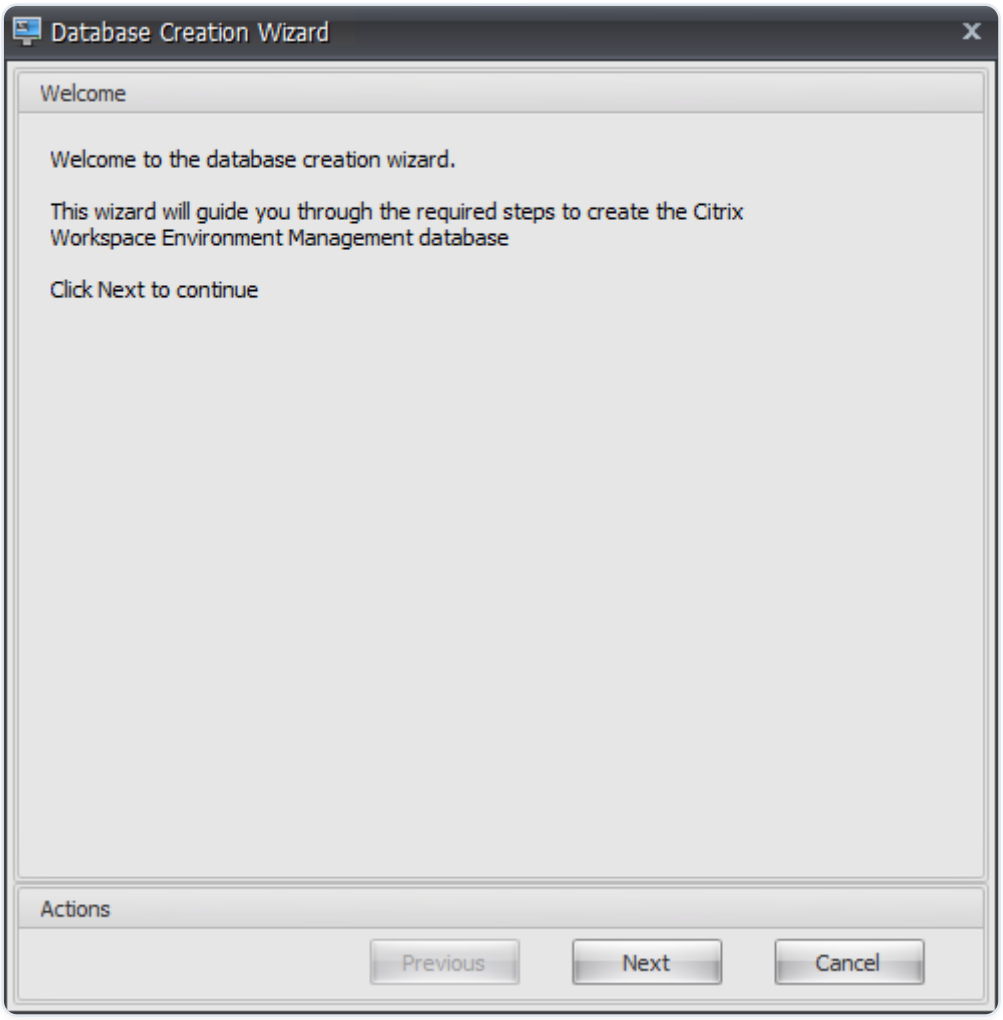
> **NOTE:**
>
> If you are using Windows authentication for your SQL Server, run the database creation utility under an identity that has system administrator permissions.

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



2. On the Welcome page, click **Next**.

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

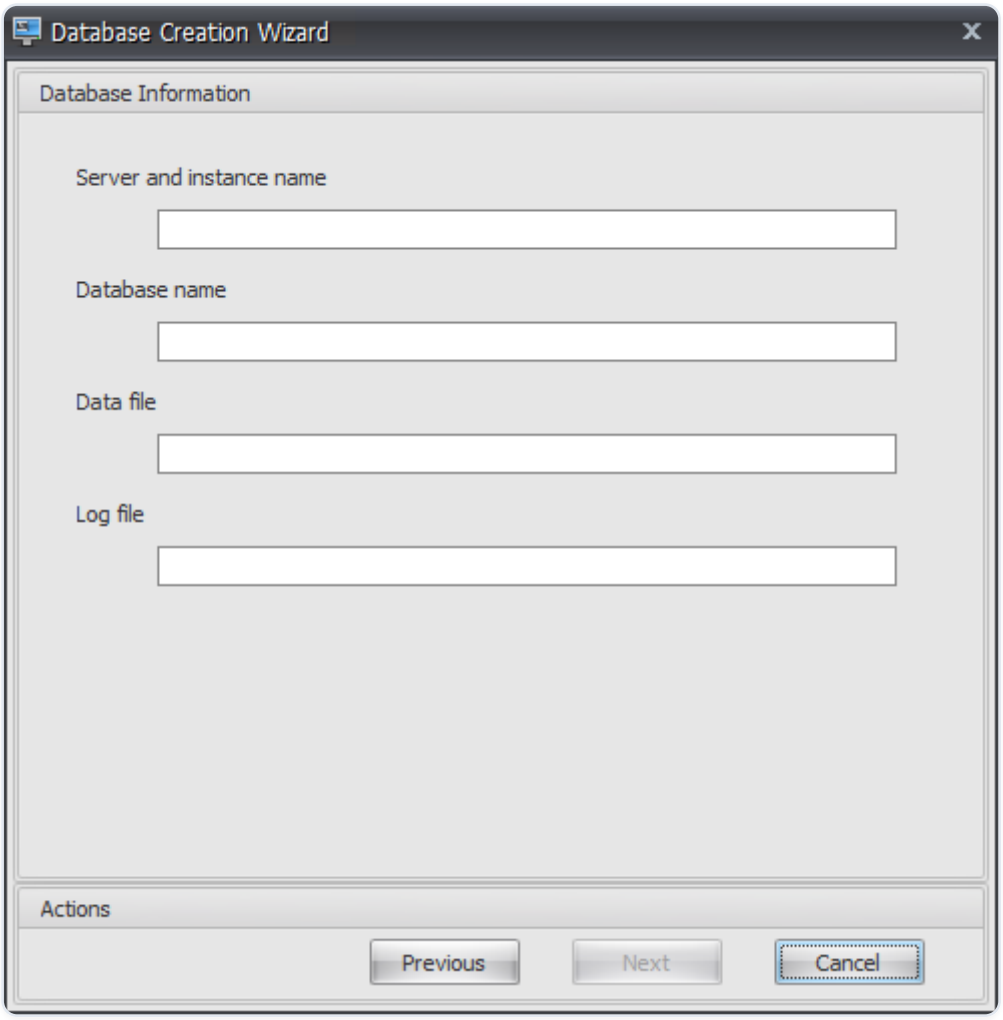


3. On the Database Information page, type the required information and then click **Next**.

NOTE:

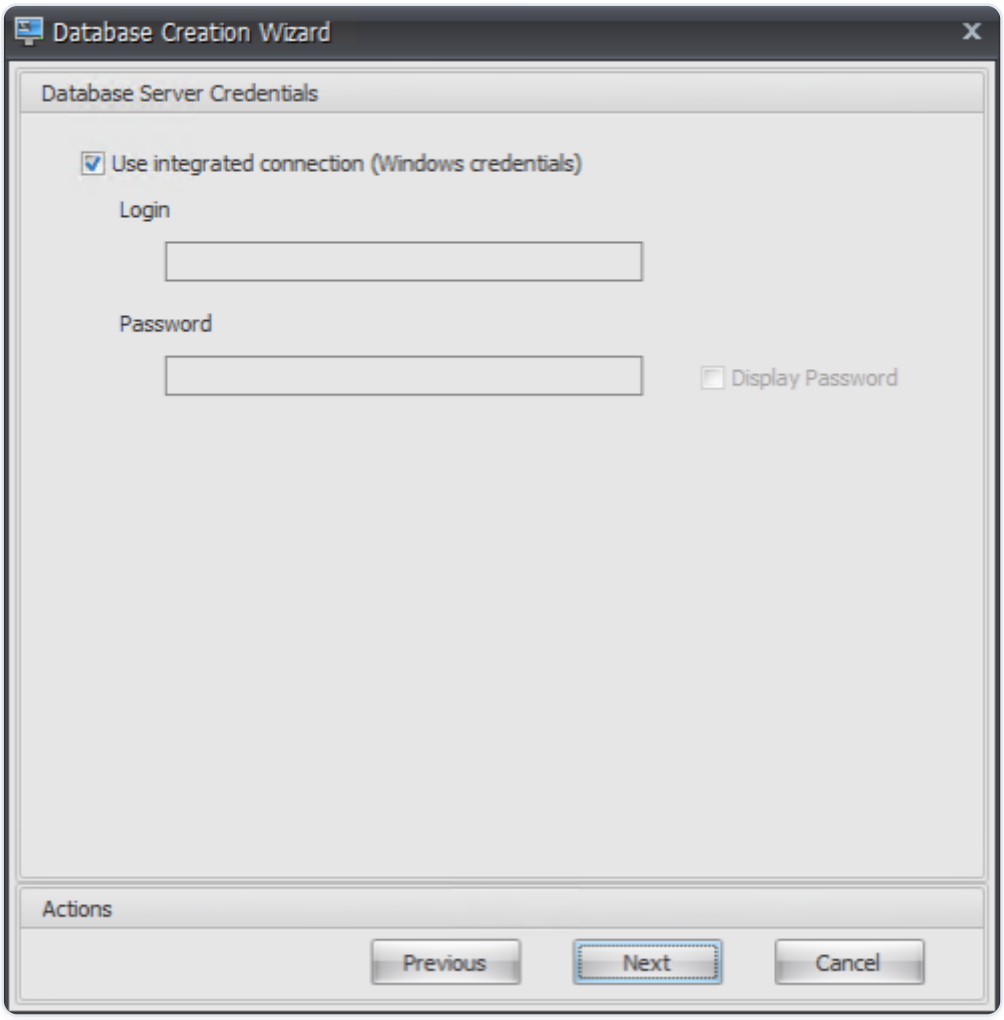
- For the server and instance name, type the machine name, fully qualified domain name, or IP address.
- For the file paths, type the exact paths specified by your database administrator. Make sure that any auto-completed file paths are correct.

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



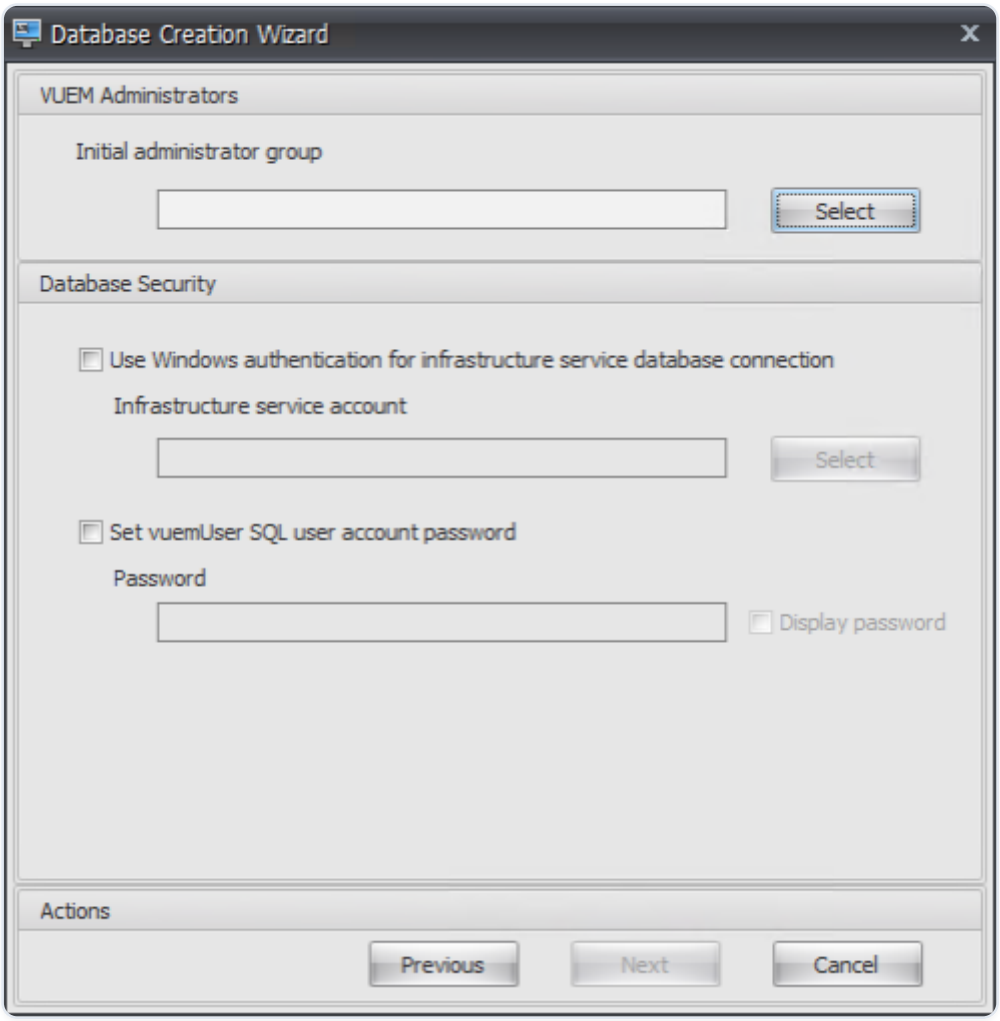
4. On the Database Server Credentials page, type the required information and then click **Next**.

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

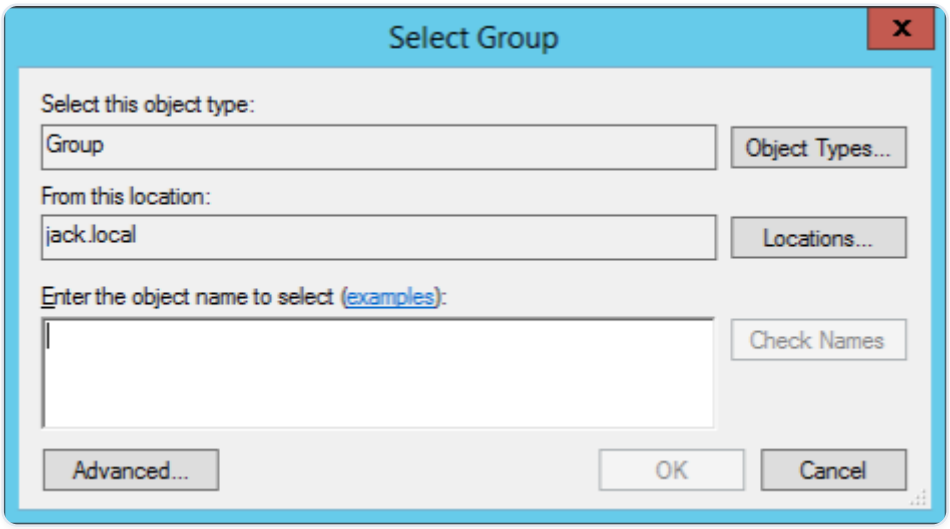


5. Under VUEM Administrators, click **Select**.

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



6. In the Select Group window, type a user group with administration permissions to the administration console, click **Check Names**, and then click **OK**.

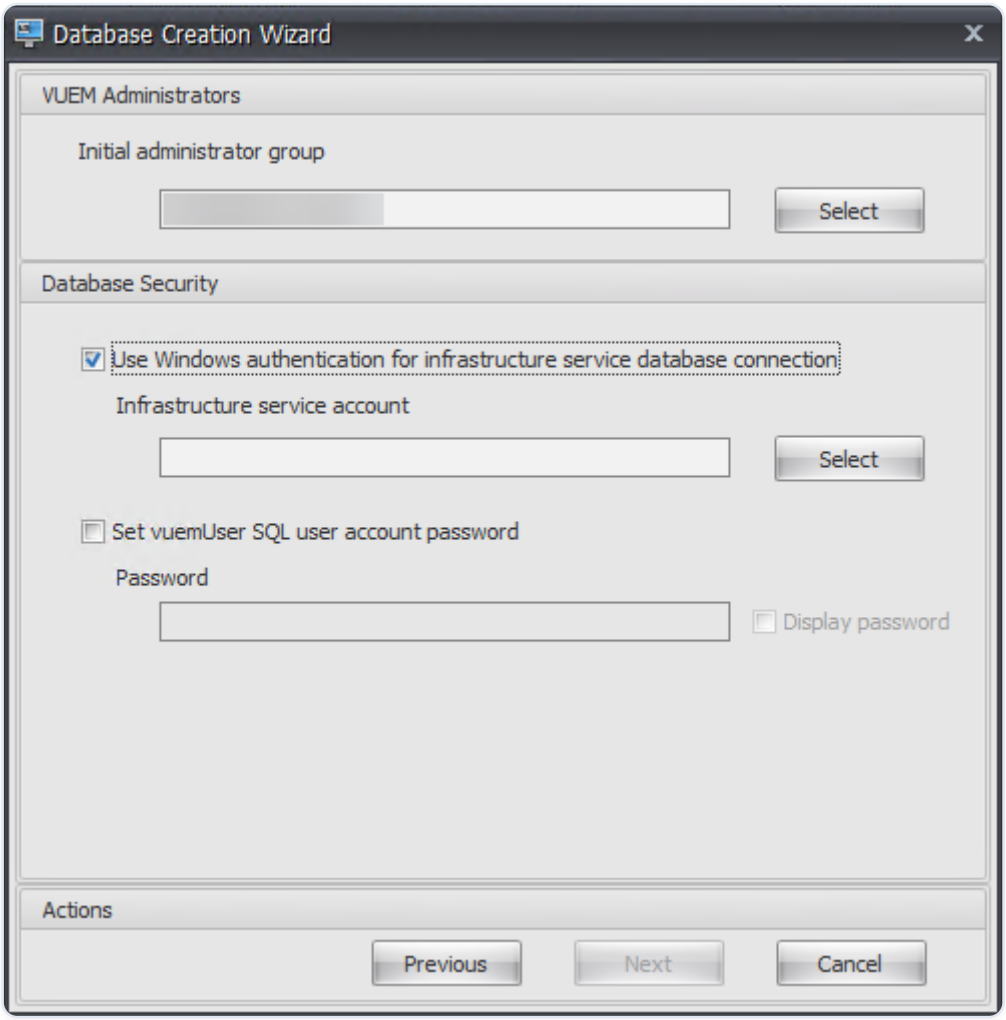


7. Under Database Security, select **Use Windows authentication for infrastructure service database connection** and then click **Select**.

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

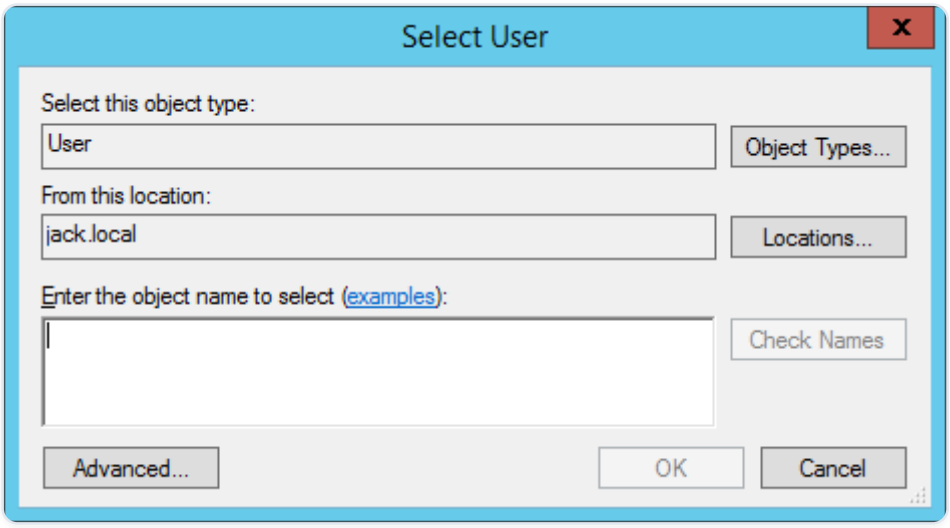
NOTE:

- If you select neither **Use Windows authentication for infrastructure service database connection** nor **Set vuemUser SQL user account password**, the SQL user account is used by default.
- To use your own vuemUser SQL account password (for example, if your SQL policy requires a more complex password), select **Set vuemUser SQL user account password**.

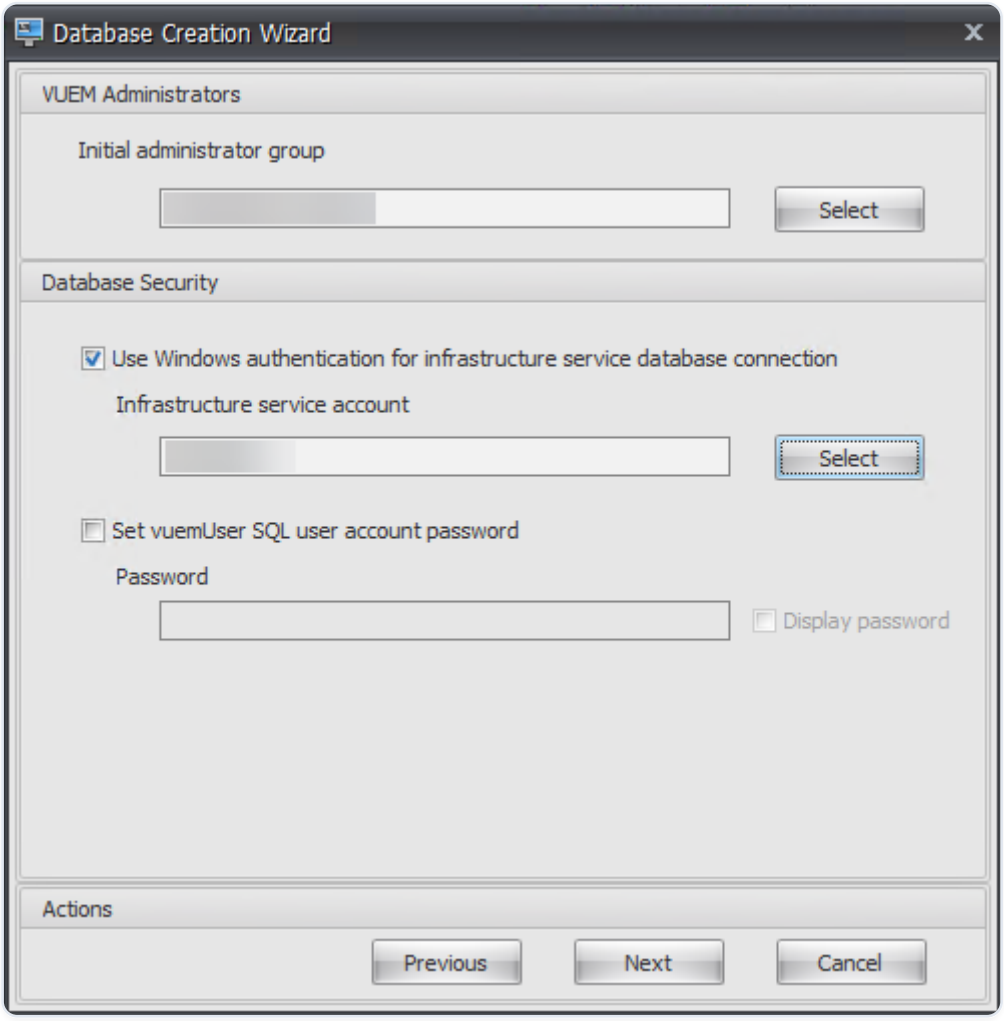


8. In the Select User window, type the name of the infrastructure service account, click **Check Names**, and then click **OK**.

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

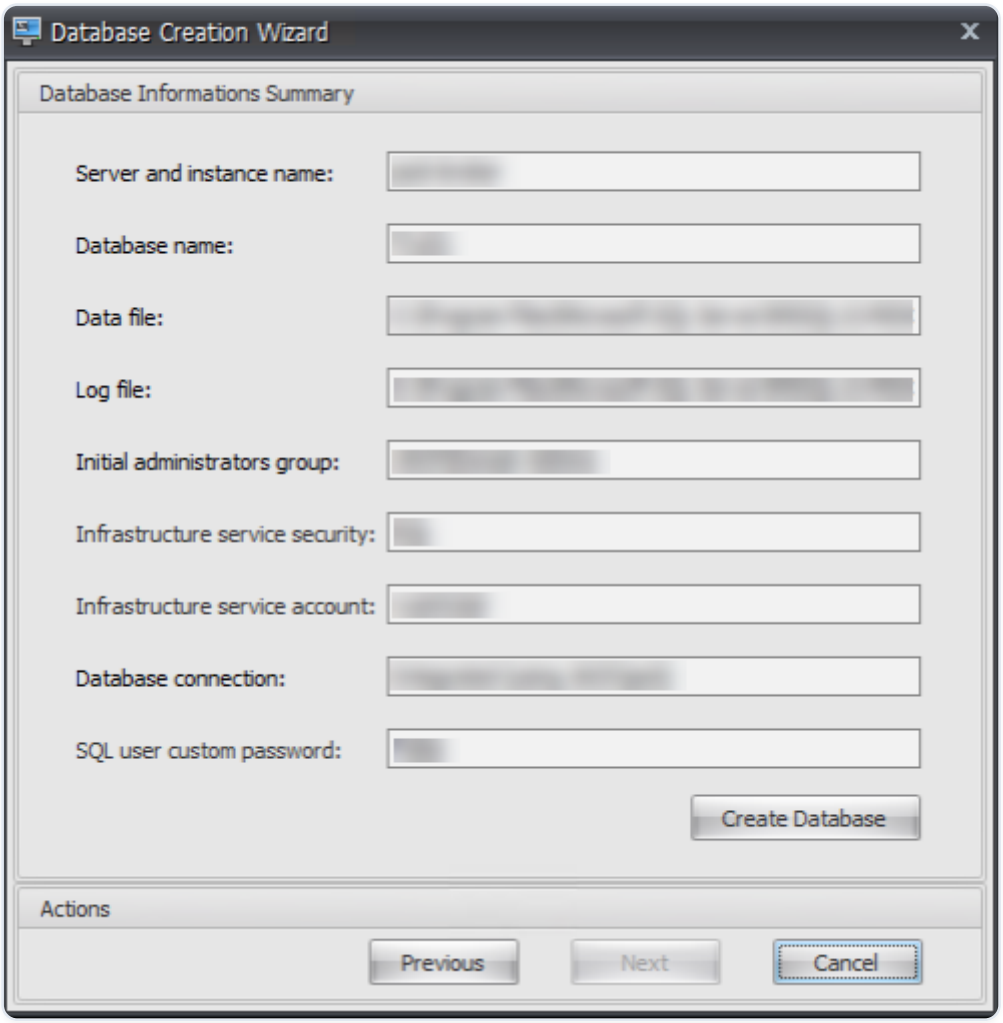


9. Click **Next**.

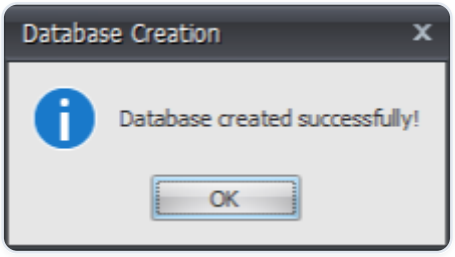


10. On the Database Information Summary page, click **Create Database**.

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

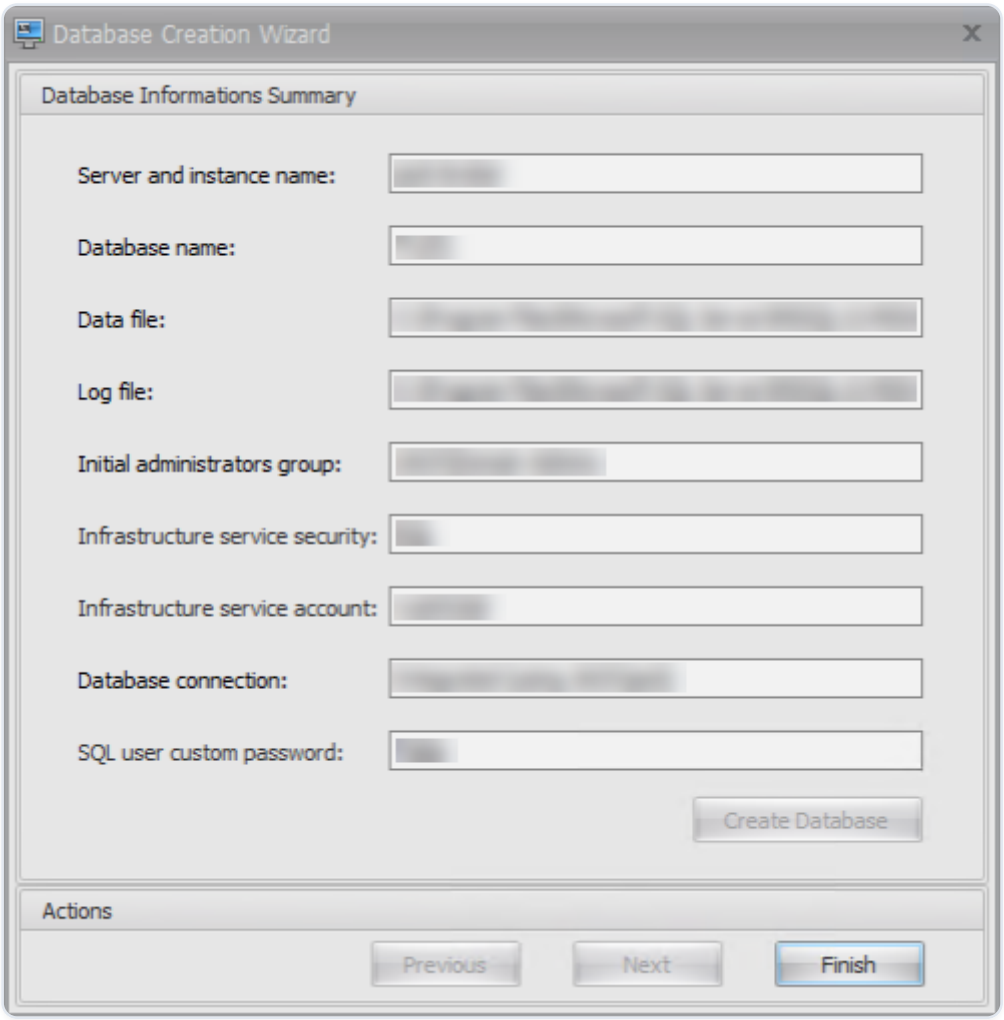


11. Click **OK**.



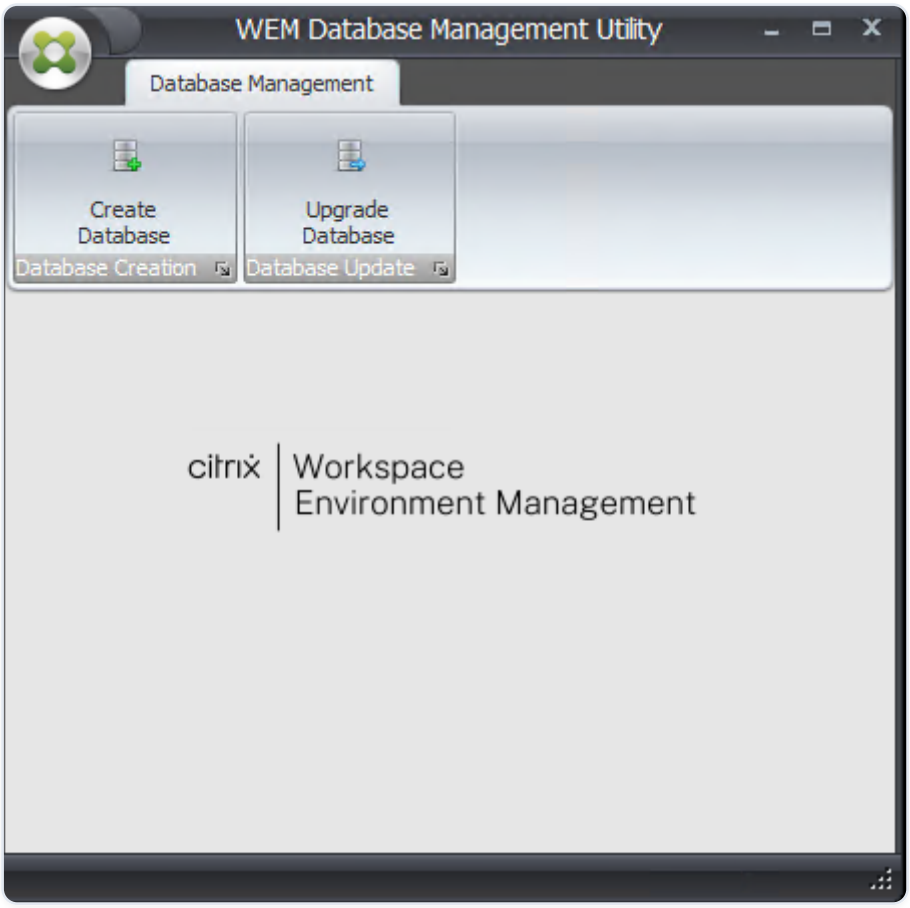
12. On the Database Information Summary page, click **Finish**.

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



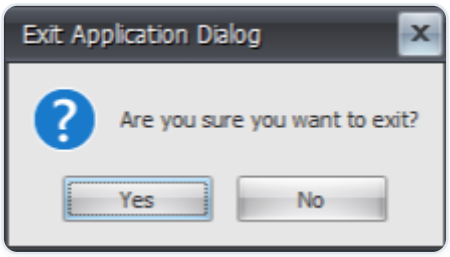
13. Close the **WEM Database Management Utility**.

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



14. In the Exit Application Dialog, click **Yes**.

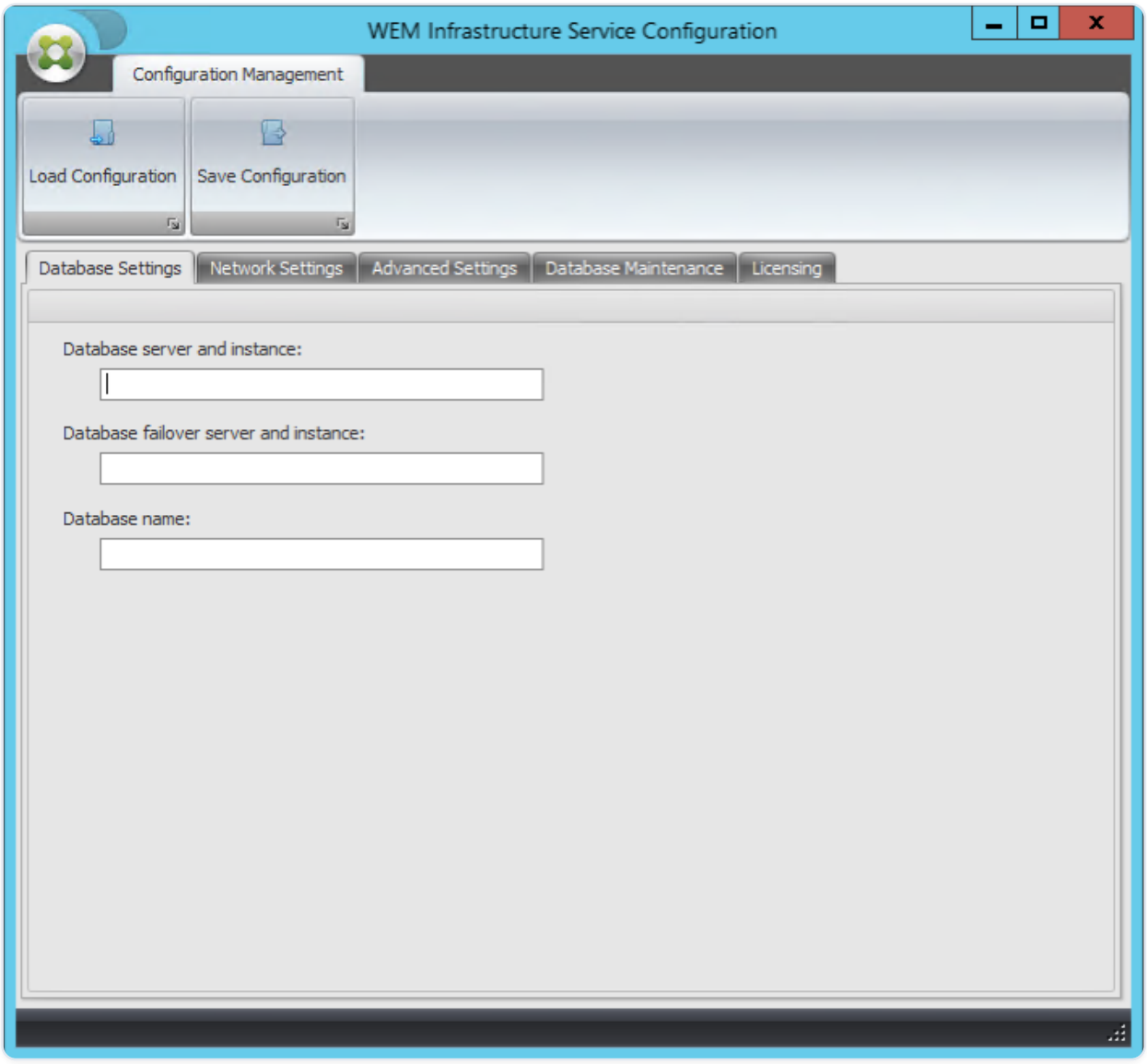
> **NOTE:**
>
> If an error occurs during the database creation, check the log file “Citrix WEM Database Management Utility Debug Log.log” in the infrastructure services installation folder for more information.



Step 3: Configure infrastructure services

1. Open the **WEM Infrastructure Service Configuration Utility** from the **Start** menu.
2. On the **Database Settings** tab, type the required information.

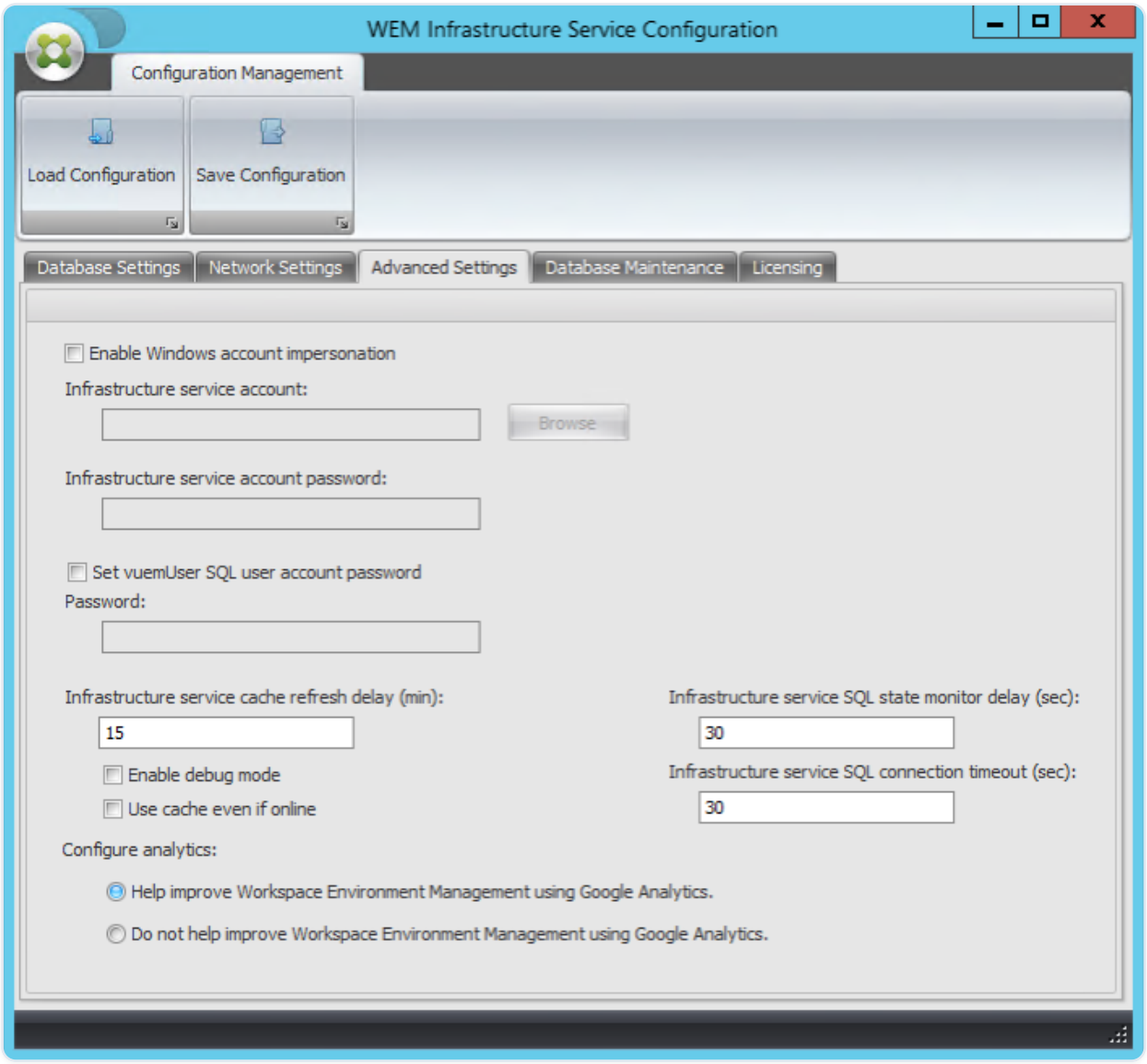
© 1997–2026 Citrix Systems, Inc. All rights reserved.



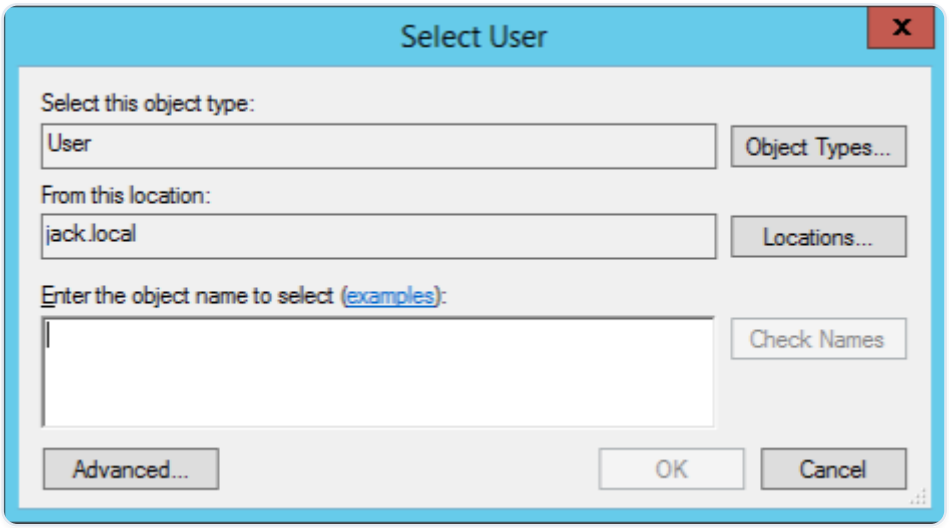
3. On the **Advanced Settings** tab, select **Enable Windows account impersonation** and then click **Browse**.

> **NOTE:**
>
> Depending on the choices you made during WEM database creation in Step 2, select **Enable Windows account impersonation** or **Set vuemUser SQL user account password**.

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

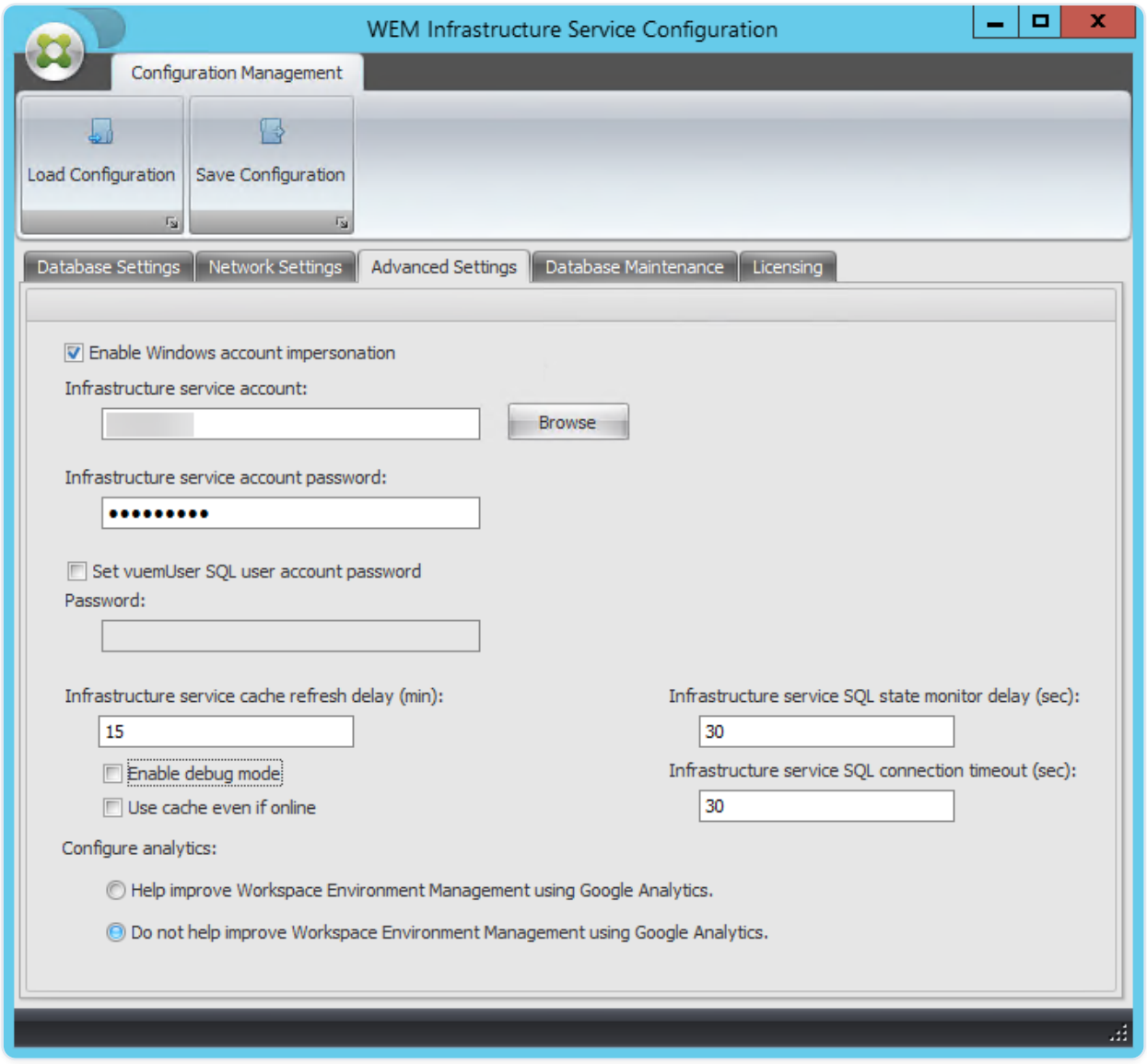


4. Type a user name, click **Check Names**, and then click **OK**.



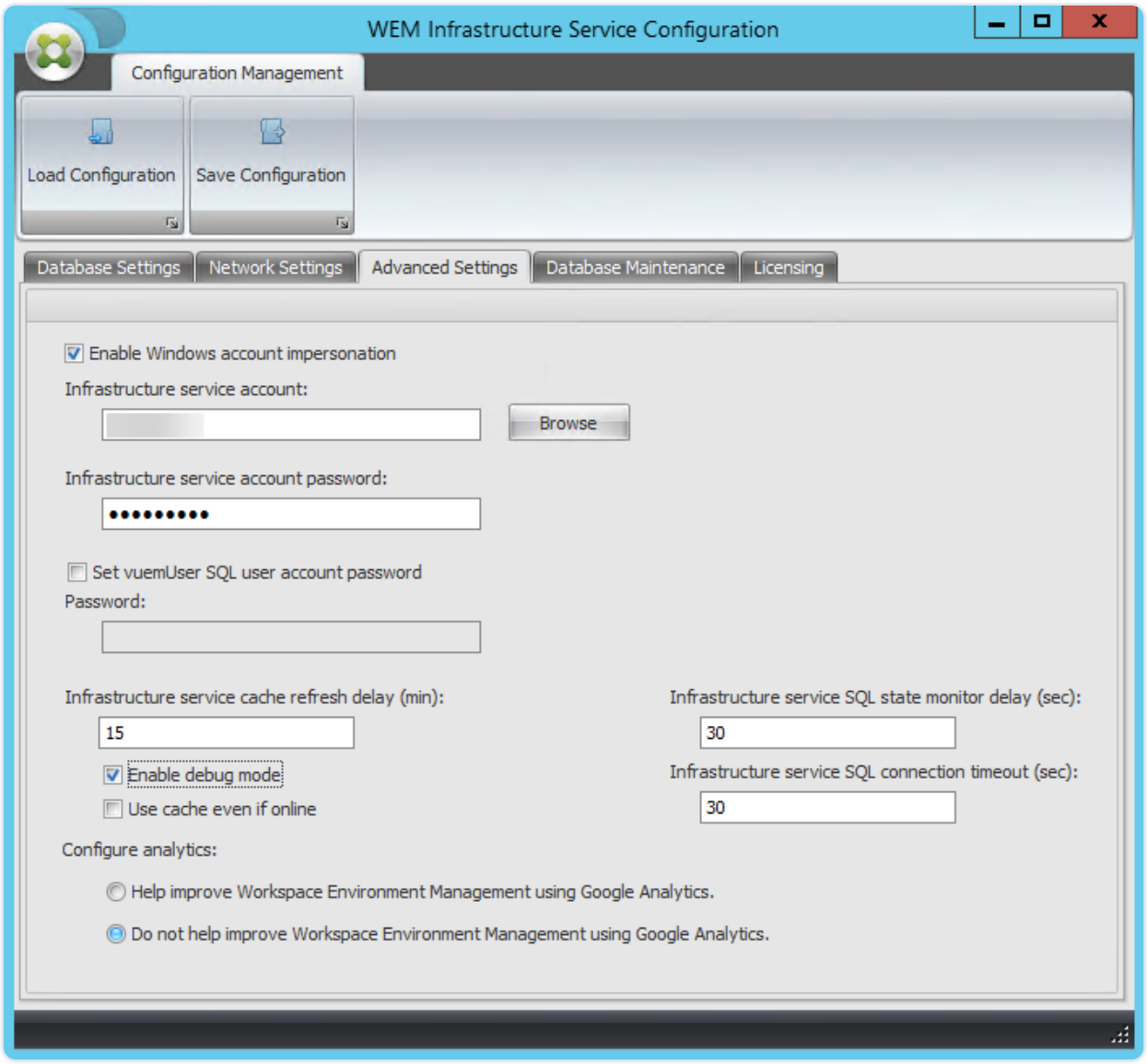
5. Type the infrastructure service account password.

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



6. Select **Enable debug mode**.

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

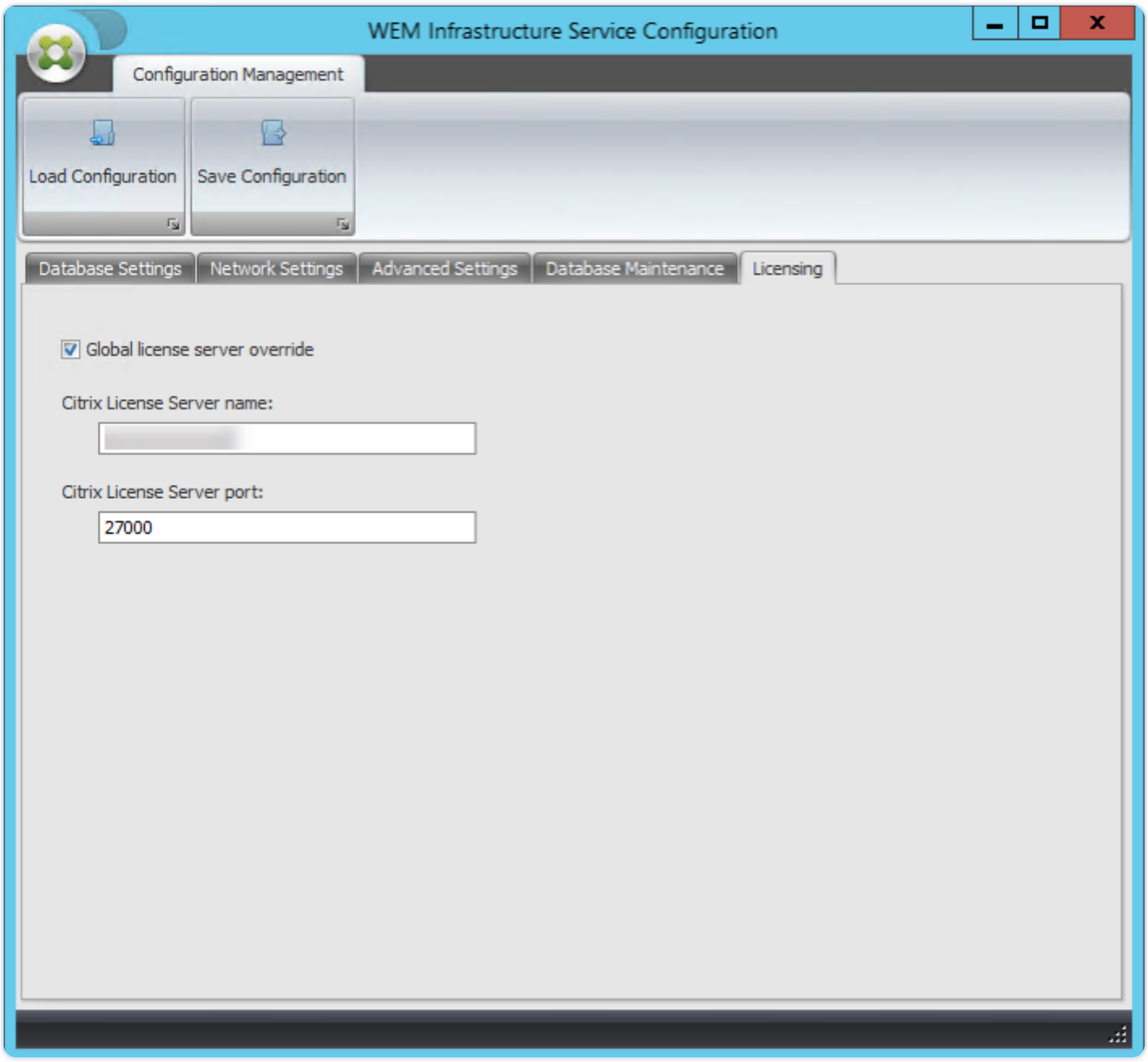


7. On the **Licensing** tab, select **Global license server override**, type your license information, and then click **Save Configuration.**

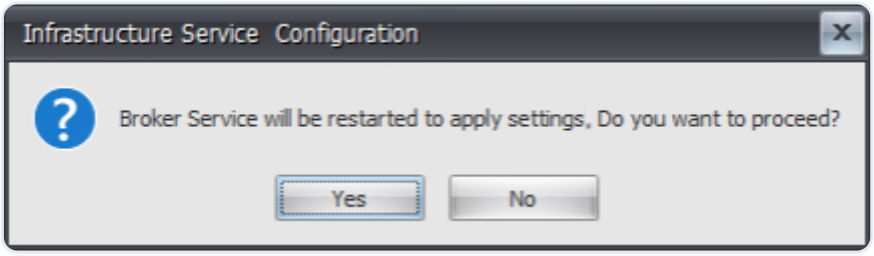
NOTE:

- For Citrix License Server name, type the machine name, fully qualified domain name, or IP address of the license server.
- For Citrix License Server port, the default port is 27000.

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



8. Click **Yes**.

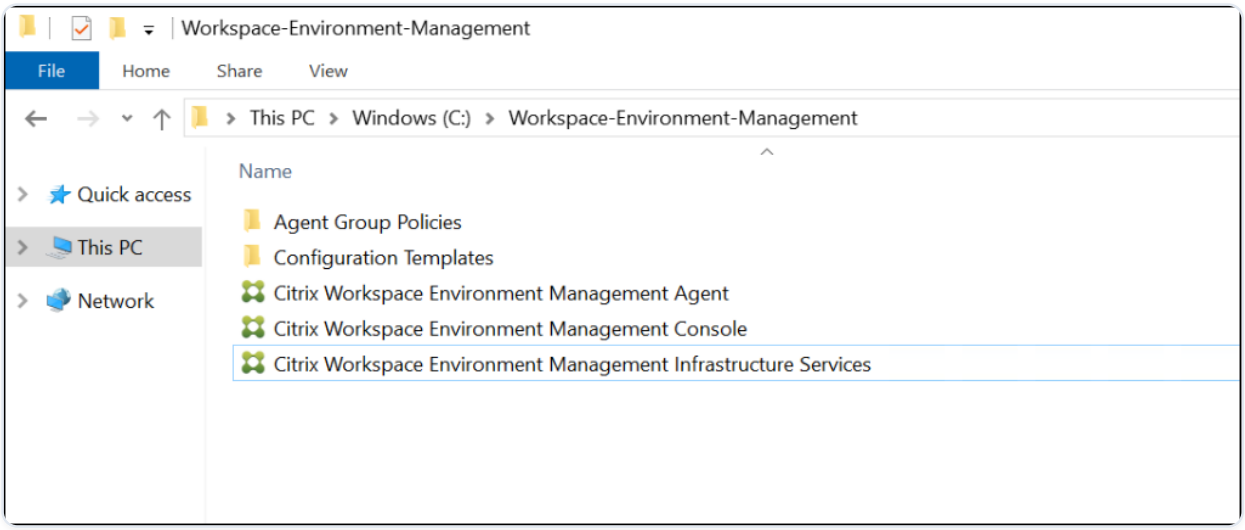


9. Close the **WEM Infrastructure Service Configuration** utility.

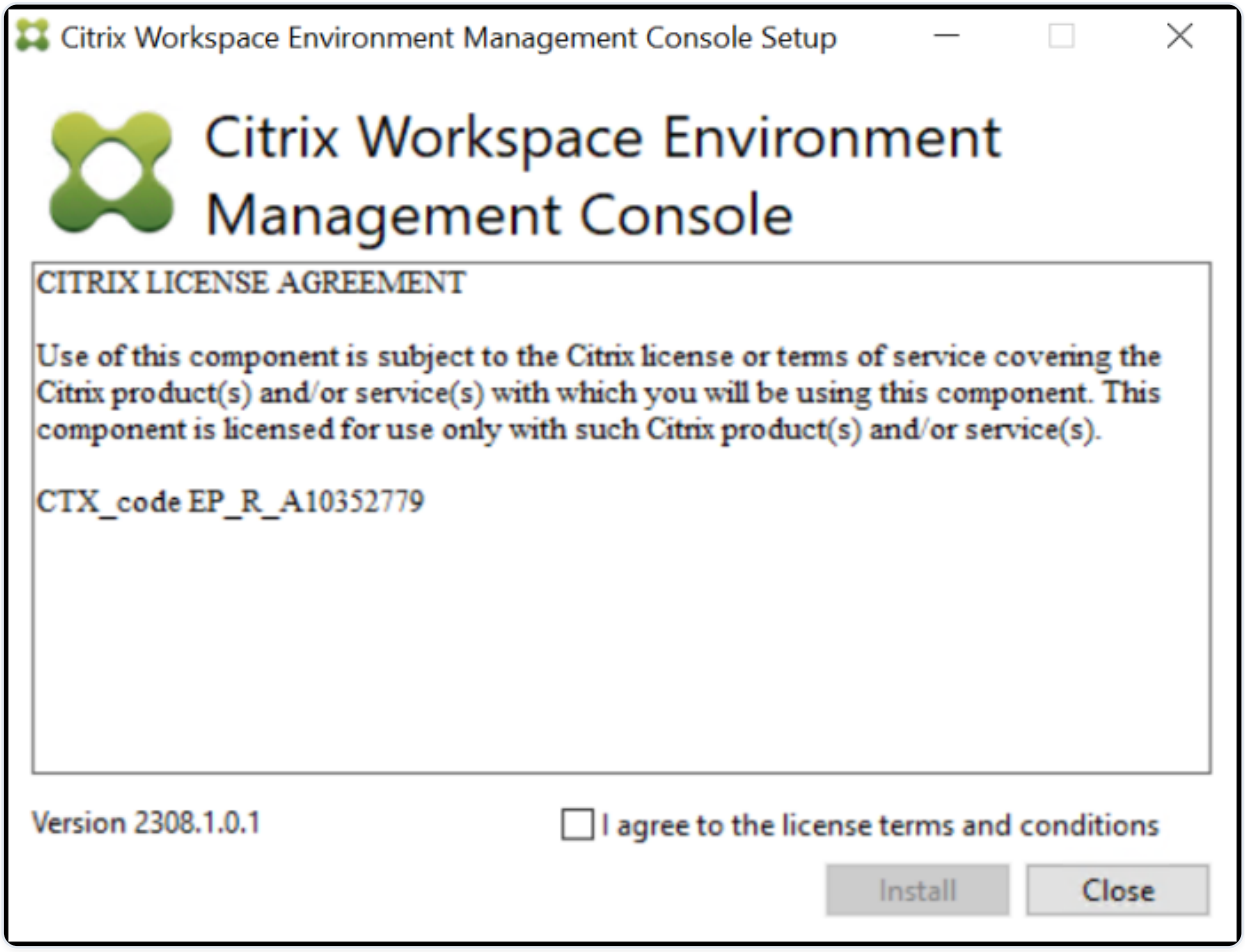
Step 4: Install the administration console

1. Run **Citrix Workspace Environment Management Console.exe**.

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



2. On the License Agreement page, select “I agree to the license terms and conditions”.

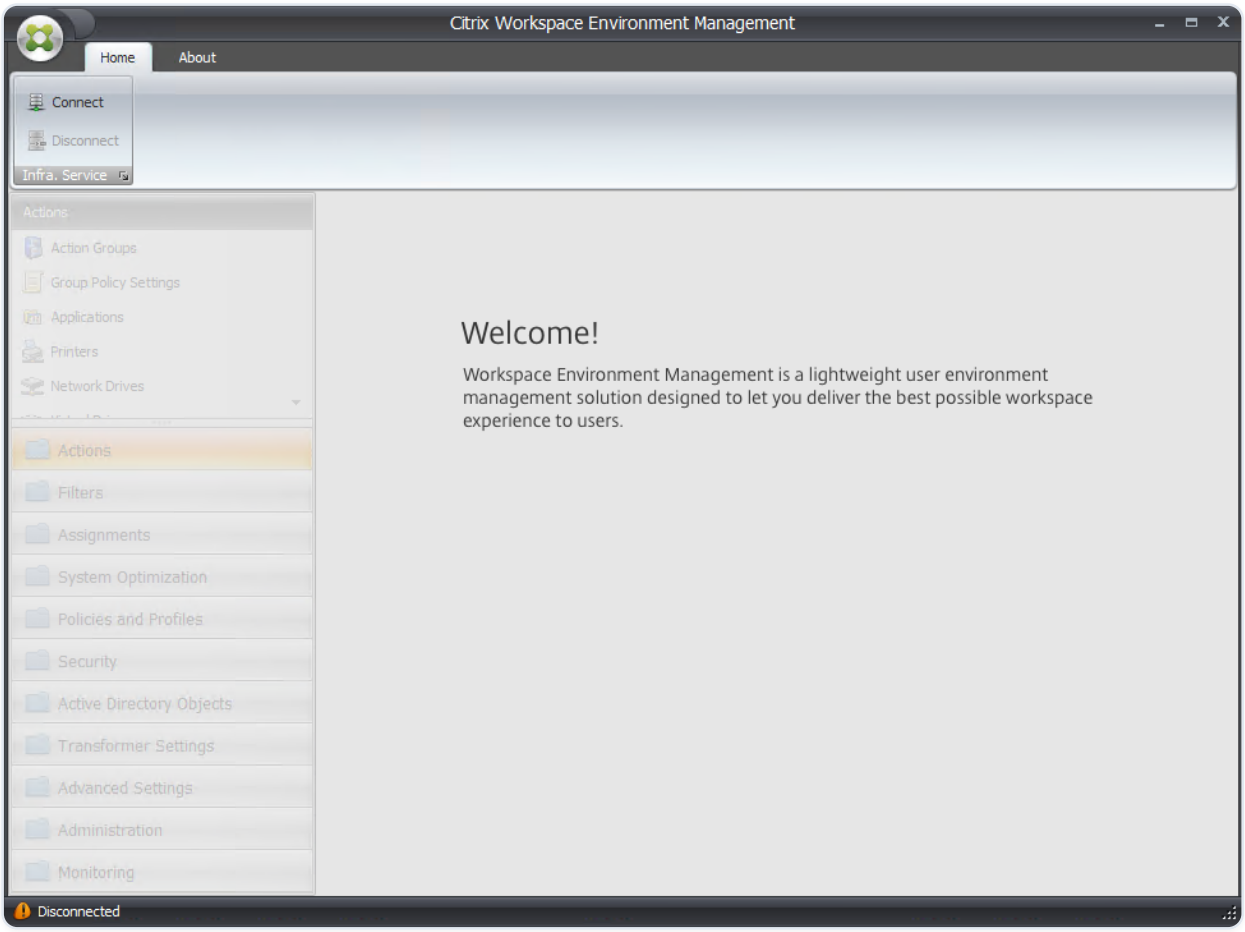


3. Follow the wizard instructions to complete the steps.

Step 5: Configure configuration sets

1. Open the **WEM Administration Console** from the **Start** menu and click **Connect**.

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

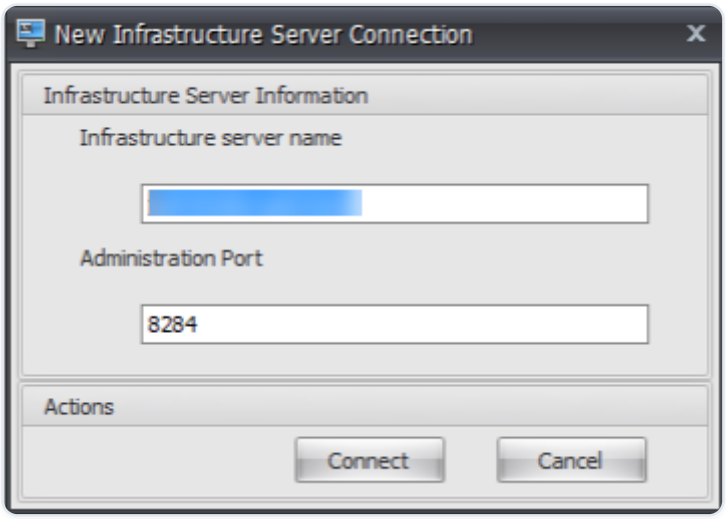


2. In the New Infrastructure Server Connection window, check the information and then click **Connect**.

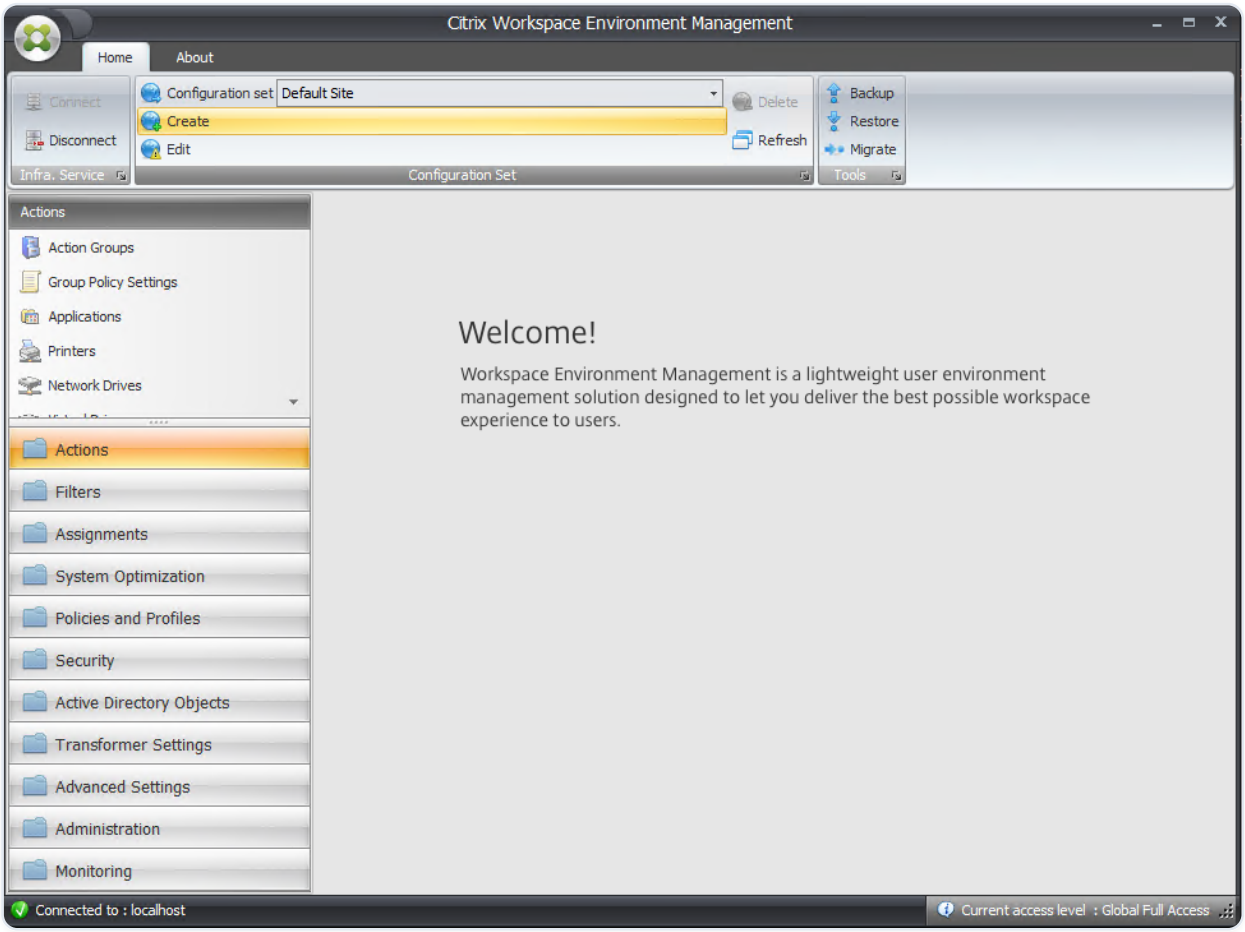
NOTE:

- For Infrastructure server name, type the machine name, fully qualified domain name, or IP address of the WEM infrastructure server.
- For Administration port, the default port is 8284.

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

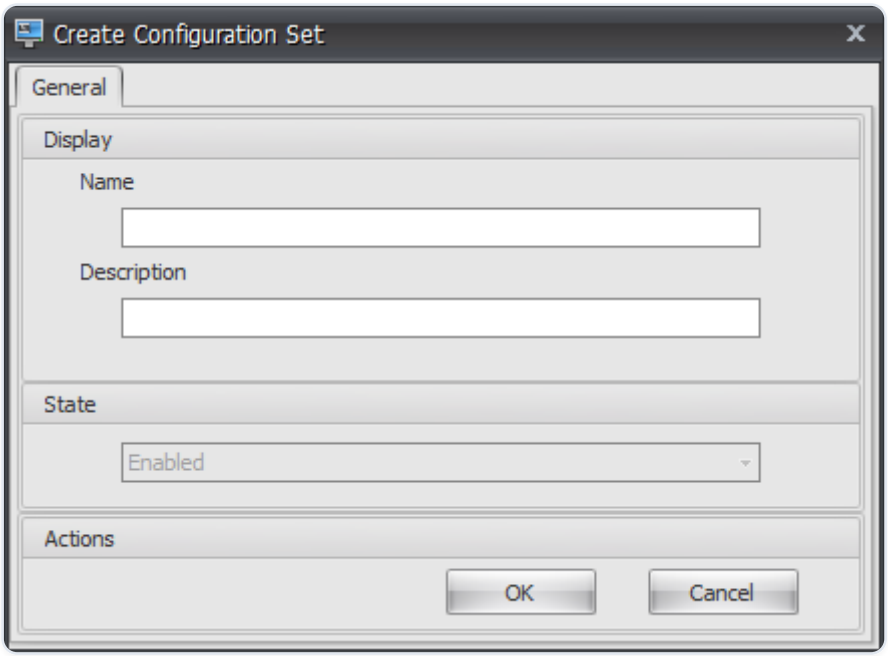


3. On the **Home** tab, on the ribbon, click **Create** to create your configuration set.

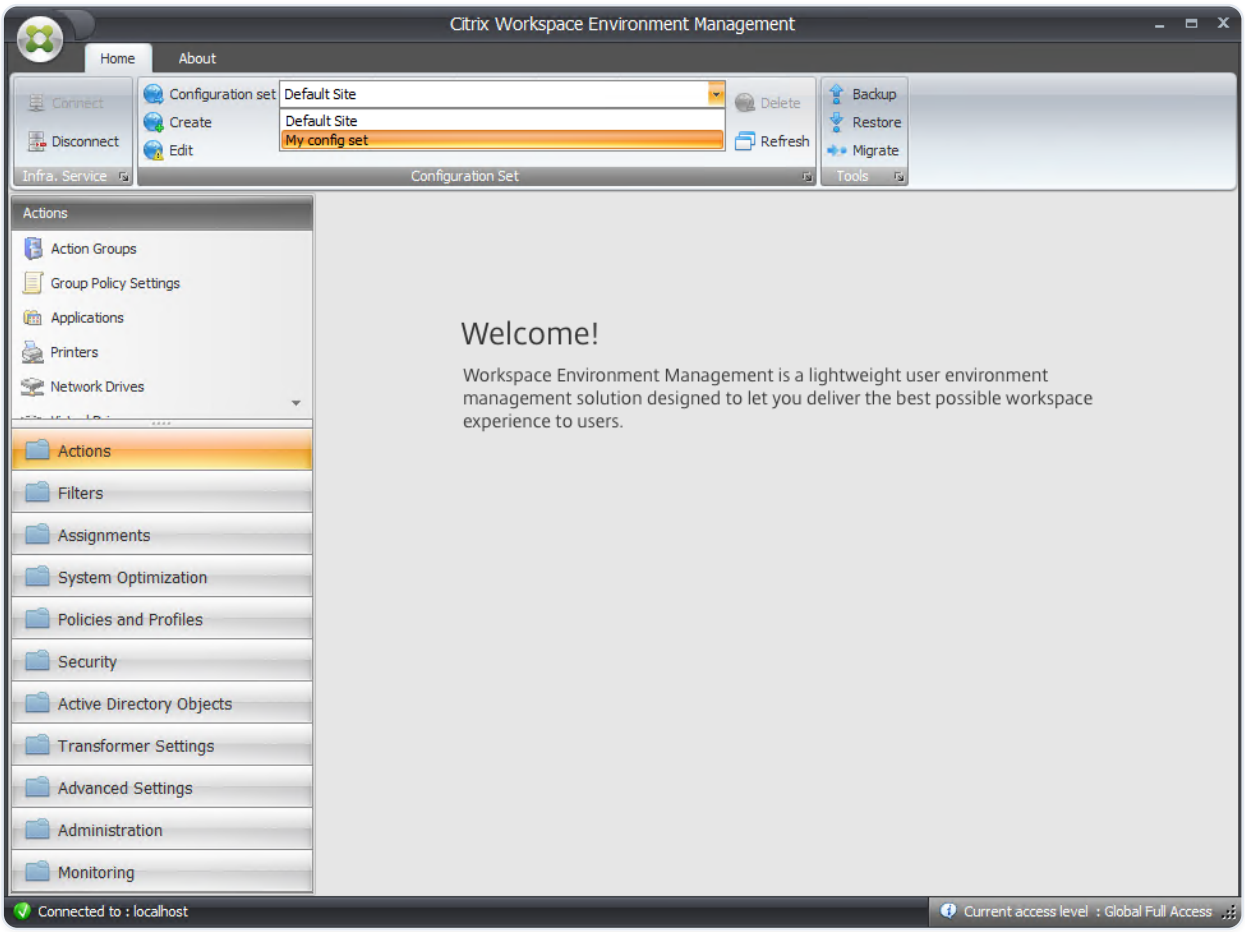


4. In the Create Configuration Set window, type a name and description for your configuration set and then click **OK**.

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

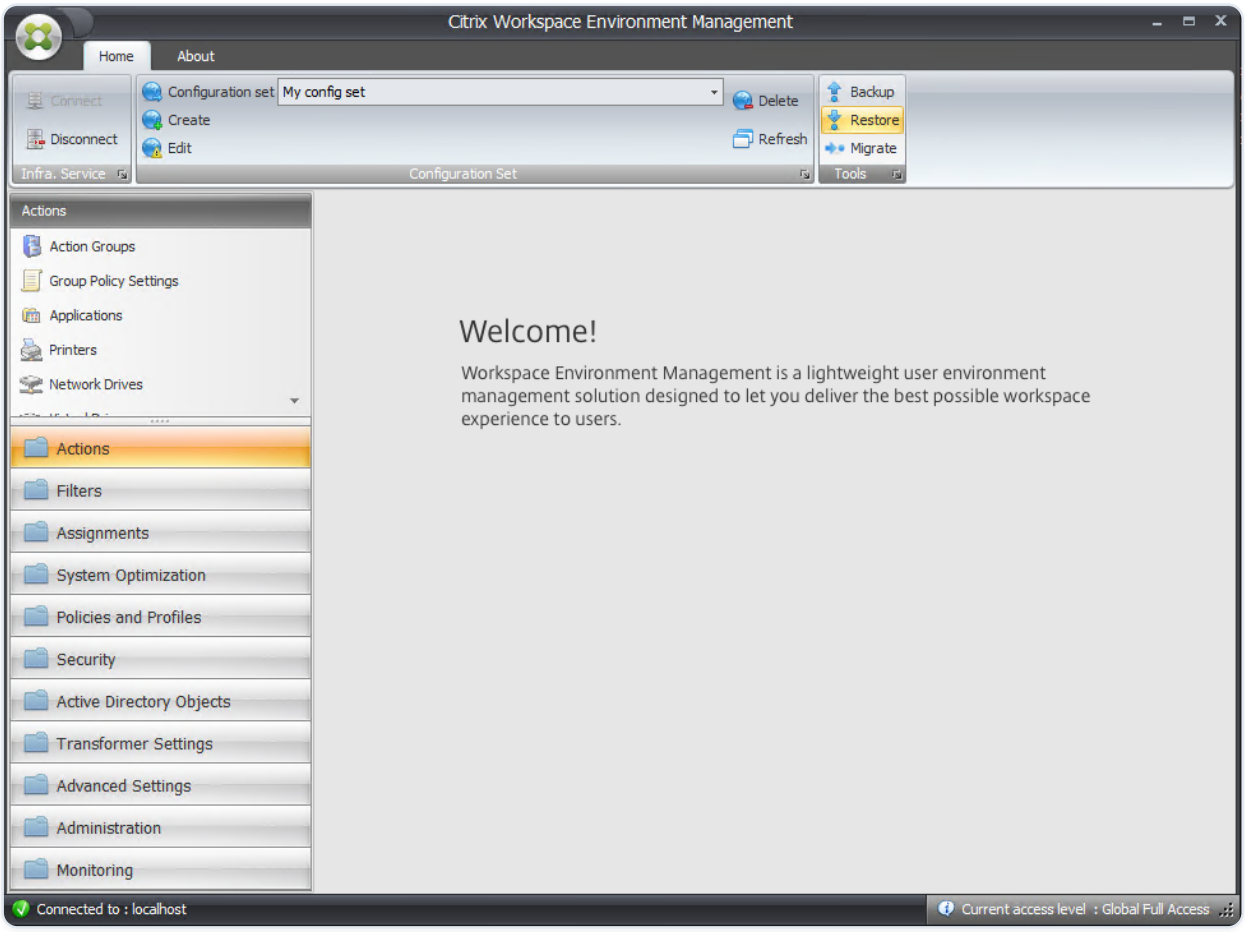


5. On the ribbon, under **Configuration Set**, select the newly created configuration set.



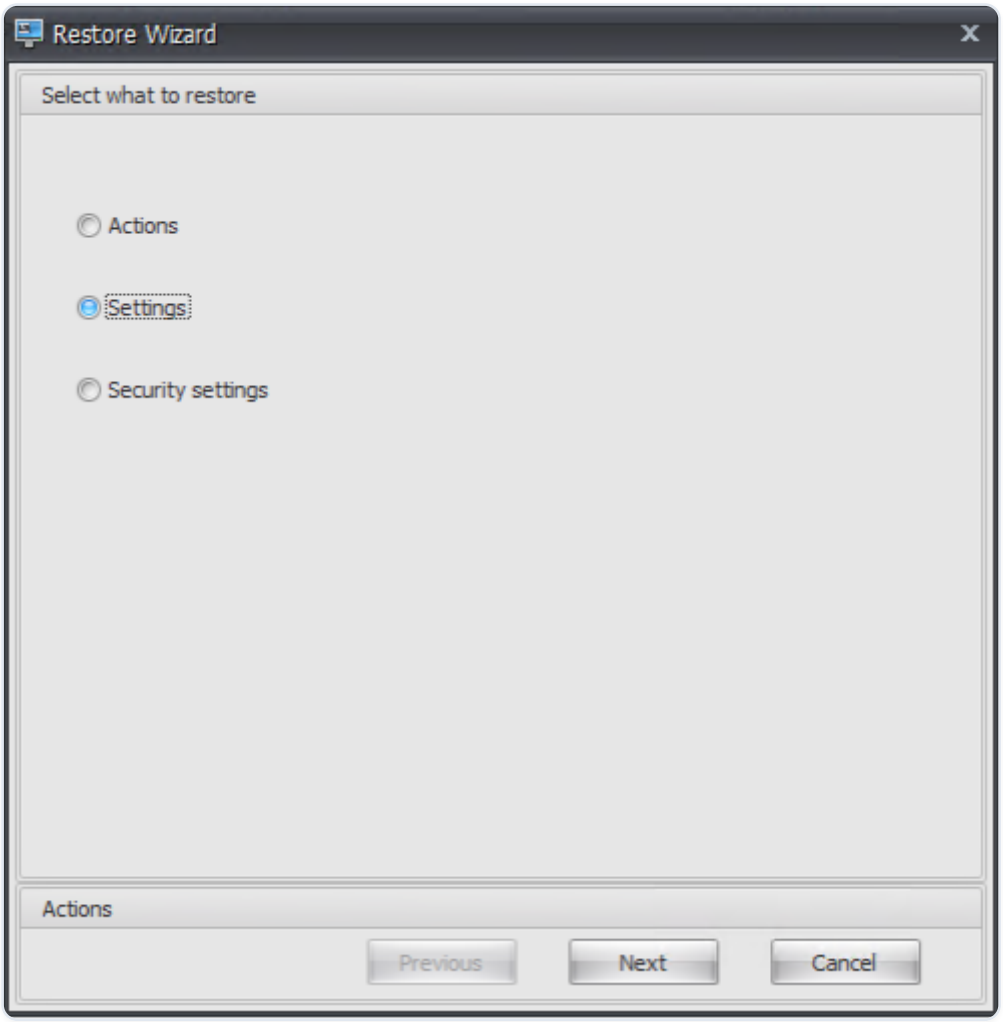
6. On the ribbon, under **Backup**, click **Restore**. The Restore wizard appears.

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



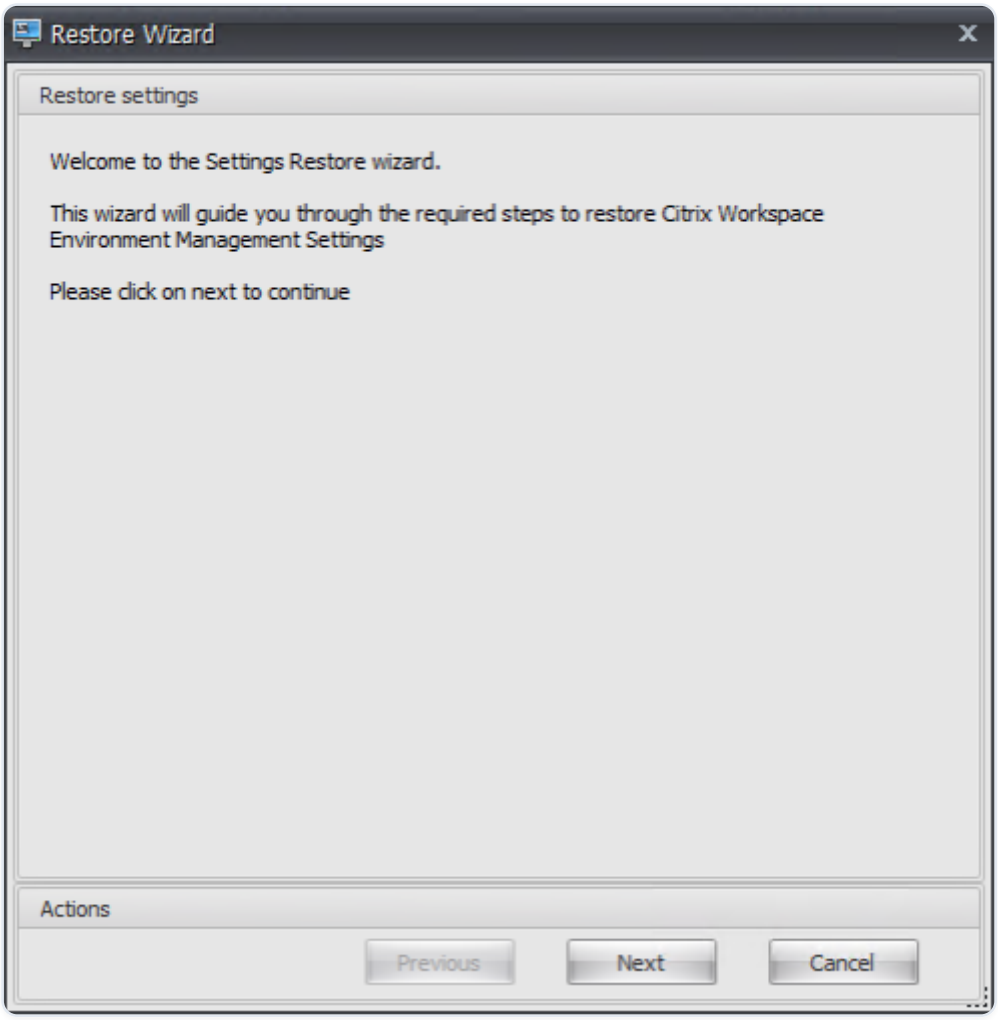
7. On the Select what to restore page, select **Settings** and then click **Next**.

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



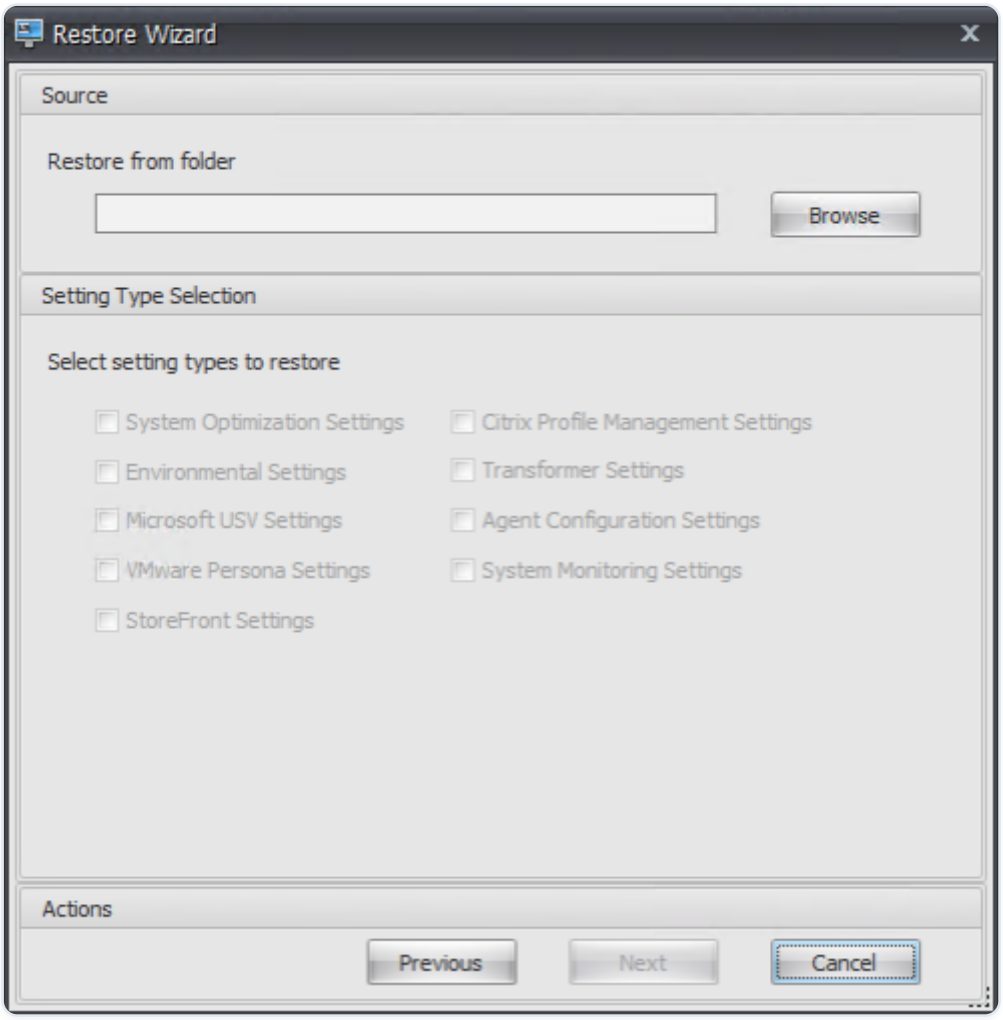
8. On the Restore settings page, click **Next**.

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

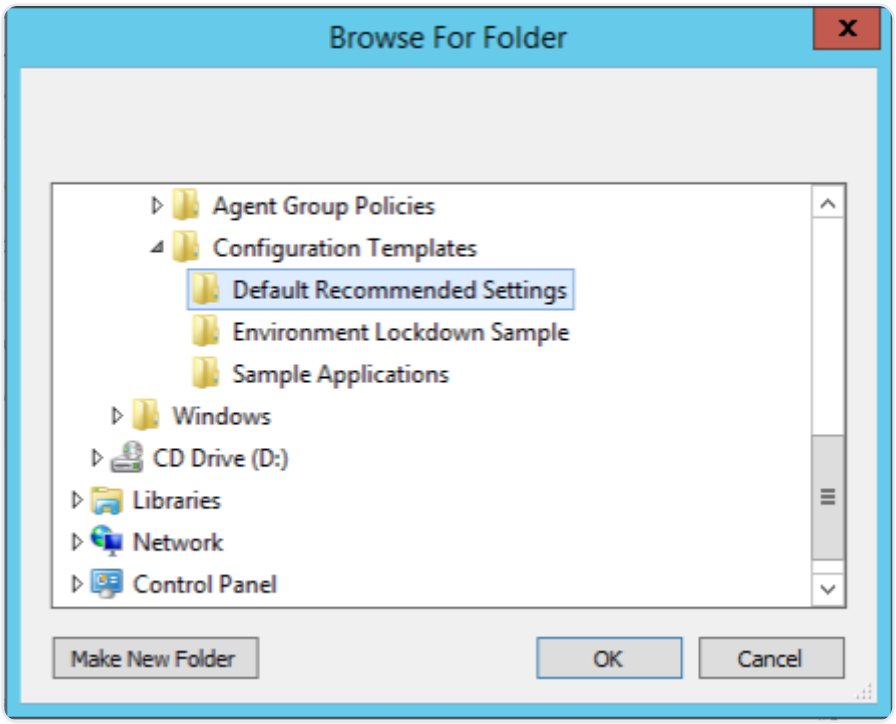


9. On the Source page, click **Browse**.

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

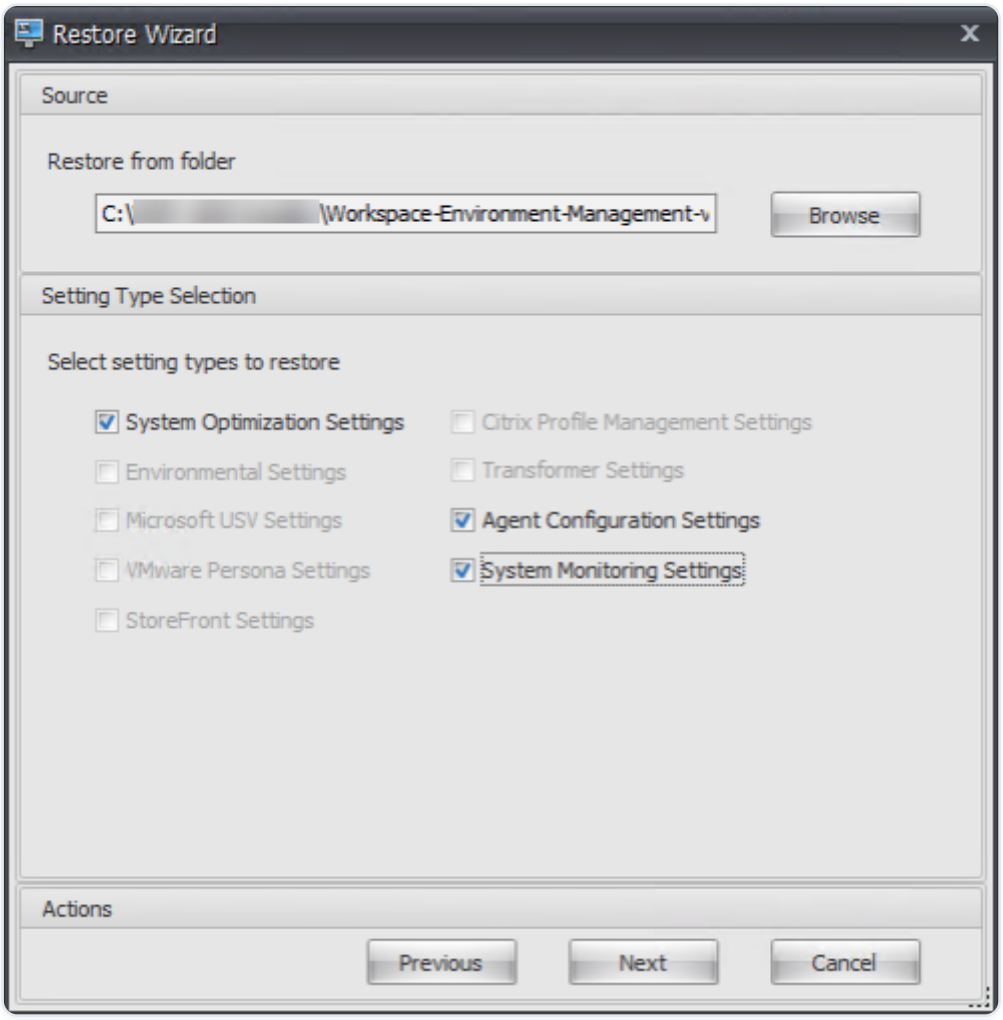


10. In the Browse For Folder window, browse to the **Default Recommended Settings** folder (provided with Workspace Environment Management) and then click **OK**.



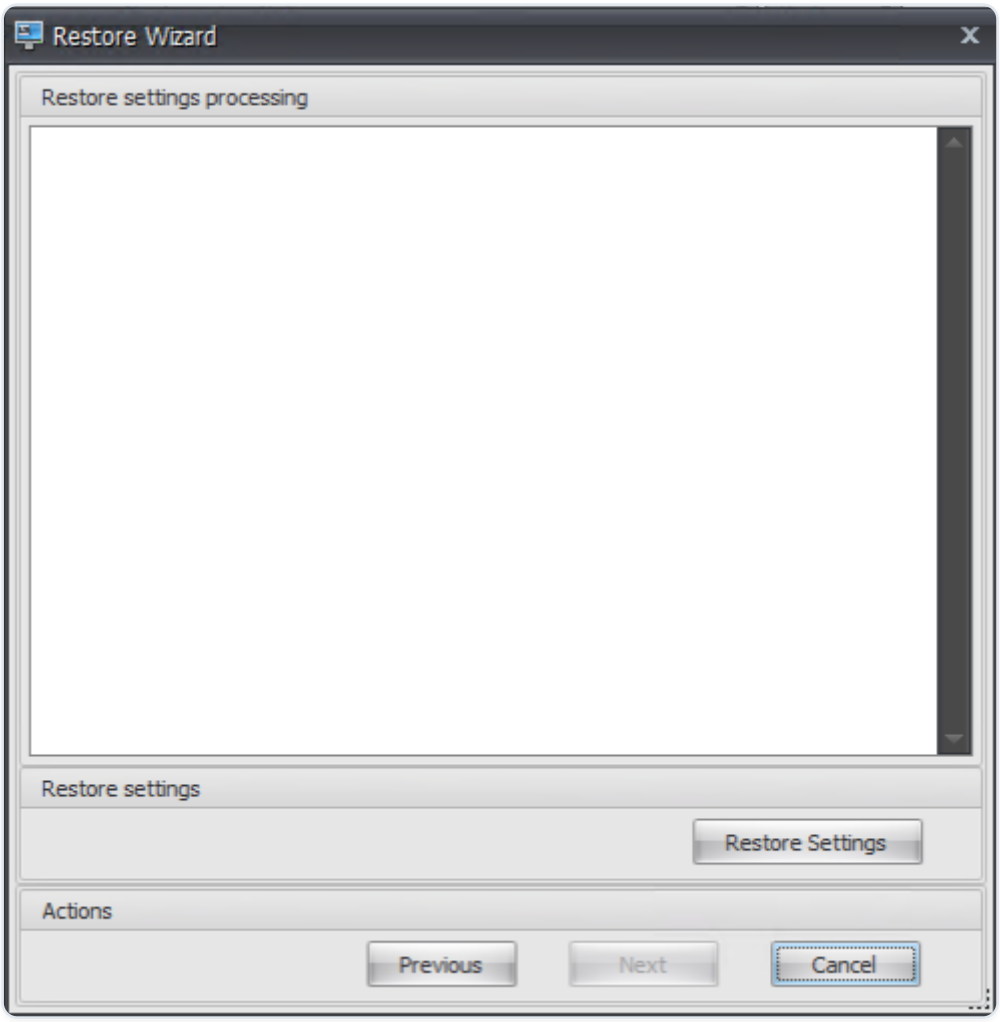
© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. On the Source page, select **System Optimization Settings**, **Agent Configuration Settings**, and **System Monitoring Settings**, and then click **Next**.

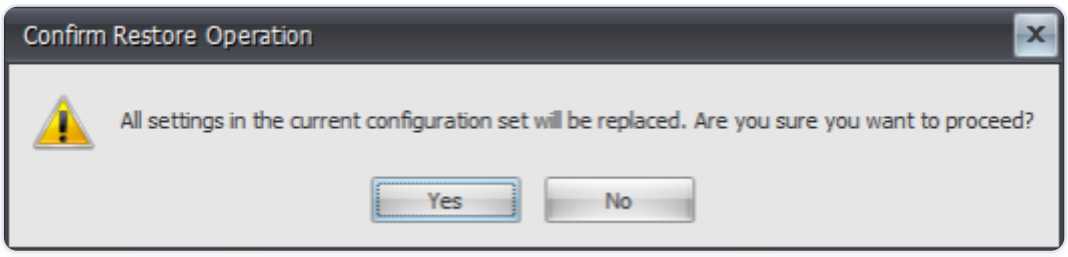


12. On the Restore settings processing page, under Restore settings, click **Restore Settings**.

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

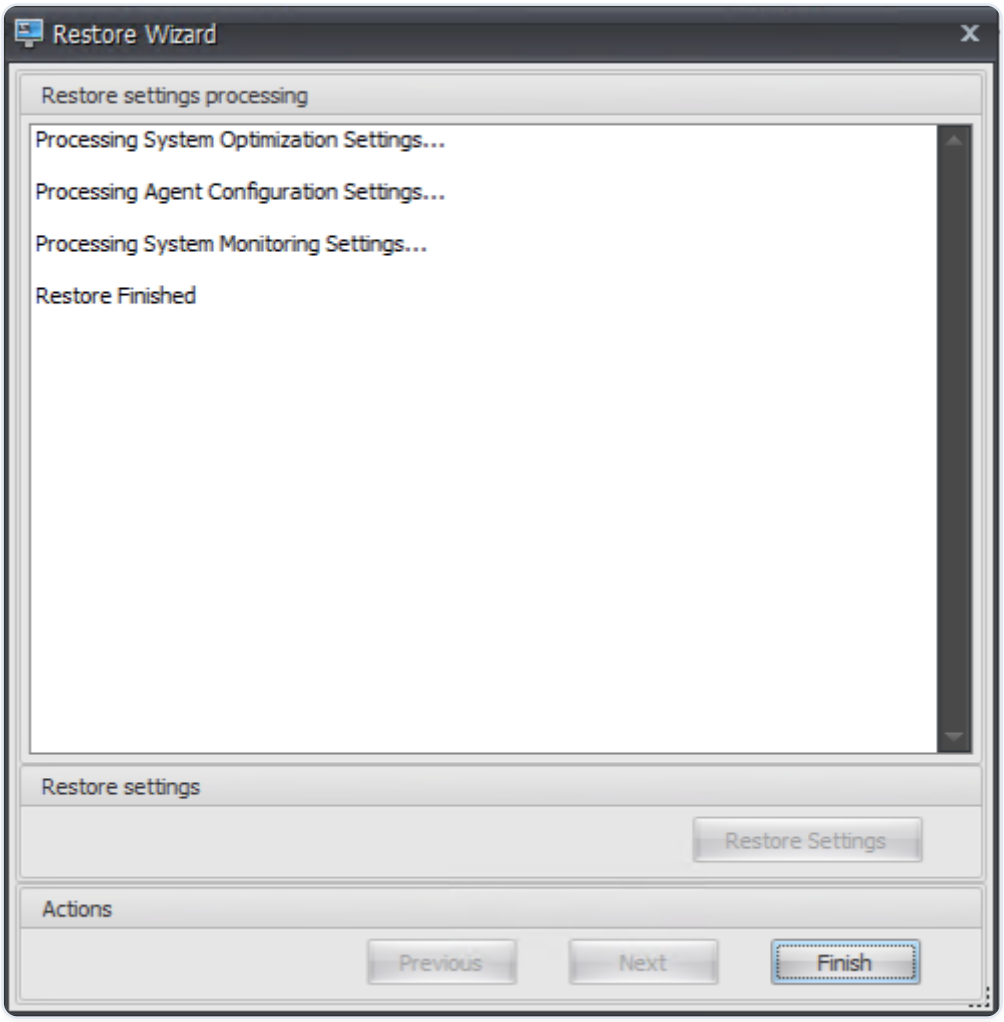


13. Click **Yes**.



14. Click **Finish**.

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



Step 6: Add the group policy template (optional)

Optionally, you can choose to configure the group policies. The **Agent Group Policies** administrative template, provided in the WEM agent package, adds the Agent Host Configuration policy.

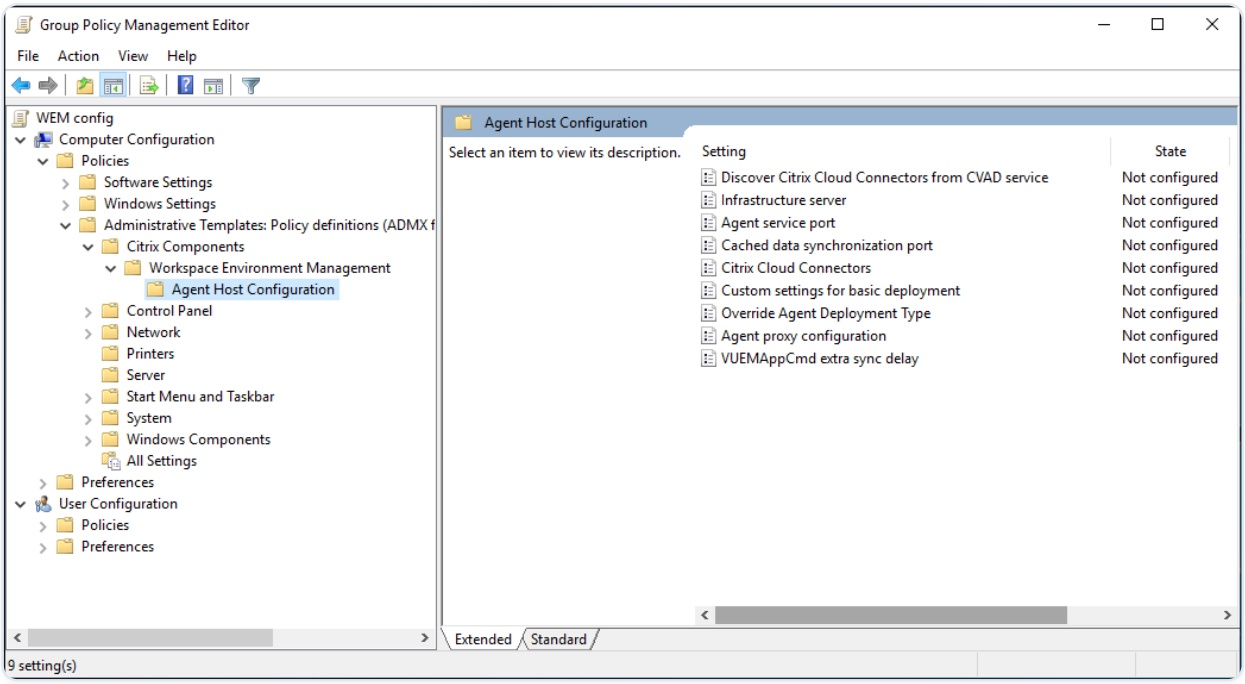
1. Copy the **Agent Group Policies** folder provided with the WEM installation package to your WEM domain controller.
2. Add the .admx files.
    a. Go to the A**gent Group Policies > ADMX** folder.
    b. Copy the two files (*Citrix Workspace Environment Management Agent Host Configuration.admx* and *CitrixBase.admx*).
    c. Go to the `<C:\Windows>\PolicyDefinitions` folder and then paste the files.
3. Add the .adml files.
    a. Go to the **Agent Group Policies > ADMX > en-US** folder.

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

b. Copy the two files (*Citrix Workspace Environment Management Agent Host Configuration.adml* and *CitrixBase.adml*).

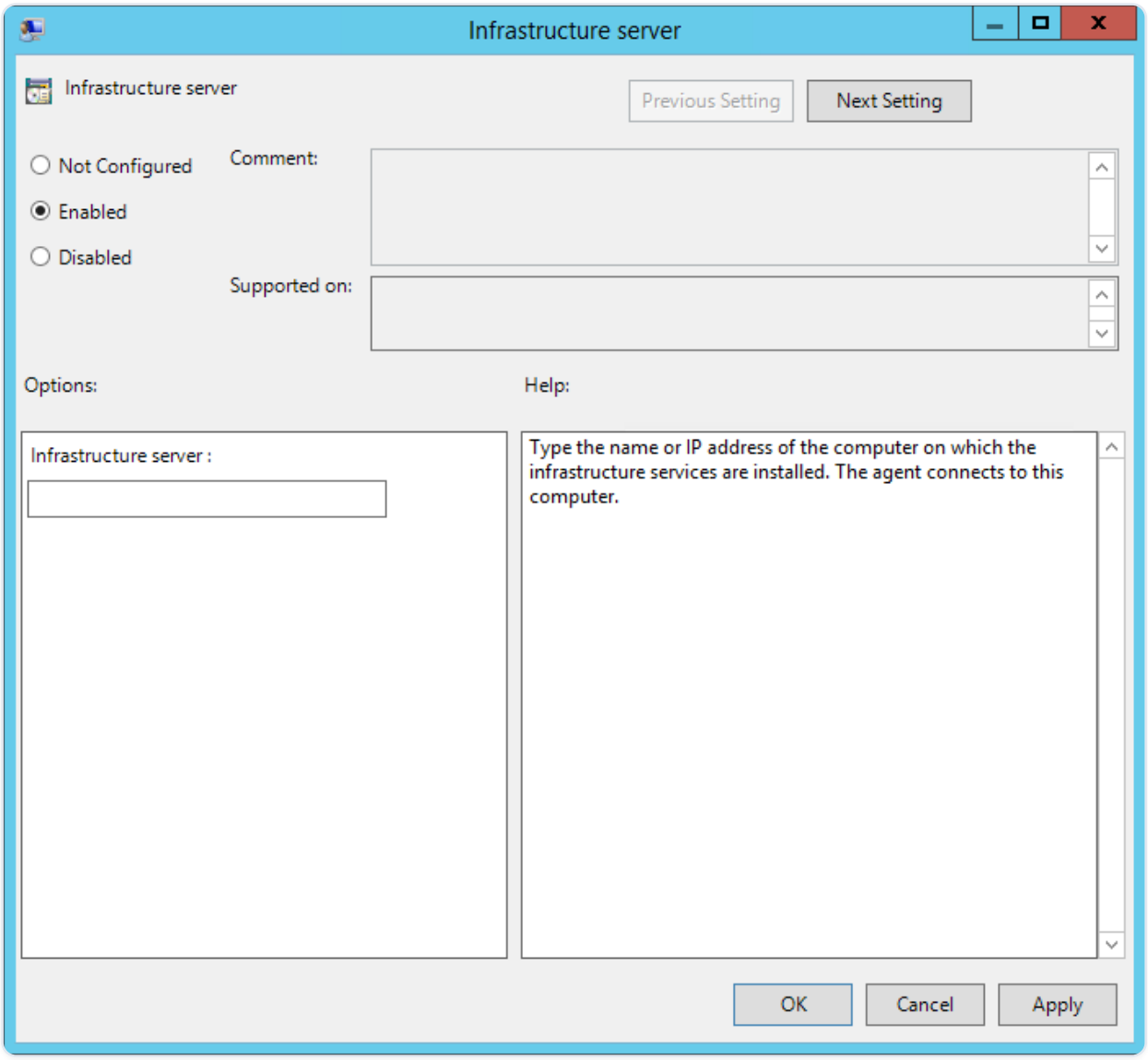
c. Go to the `<C:\Windows>\PolicyDefinitions\en-US` folder and then paste the files.

4. In the Group Policy Management Editor window, go to **Computer Configuration > Policies > Administrative Templates > Citrix Components > Workspace Environment Management > Agent Host Configuration** and double-click **Infrastructure server**.

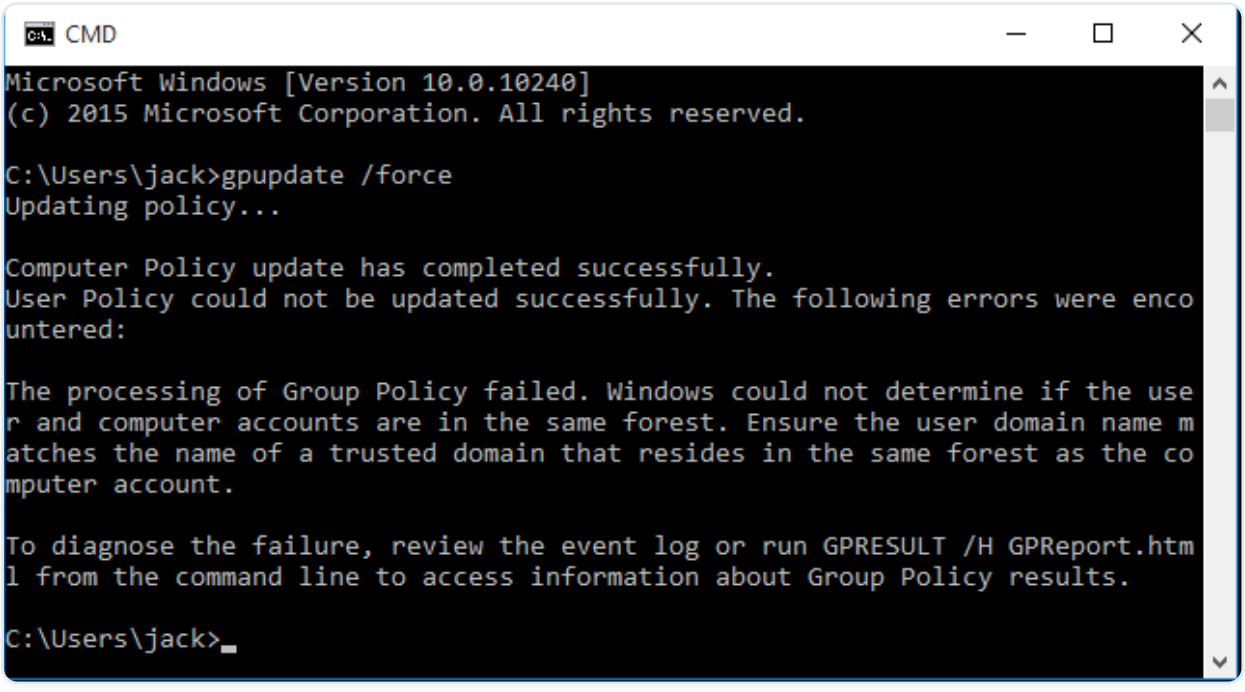


5. In the Infrastructure server window, select **Enabled**, and under Options, type the IP address of the computer on which the infrastructure services are installed, and then click **Apply** and **OK**.

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



6. Go to the agent host, open a command line, and type `gpupdate /force`.



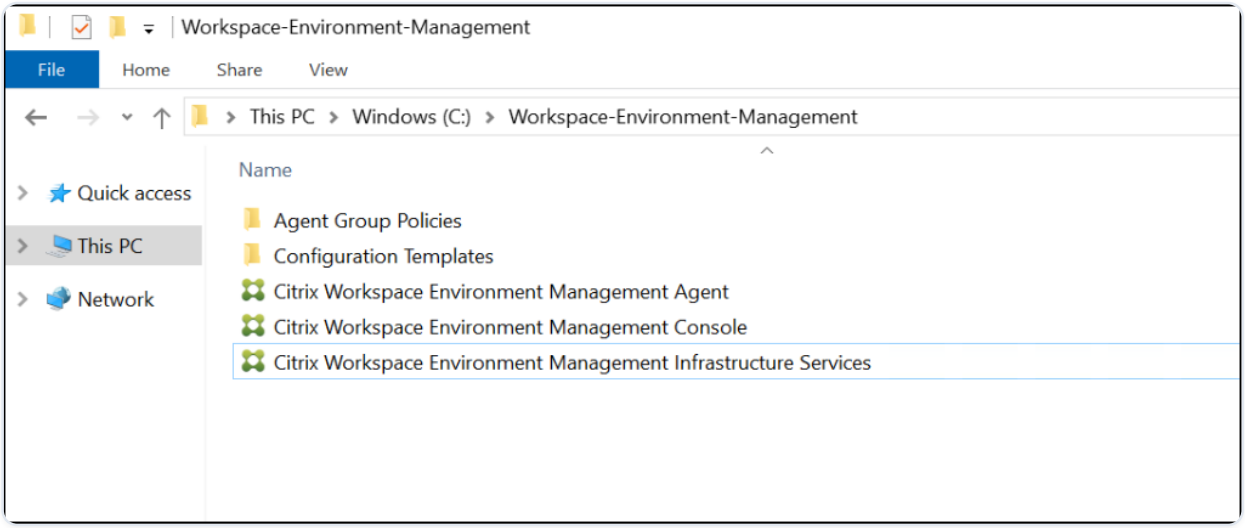
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 7: Install the agent

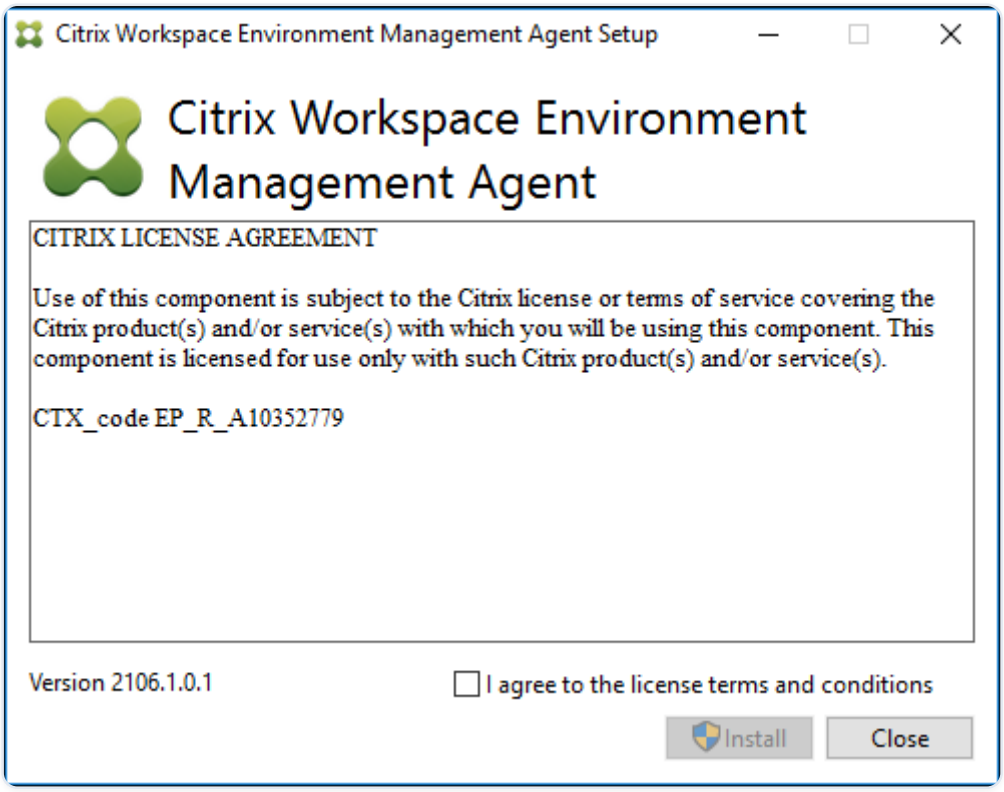
IMPORTANT:

Do not install the WEM agent on the infrastructure server.

1. Run **Citrix Workspace Environment Management Agent.exe** on your machine.

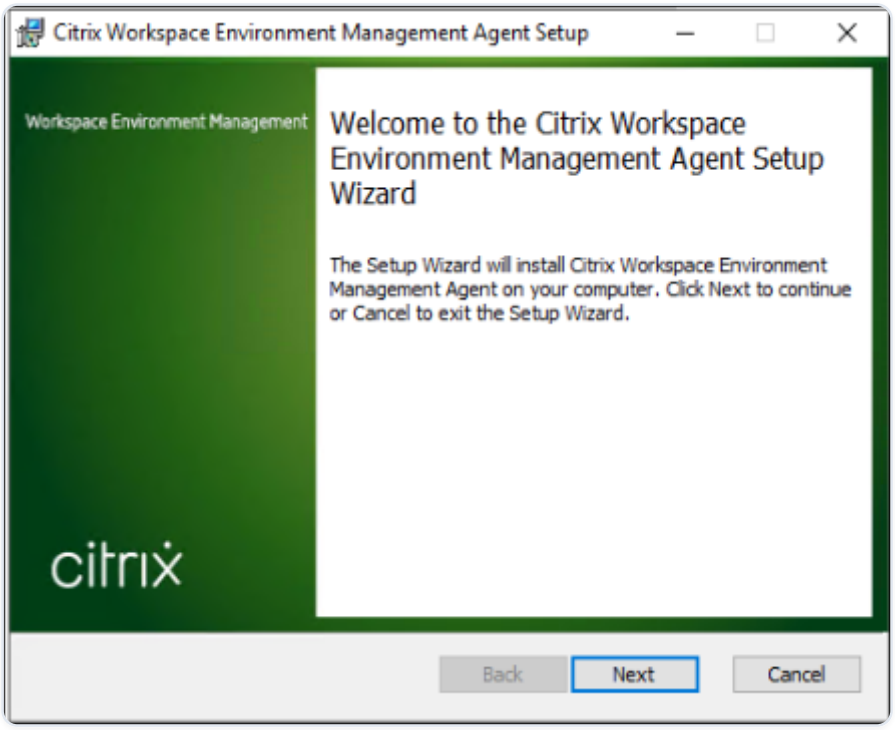


2. Select **I agree to the license terms and conditions** and then click **Install**.

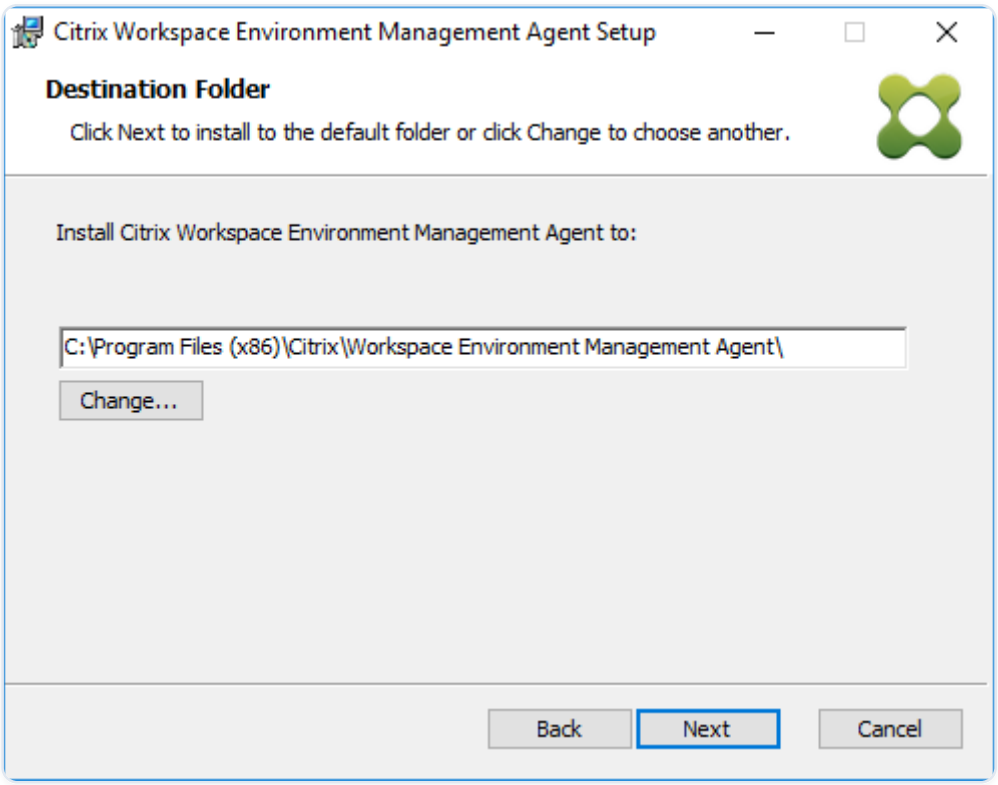


3. On the Welcome page, click **Next**.

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

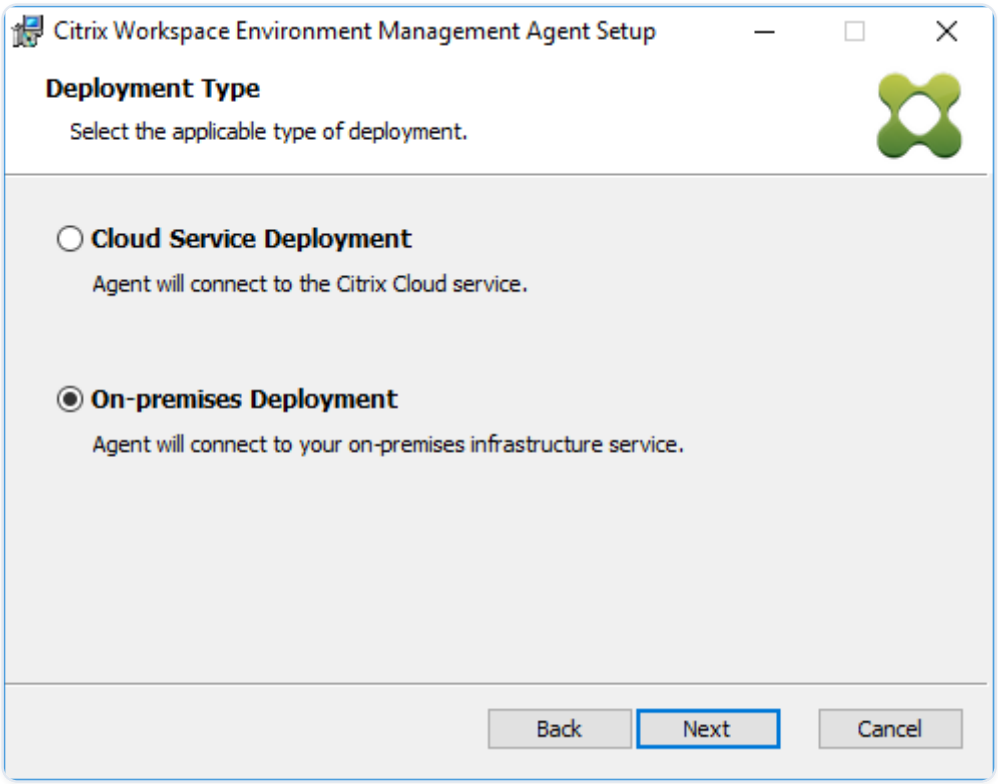


4. On the Destination Folder page, click **Next**.



5. On the Deployment Type page, select the applicable type of deployment and then click **Next**. In this case, select **On-premises Deployment**.

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

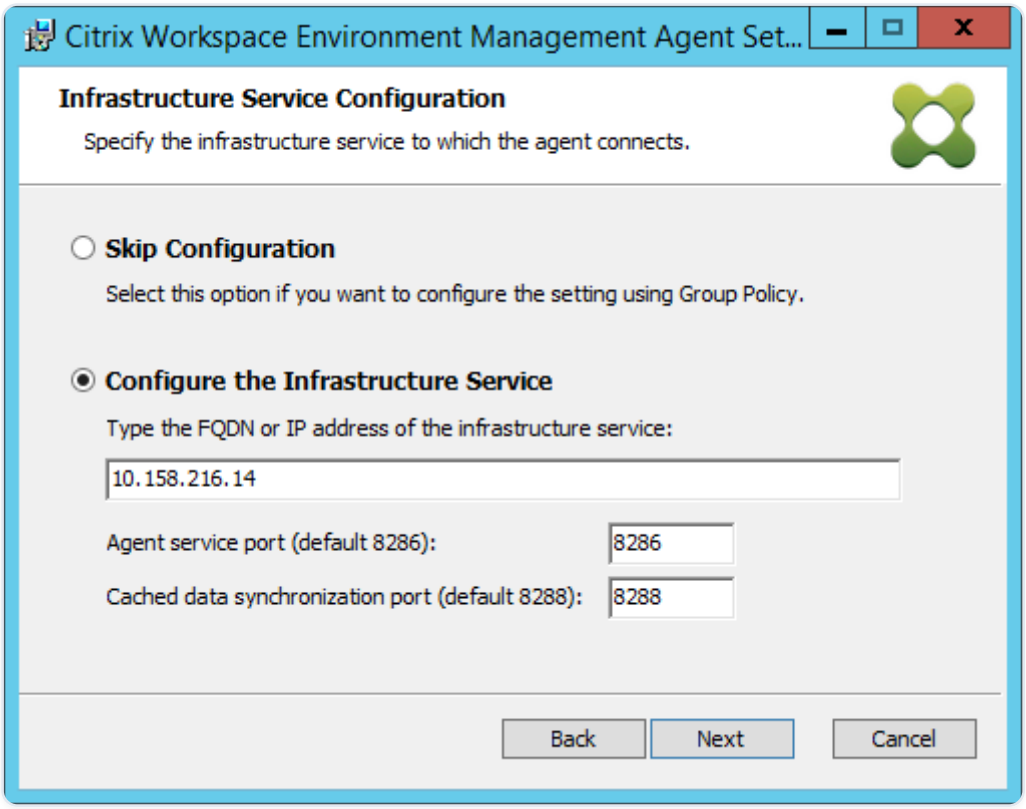


6. On the Infrastructure Service Configuration page, select **Configure the Infrastructure Service**, type the FQDN or IP address of the infrastructure service, and then click **Next**.

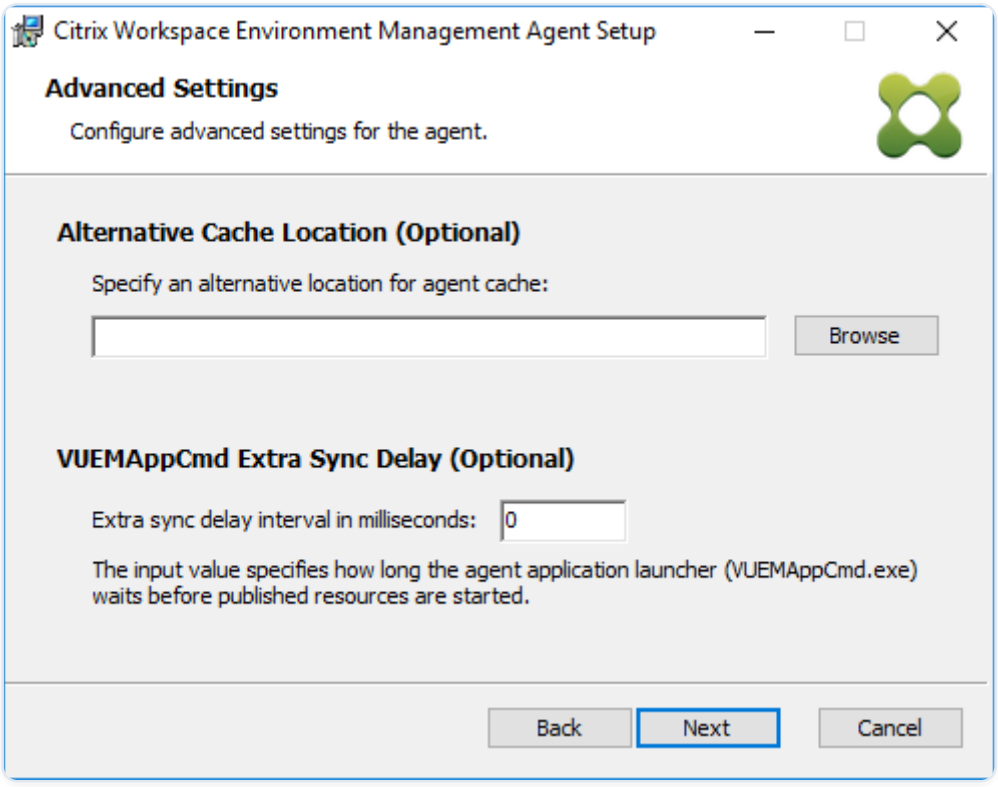
NOTE:

For the agent service port, the default port is 8286. For the cached data synchronization port, the default port is 8288. For more information, see Port information.

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



7. On the Advanced Settings page, click **Next**.

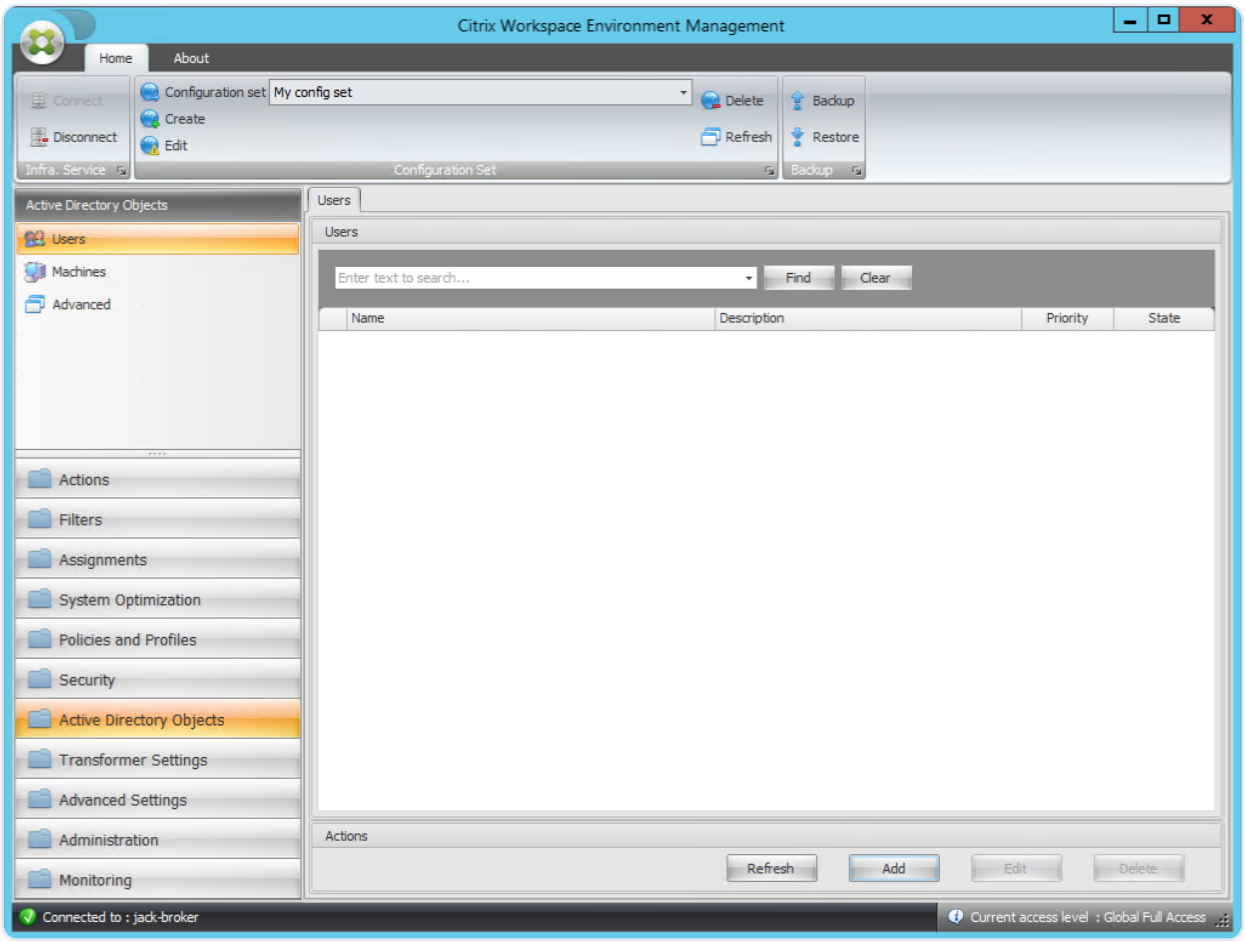


8. On the Ready to install page, click **Install**.
9. Click **Finish** to exit the installation wizard.

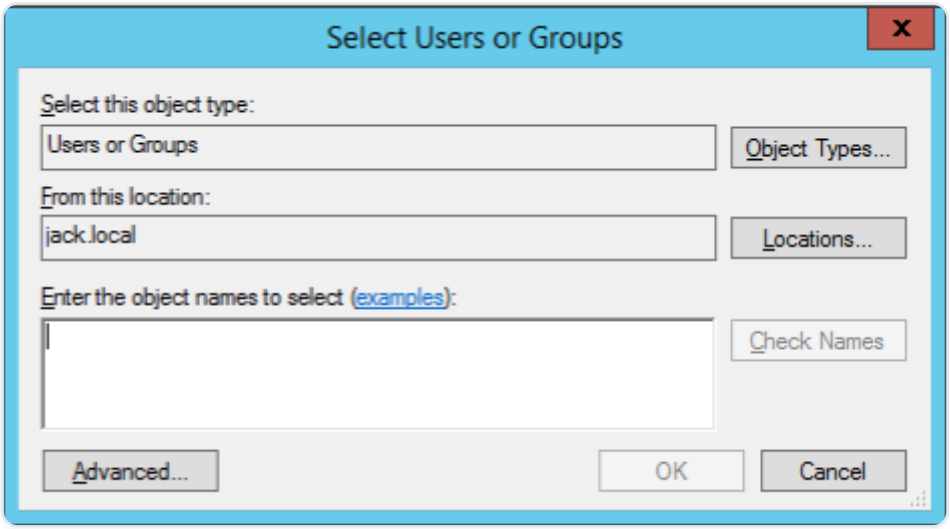
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 8: Add the agent to the configuration set you created

1. From the **Start** menu, open the **WEM Administration Console**, click **Active Directory Objects**, and then click **Add**.

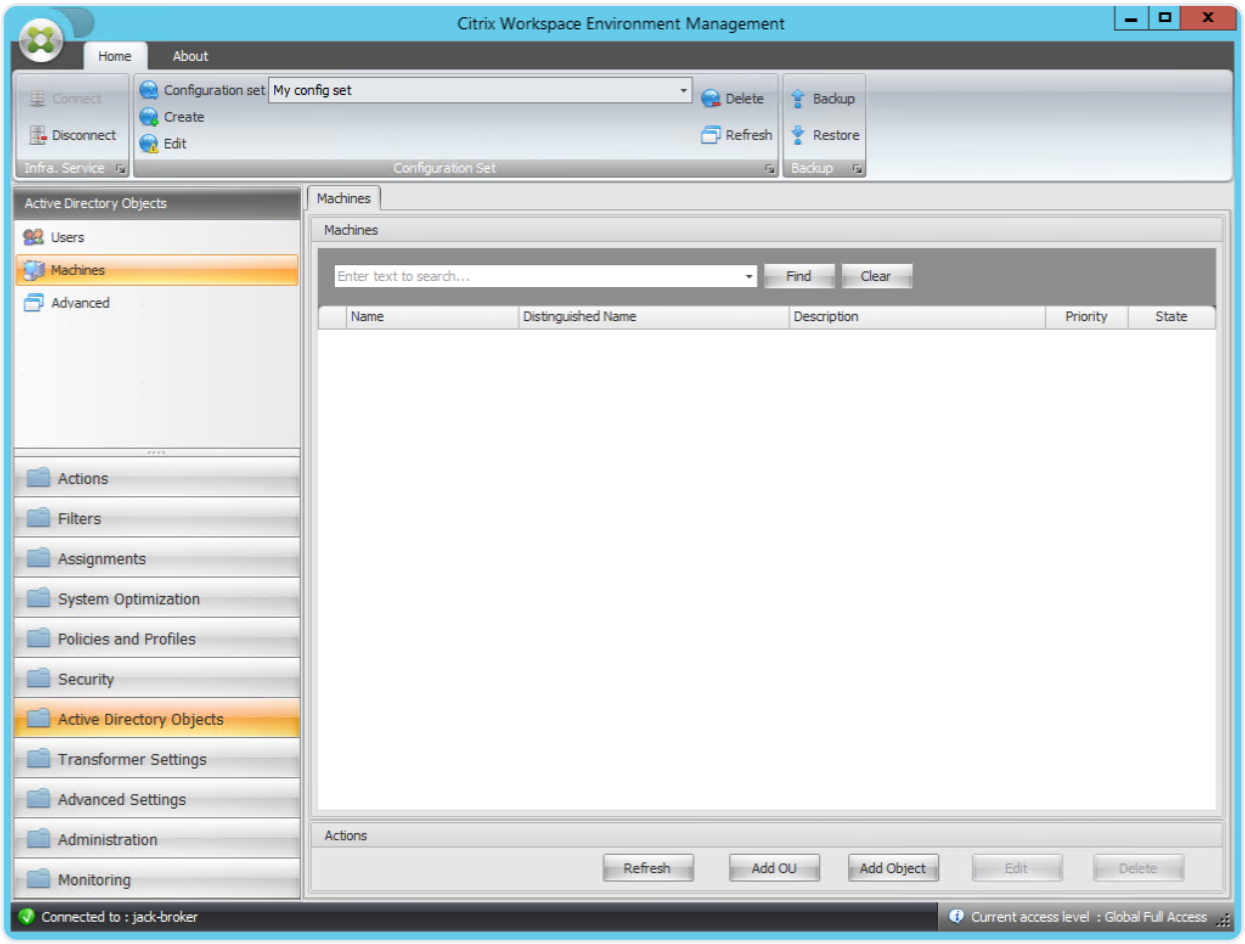


2. In the Select Users or Groups window, type the name, click **Check Names**, and then click **OK**.



3. Click **Machines**.

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



4. On the **Machines** tab, click **Add OU** or **Add Object** to add the machines that you want to manage to the configuration set you created.

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

System requirements

Software prerequisites

.NET Framework 4.8 or later. This component is required for the Workspace Environment Management Infrastructure services, Administration console, Agent, and Web console. If it is not already installed, it is automatically installed during the setup. However, we recommend installing this prerequisite manually before proceeding with the installation. Otherwise, you might have to restart your machine to continue with the installation, which can take a significant amount of time.

Microsoft Visual C++. This component is necessary for the Workspace Environment Management™ agent. If not already installed, the Microsoft Visual C++ 2015–2019 Redistributable is automatically installed during agent installation.

Microsoft Edge WebView2 Runtime version 98 or later. This component is necessary for the Workspace Environment Management service agent. If not already installed, it is automatically installed during agent installation.

NOTE:

- Only version 2209 and later require this component.
- To download and install the Microsoft Edge WebView2 Runtime, you must have internet access.

Microsoft SQL Server 2016 SP2 or later. Workspace Environment Management requires **sysadmin** access to a SQL Server instance to create its database, and **read/write** access to the database to use it. During the database creation, Workspace Environment Management creates a SQL login and then adds a database user mapping to the login. The user is *automatically* granted read/write access to the database. The SQL Server instance must use case-insensitive collation. Otherwise, database creation or upgrade fails.

NOTE:

During an upgrade, we recommend using a user account that has the **sysadmin** server role.

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

Microsoft Active Directory. Workspace Environment Management requires **read access** to your Active Directory to push configured settings out to users.

NOTE:

- WEM's global catalog does not support *External trust* relationships that store a copy of all Active Directory objects in a forest. Instead, you must use other relationship types, such as *forest trust* relationships.
- WEM also does not support a one-way forest trust relationship between forests.

Citrix License Server 11.14. Workspace Environment Management requires a Citrix license. Citrix licenses are managed and stored on Citrix License Servers.

Citrix Virtual Apps and Desktops. Any supported version of Citrix Virtual Apps or Citrix Virtual Desktops is required for this release of Workspace Environment Management.

Citrix Workspace™ app for Windows. To connect to Citrix StoreFront™ store resources that have been configured from the Workspace Environment Management administration console, Citrix Workspace app for Windows must be installed on the administration console machine and on the agent host machine. The following versions are supported:

- On administration console machines:
  - Citrix Receiver for Windows versions: 4.9 LTSR, 4.10, 4.10.1, 4.11, and 4.12
  - Citrix Workspace app 1808 for Windows and later
- On agent host machines:
  - Citrix Receiver for Windows versions: 4.4 LTSR CU5, 4.7, 4.9, 4.9 LTSR CU1, and 4.10
  - Citrix Workspace app 1808 for Windows and later

For Transformer kiosk-enabled machines, Citrix Workspace app for Windows must be installed with single sign-on enabled, and configured for pass-through authentication. For more information, see Citrix Workspace app documentation.

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

Operating system prerequisites

NOTE:

Workspace Environment Management and associated components are supported only on operating system versions supported by their manufacturer. You might need to purchase extended support from your operating system manufacturer.

Infrastructure services

Supported operating systems:

- Windows Server 2025 Standard and Datacenter Editions
- Windows Server 2022 Standard and Datacenter Editions
- Windows Server 2019 Standard and Datacenter Editions

NOTE:

Running Workspace Environment Management infrastructure services on a pool of servers (infrastructure servers) with different operating system versions is supported. To upgrade the operating system of an infrastructure server, first install the infrastructure service on a different machine with the new operating system, manually configure it with identical infrastructure service settings, then disconnect the 'old' infrastructure server.

Administration console

Supported operating systems:

- Windows 11, 32-bit and 64-bit
- Windows 10 version 1607 and newer, 32-bit, and 64-bit
- Windows Server 2025 Standard and Datacenter Editions
- Windows Server 2022 Standard and Datacenter Editions
- Windows Server 2019 Standard and Datacenter Editions

Web console

Supported operating systems:

- Windows Server 2025 Standard and Datacenter Editions

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

- Windows Server 2022 Standard and Datacenter Editions
- Windows Server 2019 Standard and Datacenter Editions

Agent

Supported operating systems:

- Windows 11, 32-bit and 64-bit
- Windows 10 version 1607 and later, 32-bit and 64-bit
- Windows Server 2025 Standard and Datacenter Editions*
- Windows Server 2022 Standard and Datacenter Editions*
- Windows Server 2019 Standard and Datacenter Editions*

* The Transformer feature is not supported on multi-session operating systems.

In WEM 4.4, Windows XP was supported.

NOTE:

Citrix Workspace Environment Management agents running on multi-session operating systems cannot operate correctly when Microsoft's Dynamic Fair Share Scheduling (DFSS) is enabled. For information about how to disable DFSS, see CTX127135.

SQL Server Always On

Workspace Environment Management supports Always On availability groups (Basic and Advanced) for database high availability based on Microsoft SQL Server. Citrix® has tested this using Microsoft SQL Server 2017.

Always-On availability groups allow databases to automatically fail over if the hardware or software of a principal or primary SQL Server fails, which ensures that Workspace Environment Management continues to work as expected. The Always-On availability groups feature requires that the SQL Server instances reside on the Windows Server failover Cluster (WSFC) nodes. For more information, see `<https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server?view=sql-server-ver15>`.

To use Workspace Environment Management (WEM) with Always On availability groups:

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

1. Open **WEM Database Management Utility** and then create a WEM database.

   - Make"sure that you select the **Set vuemUser SQL user account password** option and type a password for the vuemUser SQL user account. You must provide this password when you add the database to the availability group.
   - For "Server and instance name," type the name of the primary SQL Server.

   NOTE:

   The WEM database is created on the primary SQL Server.

2. Go to your primary SQL Server and then back up the WEM database that you created.

   - To select the WEM database on the **Add Database to Availability Group > Select Databases** page, you must type the password (the password you created in step 1). To do so, right-click the corresponding blank area in the Password column, type the password, and then click **Refresh**.
   - Select the **Full** recovery model for the database backup.

3. On the SQL Server, add the WEM database to the availability group and then configure the availability group listener.
4. The **vuemUser** login must be created on the secondary SQL instance in **Always On HA group**. For more details, see Transfer logins and passwords between instances - SQL Server.
5. Go to the WEM infrastructure service machine and then open the **WEM Infrastructure Service Configuration** utility.

   - **Database server and instance**. Type the name of the availability group listener.
   - **Database failover server and instance**. Leave empty.
   - **Database name**. Type the name of the database.

Hardware prerequisites

Infrastructure services: 4 vCPUs, 8 GB RAM, 80 GB of available disk space. For scale and size considerations for infrastructure services, see Scale and size considerations for deployments.

Administration console: minimum dual core processor with 2 GB RAM, 40 MB of available disk space (100 MB during install).

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

Agent: average RAM consumption is 10 MB, but we recommend that you provide 20 MB to be safe. 40 MB of available disk space (100 MB during installation).

Database: minimum 75 MB of available disk space for the Workspace Environment Management database.

Service dependencies

Netlogon. The agent service ("Norskale Agent Host service") is added to the Net Logon Dependencies list to ensure that the agent service is running before logons can be made.

Antivirus exclusions

By default, the Workspace Environment Management agent and infrastructure services install into the following folders:

- Agent
  - `C:\Program Files (x86)\Citrix\Workspace Environment Management Agent` (on 64-bit OS)
  - `C:\Program Files\Citrix\Workspace Environment Management Agent` (on 32-bit OS)
- Infrastructure services
  - `C:\Program Files (x86)\Citrix\Workspace Environment Management Infrastructure Services`

On-access scanning must be disabled for the entire "Citrix" installation folder for the agent and the infrastructure services. When the On-access scanning cannot be disabled for the "Citrix" installation folder, the following processes must be excluded:

In the infrastructure services installation folder

- WEM Infrastructure Service.exe
- WEM Infrastructure Service Configuration Utility.exe
- WEM Infrastructure Database Management Utility.exe

In the agent installation folder

- Agent Log Parser.exe

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

- AgentCacheUtility.exe
- AgentGroupPolicyUtility.exe
- AppsMgmtUtil.exe
- Citrix.Wem.Agent.Service.exe
- Citrix.Wem.Agent.LogonService.exe
- PrnsMgmtUtil.exe
- VUEMAppCmd.exe
- VUEMAppCmdDbg.exe
- VUEMAppHide.exe
- VUEMCmdAgent.exe
- VUEMMaintMsg.exe
- VUEMRSAV.exe
- VUEMUIAgent.exe

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

Install and configure

Install and configure the following components:

- Infrastructure services
- Administration console
- Web console service
- Set up licensing
- Agent

Download the installer

Follow these steps to download the WEM installer:

1. Access the Citrix Virtual Apps and Desktops download page.
2. Locate and expand the version that you want to download (for example, **Citrix Virtual Apps and Desktops 7 2511**).
3. Expand the **Components** node. Then click **Workspace Environment Management <Version_number>**.
4. Scroll down to the bottom and click **Download File**.
5. In the **End-User License Agreement** dialog box, accept the agreement and select the download folder to start the download.

   After the download completes, the `Workspace-Environment-Management-_<version_number>.zip` file appears in the specified folder.

NOTE:

You can also find the WEM installer on the Citrix Virtual Apps and Desktops image in the `\x64\Workspace Environment Management` directory.

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

Infrastructure services

There is one Windows infrastructure service: **Citrix WEM Infrastructure Service(NT SERVICE\\Citrix WEM Infrastructure Service)**. It manages Workspace Environment Management (WEM) infrastructure services.

Account requirements: Use `NetworkServicem` or a specified user account that is a member of the Administrator group on the infrastructure server where the service runs.

Install the infrastructure services

IMPORTANT:

- The WEM infrastructure services cannot be installed on a domain controller. Kerberos authentication issues prevent the infrastructure services from working in this scenario.
- Do not install the infrastructure services on a server where the Delivery Controller™ is installed.

Usage data collection notice:

- By default, the infrastructure services collect anonymous analytics on WEM usage each night and sends it immediately to the Google Analytics server through HTTPS. Analytics collection complies with the Citrix Privacy Policy.
- Data collection is enabled by default when you install or upgrade the infrastructure services. To opt out, in the WEM Infrastructure Service Configuration dialog **Advanced Settings** tab, select the **Do not help improve Workspace Environment Management™ using Google Analytics** option.

To Install the infrastructure services, run **Citrix Workspace Environment Management Infrastructure Services.exe** on your infrastructure server. The PowerShell SDK module is installed by default. By default, the infrastructure service is installed into the following folder: `C:\Program Files (x86)\Citrix\Workspace Environment Management Infrastructure Services`. For SDK documentation, see Citrix Developer Documentation.

You can choose a silent installation or upgrade of the infrastructure services. For example:

- .\Citrix Workspace Environment Management Infrastructure Services.exe `/quiet BrokerLocation="C:\test\Infrastructure Services" /log "C:\test\test.log"`

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

- `/quiet BrokerLocation="C:\test\Infrastructure Services" /log "C:\test\test.log"`
  - `/quiet`. Indicates silent mode.
  - `/log`. Indicates logging file location.
  - `BrokerLocation`. Indicates the installation path for infrastructure services.

Create a service principal name

IMPORTANT:

- When you use **load balancing**, all instances of the infrastructure services must be installed and configured using the same service account name.
- **Windows authentication** is a specific method of authentication for SQL instances that use AD. The other option is to use a SQL account instead.

After the installer finishes, create an SPN for the infrastructure service. In WEM, connection and communication between agent, infrastructure service, and domain controller are authenticated by Kerberos. SPNs are used by Kerberos authentication to associate a service instance with a service logon account. The relationship must be configured between the logon account of the infrastructure service instance and the account registered with the SPN. Therefore, to comply with the Kerberos authentication requirements, configure the WEM SPN to associate it with a known AD account by using the command that is suited to your environment:

- If you do not use Windows authentication or load balancing, use the following command:
  - `setspn -C -S [SPN name] [hostname]`

  where `hostname` is the name of the infrastructure server.
- If you use Windows authentication or load balancing (requiring Windows authentication), use the following command:
  - `setspn -U -S [SPN name] [accountname]`

  where `accountname` is the name of the service account that is being used for Windows authentication.

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

- The default value for `[SPN name]` is `Norskale/BrokerService`. If multiple WEM deployments are in the same forest, you may need to configure several SPNs by adding the following registry values:
  - `setspn -C -S [SPN name] [hostname]` or `setspns -U -S [SPN name] [accountname]`
  - For Agent Machine: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Agent Host
  - For infrastructure and console machine: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Infrastructure Services
  - Name: AlternativeSPN
  - Type: REG_SZ
  - Value: the actual value for the

SPNs are case sensitive.

Group Managed Service Account

You can implement a group Managed Service Account (gMSA) solution for WEM. With a gMSA solution, services can be configured for the new gMSA principal and the password management is handled by Windows. For information, see `<https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview>`. When a gMSA is used as a service principle, the Windows operating system manages the password for the account instead of relying on administrators to manage it. Doing so eliminates the need to change Windows account impersonation settings you configured for the infrastructure service if you change the password for the account later.

To implement a gMSA solution for WEM, follow these steps:

1. If you already have an existing gMSA, do the following:
   a. Bind the Citrix WEM SPN with the account using the following command:
      - `setspn -C -S Norskale/BrokerService [gMSA]$`

      where `gMSA` is the name of the gMSA account.
   b. Add the relevant machines to the account using the following command:

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

- `Set-ADServiceAccount -Identity [gMSA] -PrincipalsAllowedToRetrieveManagedPassword [hostname]`

where the is the name of the infrastructure server.

2. If you do not have a gMSA, go to your domain controller, create one, and then bind the Citrix WEM SPN with it. Use the following command:

   - `New-ADServiceAccount [gMSA] -DNSHostName [hostname 1] -PrincipalsAllowedToRetrieveManagedPassword [hostname 2], [hostname 3] -KerberosEncryptionType RC4, AES128, AES256 -ServicePrincipalNames Norskale/BrokerService`

   where is the name of the DNS server.

   where , are the names of the infrastructure server.

   For more information about creating a gMSA, see `<https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts>`.

3. Configure a gMSA manually.

   a. Enable the account to access the database.

      i. On your primary SQL Server, navigate to **Security > Logins**, right-click **Logins**, and then select **New Login**.

      ii. In the **Login - New window**, click **Search**.

      iii. In the **Select User or Group** window, configure the settings as follows and click **OK** to exit the window.

         - **Object Types**. Select only **Service Accounts**.
         - **Locations**. Select **Managed Service Accounts**.
         - Object name. Type the account name that you created in Step 1.

      iv. On the **User Mapping** page, select the database to which you want to apply gMSA and then select **db-owner** as the role membership for the database.

      v. On the **Status** page, verify that the **Grant** and **Enabled** options are selected.

      vi. Click **OK** to exit the **Login - New** window.

   b. Use the service account that you added to start the Citrix WEM Infrastructure Service.

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

i. On your infrastructure server, open the Windows Services manager, right-click the Citrix WEM Infrastructure Service, and then select **Properties**.

ii. On the **Log On** page, select **This account**, click **Browse**, and configure settings as described in the third substep of Step 3.

iii. Click **OK** to exit the **Citrix WEM Infrastructure Service Properties** window.

iv. In the Windows Services manager, restart the Citrix WEM Infrastructure Service.

NOTE:

Alternatively, you can configure the account using the WEM GUI. See Create a WEM database and Configure the infrastructure service.

Configure load balancing

TIP:

The Load balancing with Citrix ADC article provides details of how to configure a Citrix ADC appliance to load balance incoming requests from the WEM administration console and the WEM agent.

To configure WEM with a load balancing service:

1. Create a Windows infrastructure service account for the WEM infrastructure service to connect to the WEM database.
2. When you create the WEM database, select the **Use Windows authentication for infrastructure service database connection** option and specify the infrastructure service account name. For more information, see Create a Workspace Environment Management database.
3. Configure each infrastructure service to connect to the SQL database using Windows authentication instead of SQL authentication: select the **Enable Windows account impersonation** option and provide the infrastructure service account credentials. For more information, see Configure the Infrastructure Service.
4. Configure the SPNs for the WEM infrastructure services to use the infrastructure service account name. For more information, see Create a service principal name.

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

IMPORTANT:

Decide whether to use a service account or machine account before deploying a WEM environment. After a WEM environment is already deployed, you cannot switch back. For example, if you want to load balance incoming requests after you already use the machine account, you must use the machine account instead of the service account.

5. Create a virtual IP address (VIP) that covers the number of infrastructure servers you want to put behind a VIP. All the infrastructure servers covered by a VIP are eligible when agents connect to the VIP.
6. When you configure the Agent Host Configuration GPO, set the infrastructure server setting to the VIP instead of the address for any individual infrastructure server. For more information, see Install and configure the agent.
7. Session persistence is required for the connection between administration consoles and the infrastructure service. (Session persistence between the agent and the infrastructure service is not required.) We recommend that you directly connect each administration console to an infrastructure service server rather than using the VIP.

Create a Workspace Environment Management database

TIP:

You can also create the database using the WEM PowerShell SDK module. For SDK documentation, see Citrix Developer Documentation.

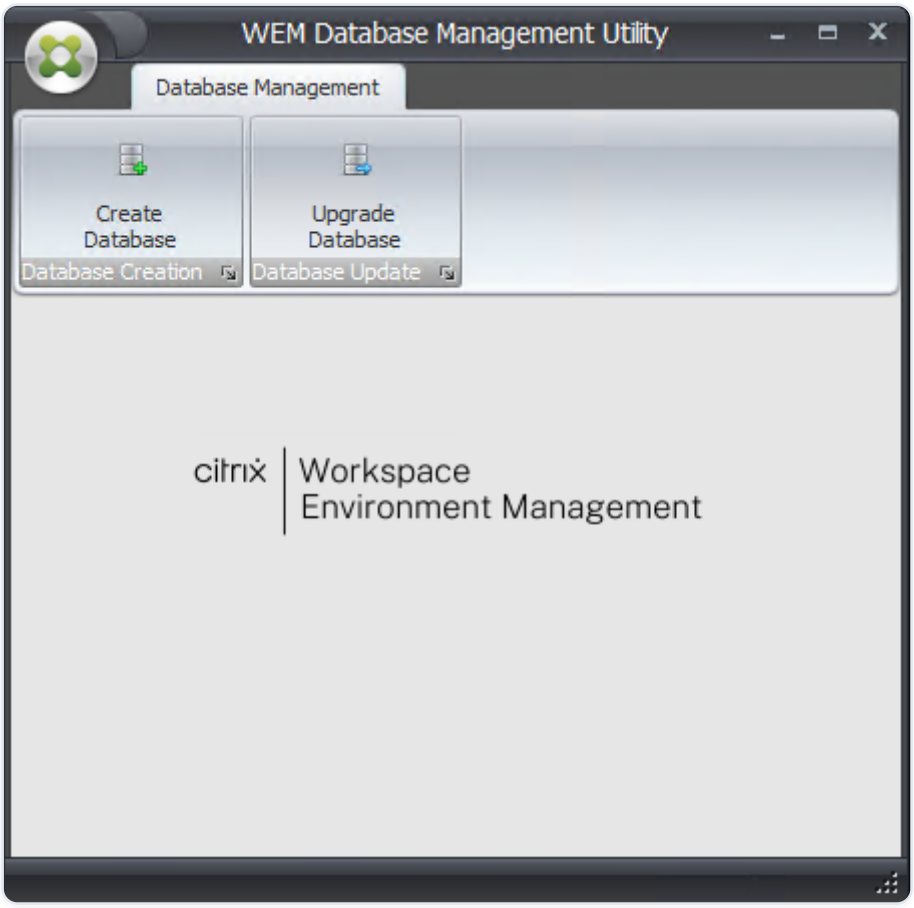
Note:

- If you are using Windows authentication for your SQL Server, run the database creation utility under an identity that has sysadmin permissions.
- Citrix recommends that you configure the primary file (.mdf file) of the WEM database with a default size of 50 MB.

Use the **WEM Database Management Utility** to create the database. This is installed during the infrastructure services installation process, and it starts immediately afterwards.

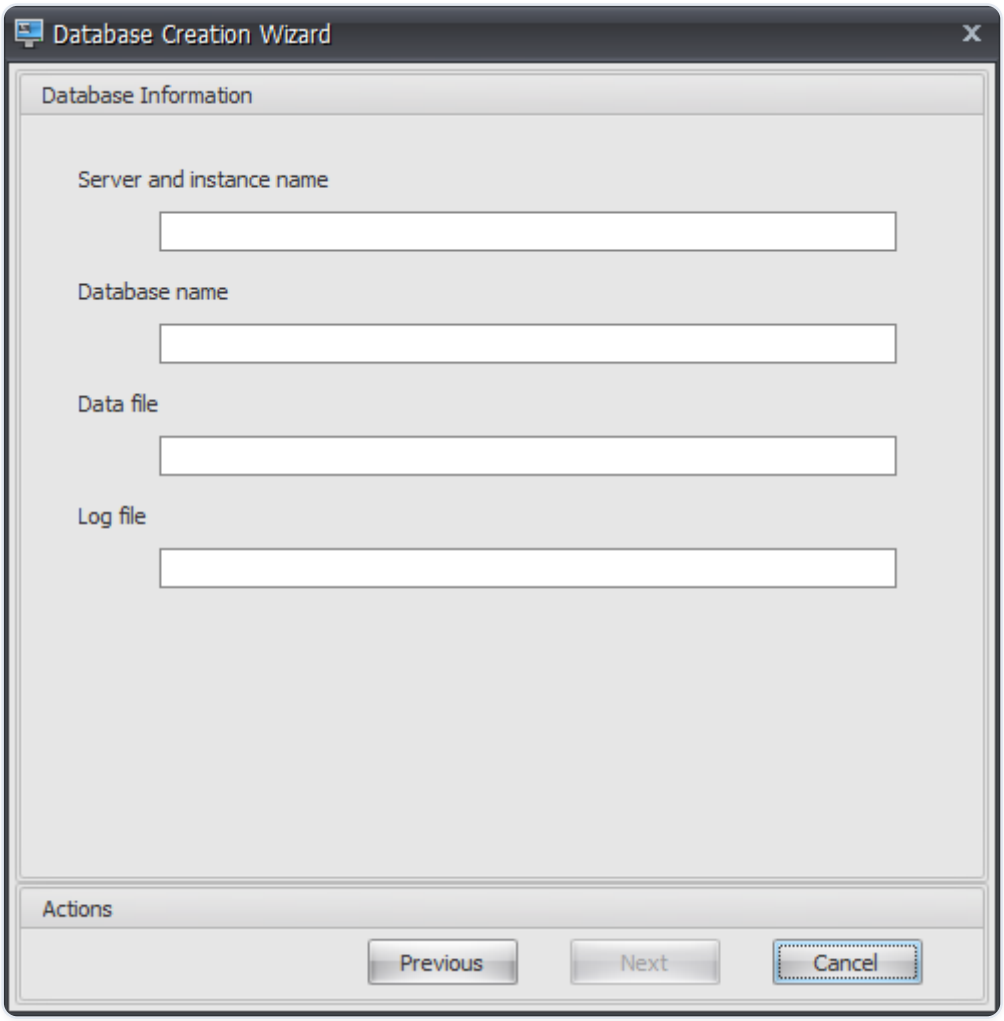
1. If the Database Management Utility is not already open, from the **Start** menu select **Citrix>Workspace Environment Management>WEM Database Management Utility**.

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



2. Click **Create Database**, then click **Next**.

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



3. Type the following Database Information, then click **Next**:

   - **Server and instance name**. Address of the SQL Server on which the database will be hosted. This address must be reachable exactly as typed from the infrastructure server. Type the server and instance name as the machine name, fully qualified domain name, or IP address. Specify a full instance address as **serveraddress,port\\instancename**. If the port is unspecified the default SQL port number (1433) is used.
   - **Database name**. Name of the SQL database to create.

   NOTE:

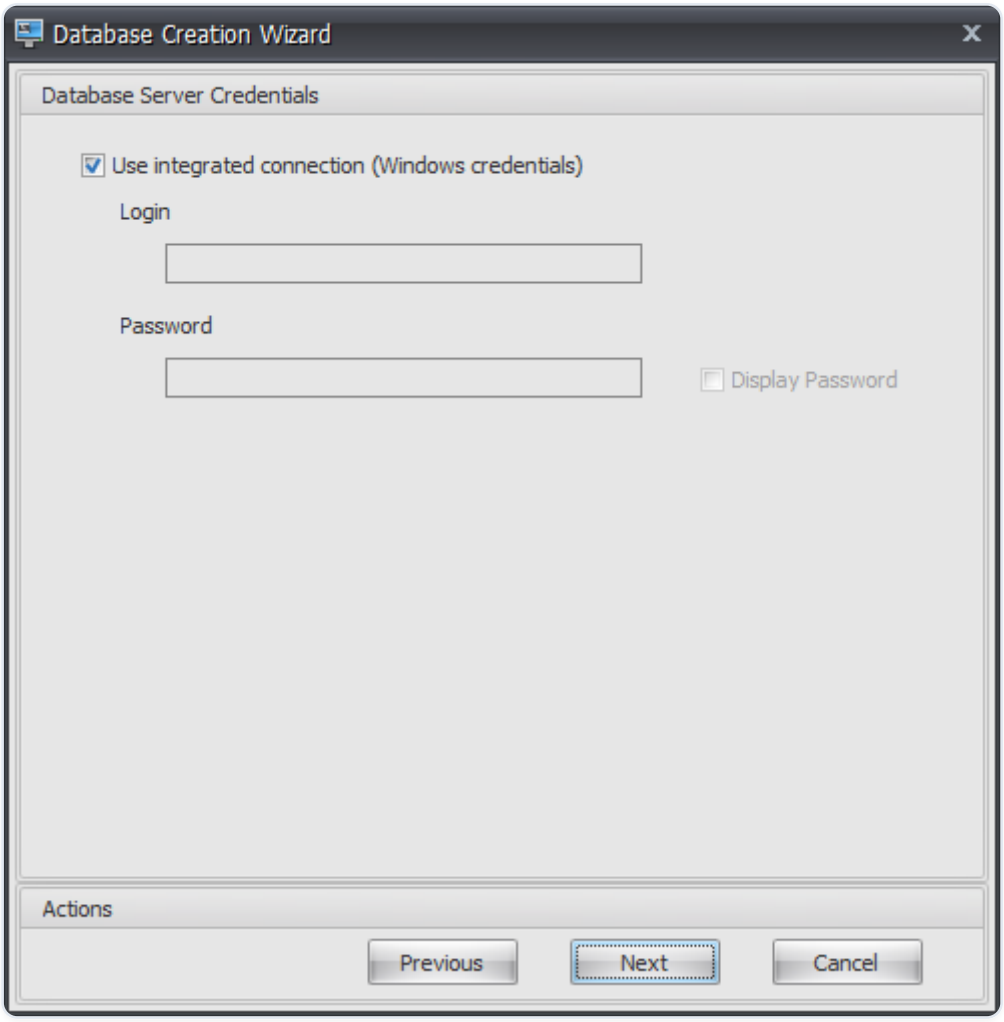
   Special characters such as hyphens (-) and dashes (/) are not allowed in the database name.

   - **Data file**: path to the **.mdf** file location on the SQL Server.
   - **Log file**: path to the **.ldf** file location on the SQL Server.

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

NOTE:

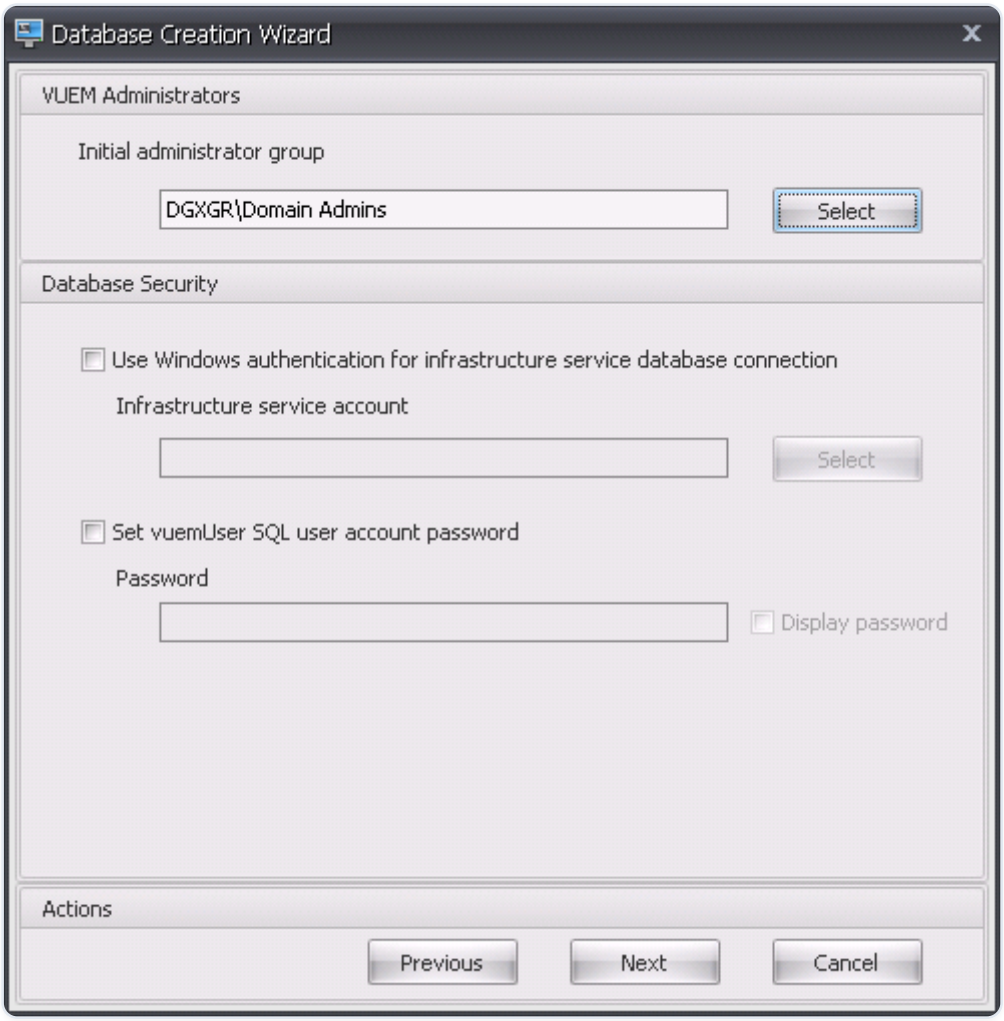
The database management utility cannot query your SQL Server for the default location of the data and log files. They default to the default values for a default installation of MS SQL Server. Make sure that the values in these two fields are correct for your MS SQL Server installation or the database creation process will fail.



4. Provide Database Server Credentials which the wizard can use to create the database, then click **Next**. These credentials are independent from the credentials that the infrastructure service uses to connect to the database after it is created. They are not stored.

   The option **Use integrated connection** is selected by default. It allows the wizard to use the Windows account of the identity it is running under to connect to SQL and create the database. If this Windows account does not have sufficient permissions to create the database, you can either run the database management utility as a Windows account with sufficient privileges, or you can clear this option and provide an SQL account with sufficient privileges instead.

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



5. Enter VUEM Administrators and Database Security details, and then click **Next**. The credentials you provide here are used by the infrastructure service to connect to the database after it is created. They are stored in the database.

   - **Initial administrator group**. This user group is pre-configured as Full Access administrators for the Administration Console. Only users configured as Workspace Environment Management administrators are allowed to use the administration console. Specify a valid user group or you will not be able to use the administration console yourself.

NOTE:

By default, *LDAP* is used when browsing the account. To enforce secure communication over *LDAPS*, add the following registry entry:

- Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\WEM`
- Name: `EnableLDAPS`
- Type: `REG_SZ`

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

- Value: `1`

- **Use Windows authentication for infrastructure service database connection**. When this option is cleared (the default) the database expects the infrastructure service to connect to it using the *vuemUser* SQL user account. The vuemUser SQL user account is created by the installation process. This requires Mixed-Mode Authentication to be enabled for the SQL instance.

When this option is selected, the database expects the infrastructure service to connect to it using a Windows account. In this case the Windows account you select must not already have a login on the SQL instance. In other words, you cannot use the same Windows account to run the infrastructure service as you used to create the database.

To select a gMSA, follow the same steps as selecting an AD user.

- **Set vuemUser SQL user account password**. By default, the vuemUser SQL account is created with an 8-character password which uses upper and lower case letters, digits, and punctuation. Select this option if you want to enter your own vuemUser SQL account password (for example, if your SQL policy requires a more complex password).

IMPORTANT:

- You must set the vuemUser SQL user account password if you intend to deploy the Workspace Environment Management database in an SQL Server Always On availability group.
- If you set the password here, remember to specify the same password when you configure the infrastructure service.

6. In the summary pane, review the settings you have selected, and when you are satisfied click **Create Database**.
7. When you are notified that the database creation has completed successfully, click **Finish** to exit the wizard.

   If an error occurs during the database creation, check the log file "Citrix WEM Database Management Utility Debug Log.log" in the **Logs** folder under the infrastructure services installation directory.

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

Configure the infrastructure service

TIP:

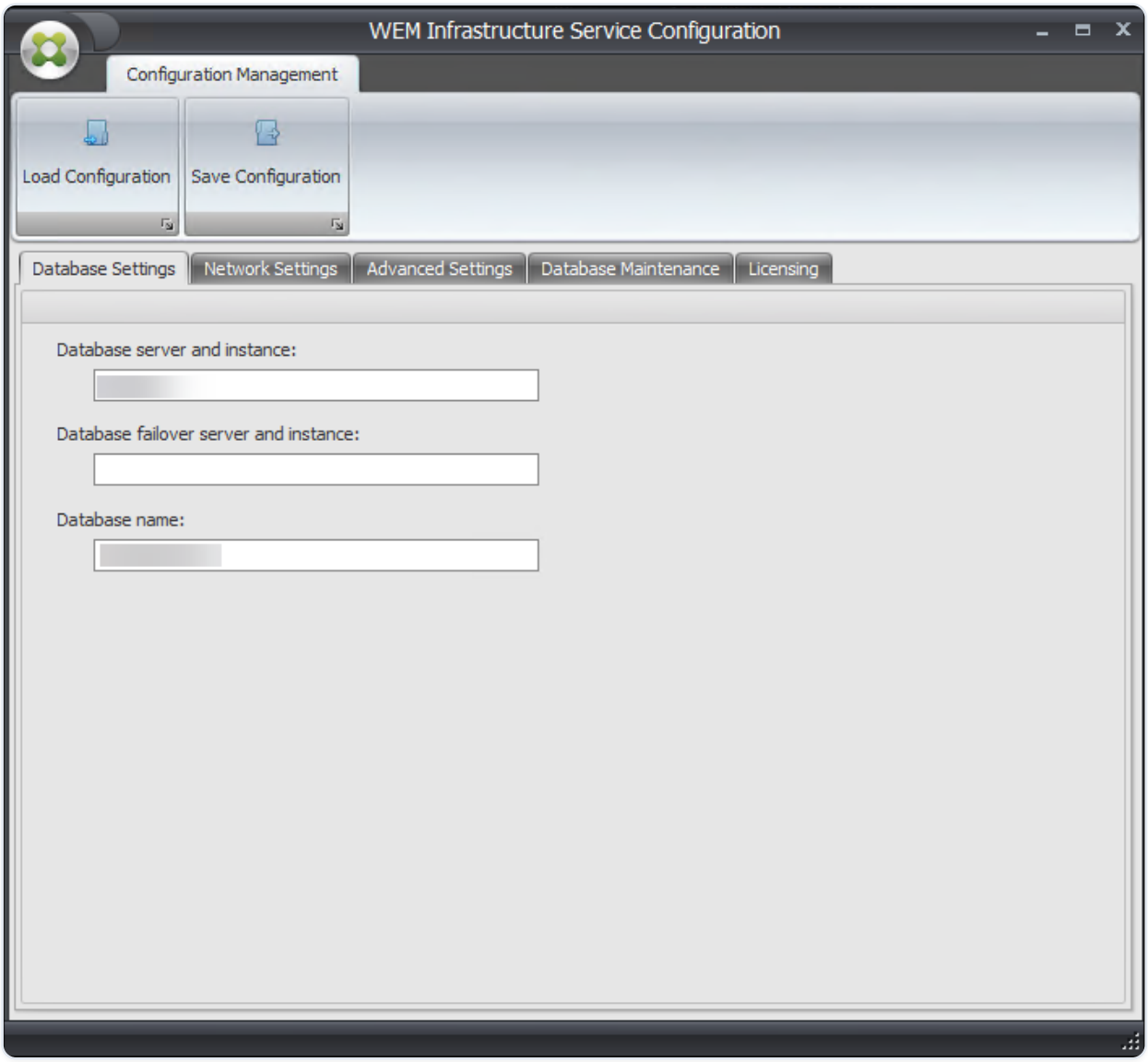
You can also configure the infrastructure service using the Workspace Environment Management PowerShell SDK module. For SDK documentation, see Citrix Developer Documentation.

Before the infrastructure service runs, you must configure it using the **WEM Infrastructure Service Configuration** utility, as described here.

1. From the **Start** menu select **Citrix > Workspace Environment Management > WEM Infrastructure Service Configuration Utility**.
2. In the **Database Settings** tab enter the following details:

    - **Database server and instance**. Address of the SQL Server instance on which the Workspace Environment Management database is hosted. This must be reachable exactly as typed from the infrastructure server. Specify a full instance address as "serveraddress, port\\instancename". If the port is unspecified the default SQL port number (1433) is used.
    - **Database failover server and instance**. If you are using database mirroring, specify the failover server address here.
    - **Database name**. Name of the Workspace Environment Management database on the SQL instance.

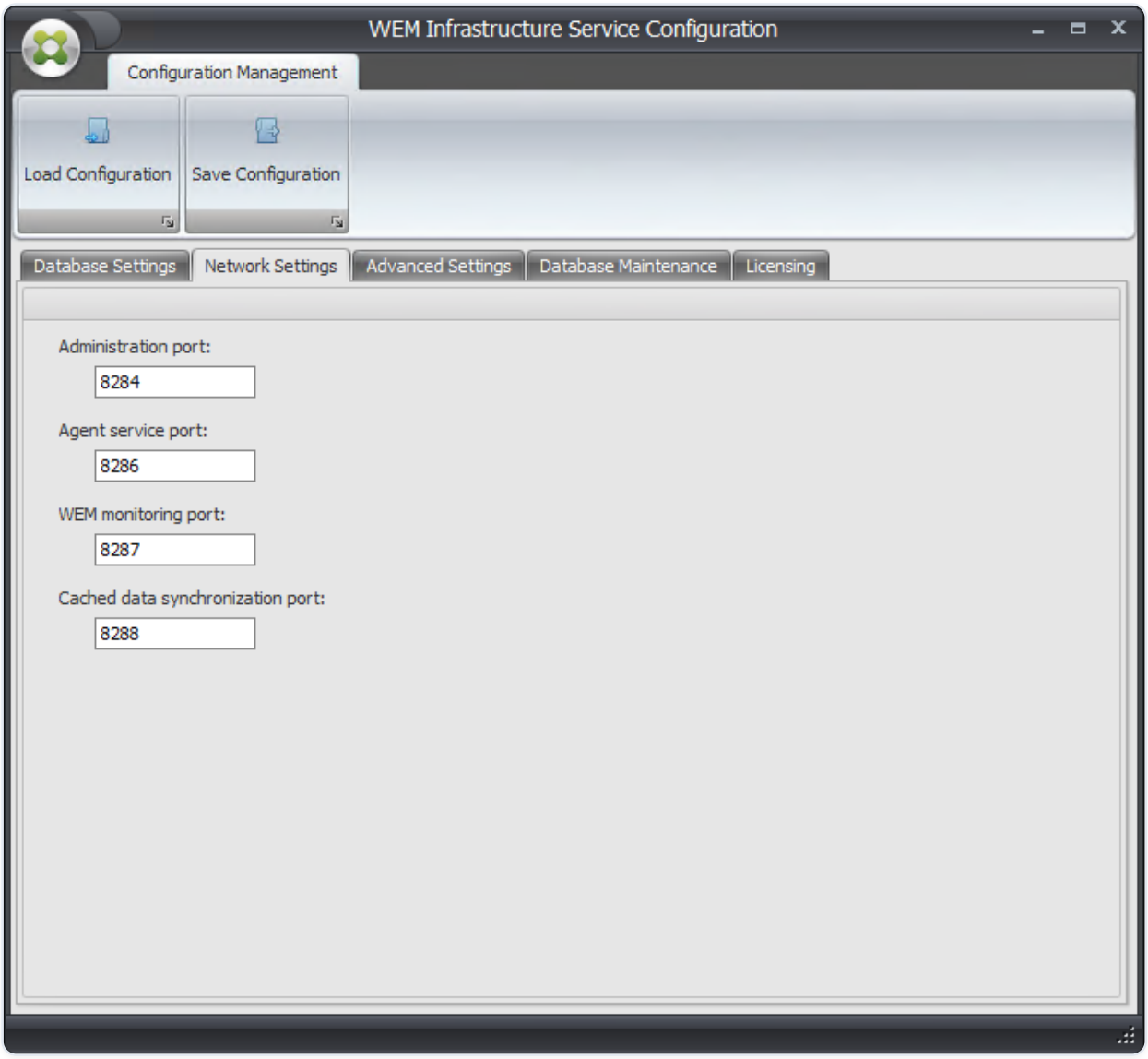
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. In the **Network Settings** tab type the ports the infrastructure service uses:

   - **Administration port**. This port is used by the administration console to connect to the infrastructure service.
   - **Agent service port**. This port is used by your agent hosts to connect to the infrastructure service.
   - **Cache synchronization port**. This port is used by the agent service to synchronize its cache with the infrastructure service.
   - **WEM monitoring port**.

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



4. In the **Advanced Settings** tab, enter impersonation and automatic refresh settings.

   - **Enable Windows account impersonation**. By default, this option is cleared and the infrastructure service uses mixed-mode authentication to connect to the database (using the SQL account *vuemUser* created during database creation). If you instead selected a Windows infrastructure service account during database creation, you must select this option and specify the same Windows account for the infrastructure service to impersonate during connection. The account you select must be a local administrator on the infrastructure server.

     To select a gMSA, follow the same steps as selecting an AD user.

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

NOTE:

By default, *LDAP* is used when browsing the account. To enforce secure communication over *LDAPS*, add the following registry entry:

- Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\WEM`
- Name: `EnableLDAPS`
- Type: `REG_SZ`
- Value: `1`

- **Set vuemUser SQL user account password**. Allows you to inform the infrastructure service of a custom password configured for the *vuemUser* SQL user during database creation. Only enable this option if you provided your own password during database creation.
- **Infrastructure service cache refresh delay**. Time (in minutes) before the infrastructure service refreshes its cache. The cache is used if the infrastructure service is unable to connect to SQL.
- **Infrastructure service SQL state monitor delay**. Time (in seconds) between each infrastructure service attempt to poll the SQL server.
- **Infrastructure service SQL connection timeout**. Time (in seconds) which the infrastructure service waits when trying to establish a connection with the SQL server before terminating the attempt and generating an error.
- **Enable debug mode**. If enabled, the infrastructure service is set to verbose logging mode.
- **Use cache even if online**. If enabled, the infrastructure service always reads site settings from its cache.
- **Enable performance tuning**. Lets you optimize the performance in scenarios where the number of connected agents exceeds a certain threshold (by default, 200). As a result, it takes a shorter time for the agent or the administration console to connect to the infrastructure service.
    - **Minimum number of worker threads**. Specifies the minimum number of worker threads that the thread pool creates on demand. Set the number of worker threads in the range of 30-3000. Determine the value based on the number of connected agents. By default, the minimum number of worker threads is 200.

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

- **Minimum number of asynchronous I/O threads**. Specifies the minimum number of asynchronous I/O threads that the thread pool creates on demand. Set the number of asynchronous I/O threads in the range of 30-3000. Determine the value based on the number of connected agents. By default, the minimum number of asynchronous I/O threads is 200.

IMPORTANT:

This feature is especially useful when the agent or the administration console intermittently disconnects from the infrastructure service.

Note:

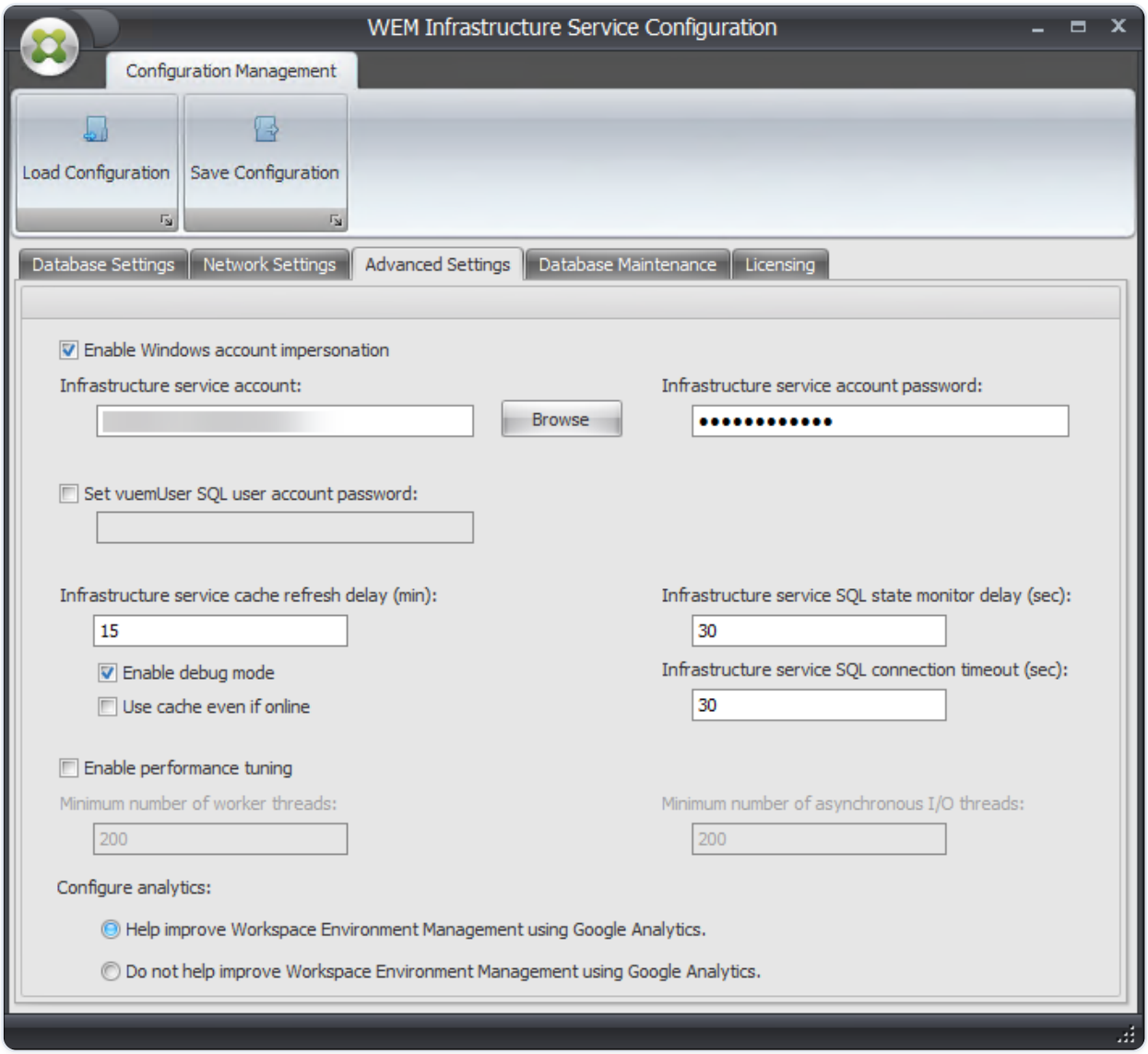
The values you set in the Enable performance tuning fields are used when new requests are made and before switching to an algorithm for managing thread creation and destruction. For more information, see `<https://docs.microsoft.com/en-us/dotnet/api/system.threading.threadpool.setminthreads?view=netframework-4.8>` and `<https://support.microsoft.com/en-sg/help/2538826/wcf-service-may-scale-up-slowly-under-load>`.

- **Help improve Workspace Environment Management using Google Analytics**. If selected, the infrastructure service sends anonymous analytics to the Google Analytics server.
- **Do not help improve Workspace Environment Management using Google Analytics**. If selected, the infrastructure service does not send anonymous analytics to the Google Analytics server.

IMPORTANT:

Starting with 2212, Workspace Environment Management determines which option to select based on the region of the machine hosting the infrastructure service. If the machine resides in non-European regions, the first option is selected. If the machine resides in European regions, the second option is selected. The behavior applies only to fresh installations.

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



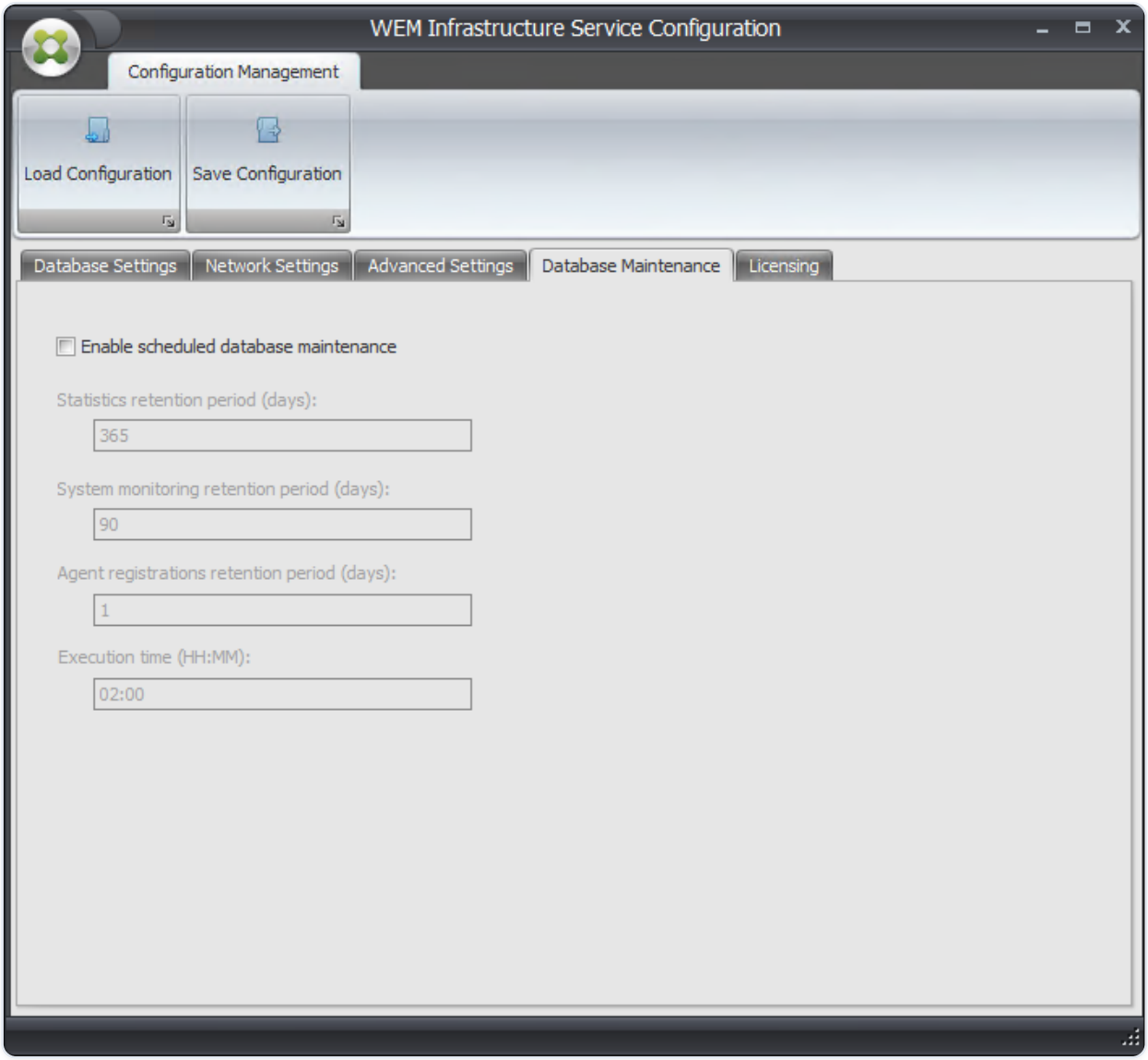
5. You can use the **Database Maintenance** tab to configure database maintenance.

   - **Enable scheduled database maintenance**. If enabled, this setting deletes old statistics records from the database at periodic intervals.
   - **Statistics retention period**. Determines how long user and agent statistics are retained. The default is 365 days.
   - **System monitoring retention period**. Determines how long system optimization statistics are retained. The default is 90 days.
   - **Agent registrations retention period**. Determines how long agent registration logs are retained in the database. The default is 1 day.
   - **Execution time**. Determines the time at which the database maintenance action is performed. The default is 02:00.

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

TIP

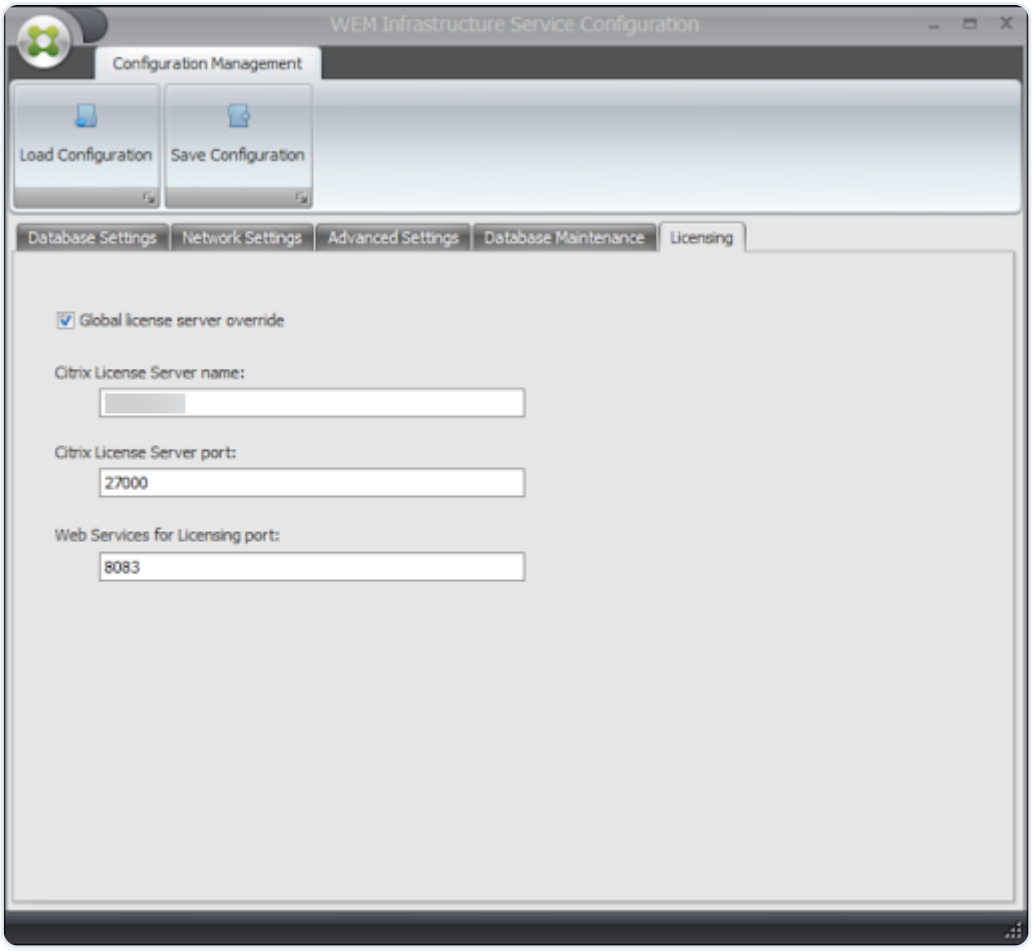
As a best practice, we recommend that you enable scheduled database maintenance to reduce the database size and achieve the best performance. If there is more than one infrastructure service in a single WEM deployment, enable it only for one infrastructure service.



6. You can optionally use the **Licensing** tab to specify a Citrix License Server during infrastructure service configuration. If you do not, when an administration console connects to a new Workspace Environment Management database for the first time, you must enter the Citrix License Server credentials in the **About** tab of the administration console ribbon. The Citrix License Server information is stored in the same location in the database in both cases.

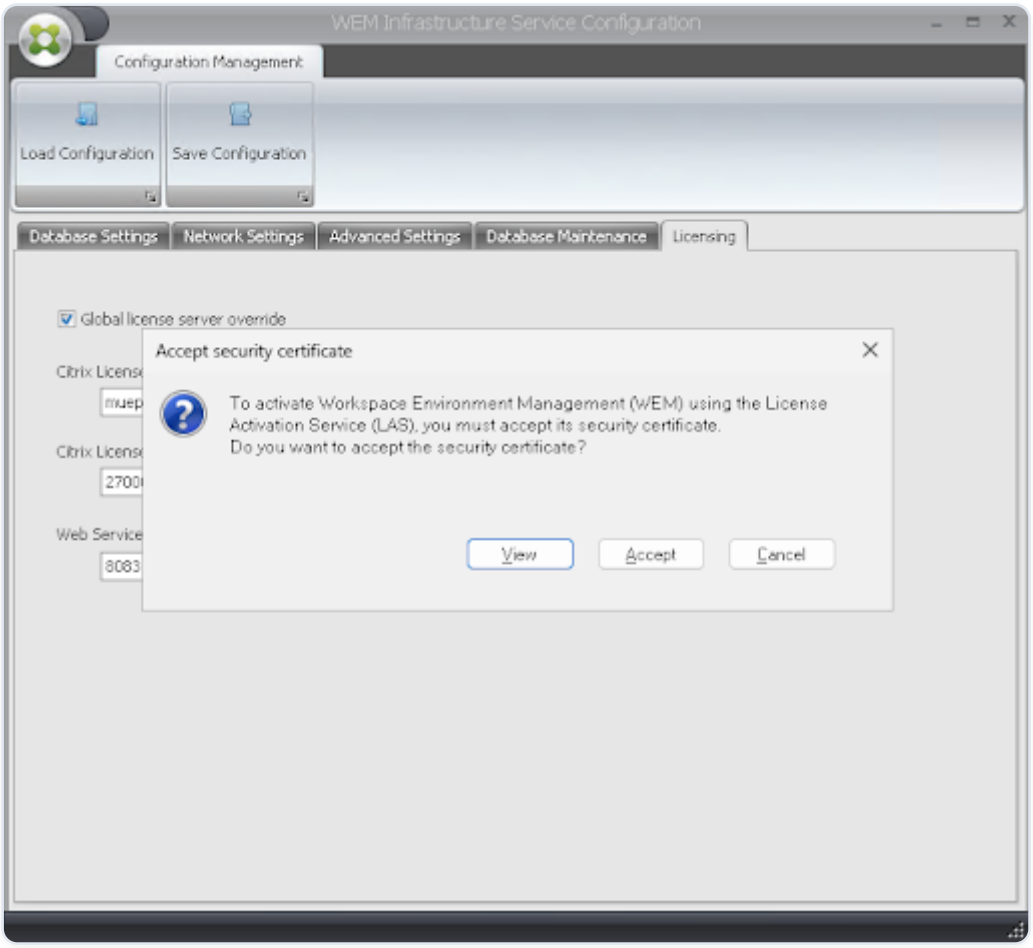
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Global license server override**. Select this option to specify the Citrix License Server details for Workspace Environment Management. Enter the Citrix License Server name, Citrix License Server port, and Web Services for Licensing port (also called the License Activation Service port). These settings override any existing Citrix License Server information stored in the Workspace Environment Management database.



7. Click **Save Configuration** to save your settings.
8. To activate Workspace Environment Management (WEM) using the License Activation Service (LAS), click **Accept** in the dialog box to approve its security certificate.

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



NOTE:

If the LAS is unavailable, WEM falls back to the legacy Citrix License Server for activation.

Administration console

Install the administration console

NOTE:

If you intend to assign resources published in Citrix StoreFront stores as application shortcuts in Workspace Environment Management from the administration console, ensure that Citrix Workspace app for Windows is installed on the administration console machine and on the agent host machine. For more information see System requirements.

Run **Citrix Workspace Environment Management Console.exe** on your administrator console environment.

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

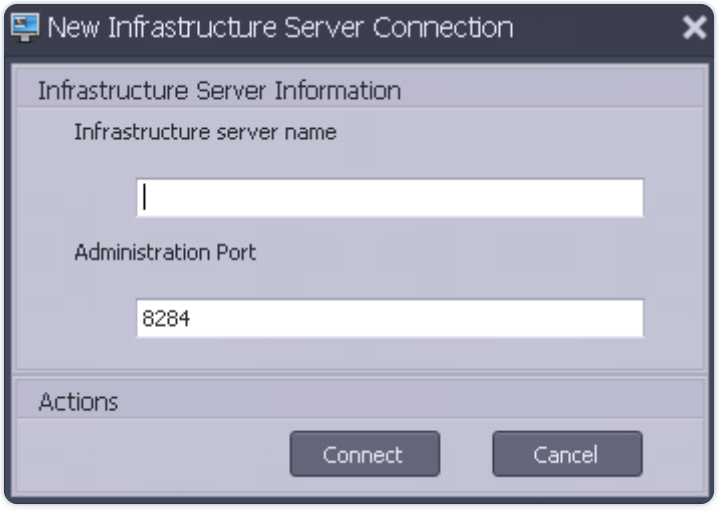
You can choose a silent installation or upgrade of the infrastructure services. For example:

- .\Citrix Workspace Environment Management Console.exe `/quiet ConsoleLocation="C:\test\Administration Console" /log "C:\test\test.log"`
- `/quiet ConsoleLocation="C:\test\Administration Console" /log "C:\test\test.log"`
  - `/quiet`. Indicates silent mode.
  - `/log`. Indicates logging file location.
  - `ConsoleLocation`. Indicates the installation path for the administration console.

Create an infrastructure server connection

In the **Start** menu select **Citrix®>Workspace Environment Management™>WEM Administration Console**. By default, the administration console launches in a disconnected state.

In the ribbon, click **Connect** to open the **New Infrastructure Server Connection window**.



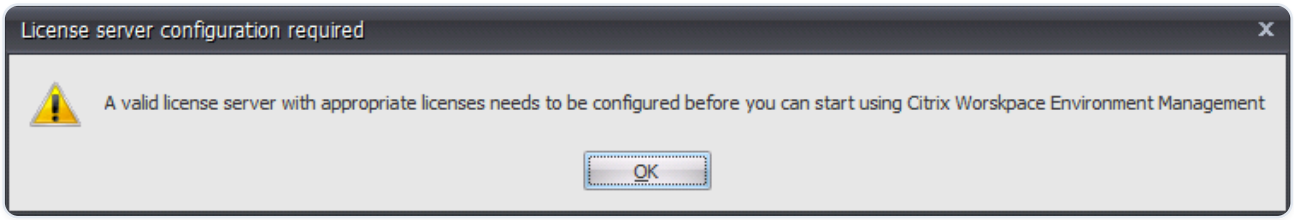
Enter the following values and click **Connect**:

Infrastructure server name. The name of the Workspace Environment Management infrastructure server. It must resolve from the administration console environment exactly as you type it.

Administration port. The port on which the administration console connects to the infrastructure service.

The first time you connect to a new database, you see the following message because a Citrix License Server with valid licenses is not yet configured:

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

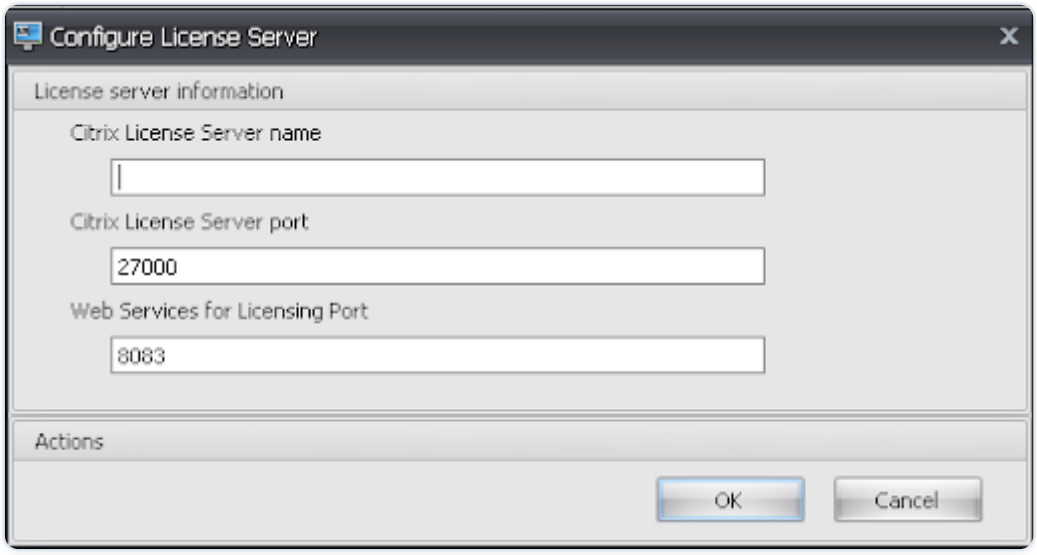


Configure the database with a license server

To configure the database with a license server, in the administration console ribbon, click **About**, then click **Configure License Server** and enter your Citrix License Server details:

- Citrix License Server name: Enter the server FQDN.
- Citrix License Server port: Enter the server port.
- Web Services for Licensing Port: Enter the License Activation Service port.

The Citrix License Server address must resolve from the administration console environment exactly as entered.



NOTE:

To activate Workspace Environment Management (WEM) using the License Activation Service (LAS), accept its security certificate by clicking **Accept** in the dialog box that appears after you click **OK** to save changes.

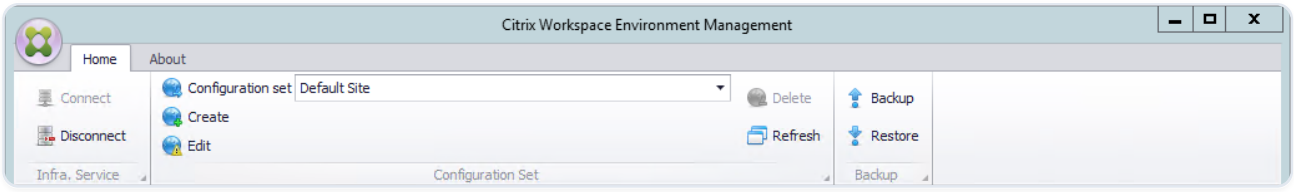
Import quickstart settings

Workspace Environment Management includes XML files which you can use to pre-configure your Workspace Environment Management database so that it is proof-of-concept-ready out of the box.

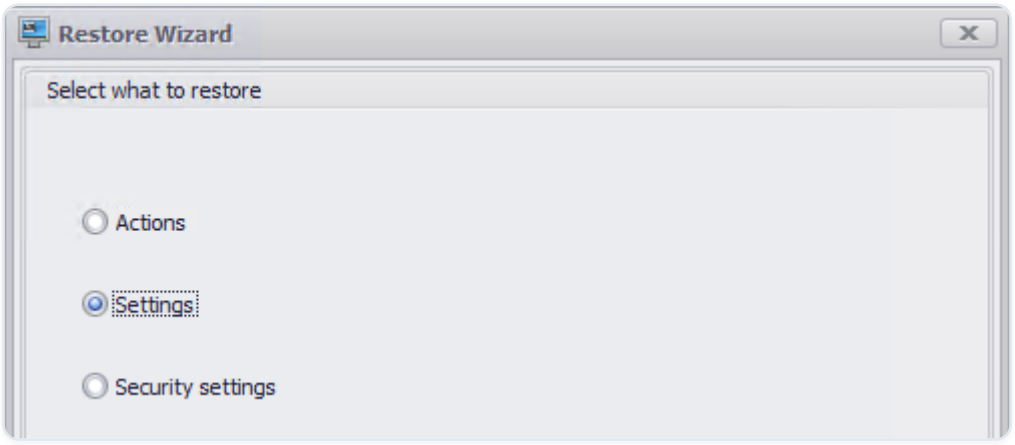
© 1997–2026 Citrix Systems, Inc. All rights reserved.

The XML files are provided in the folder "Configuration Templates" in the Workspace Environment Management installer package.

To import the quickstart setting files, in the **Home** ribbon click **Restore**:



In the **Restore Wizard**, select **Settings** and click **Next**.

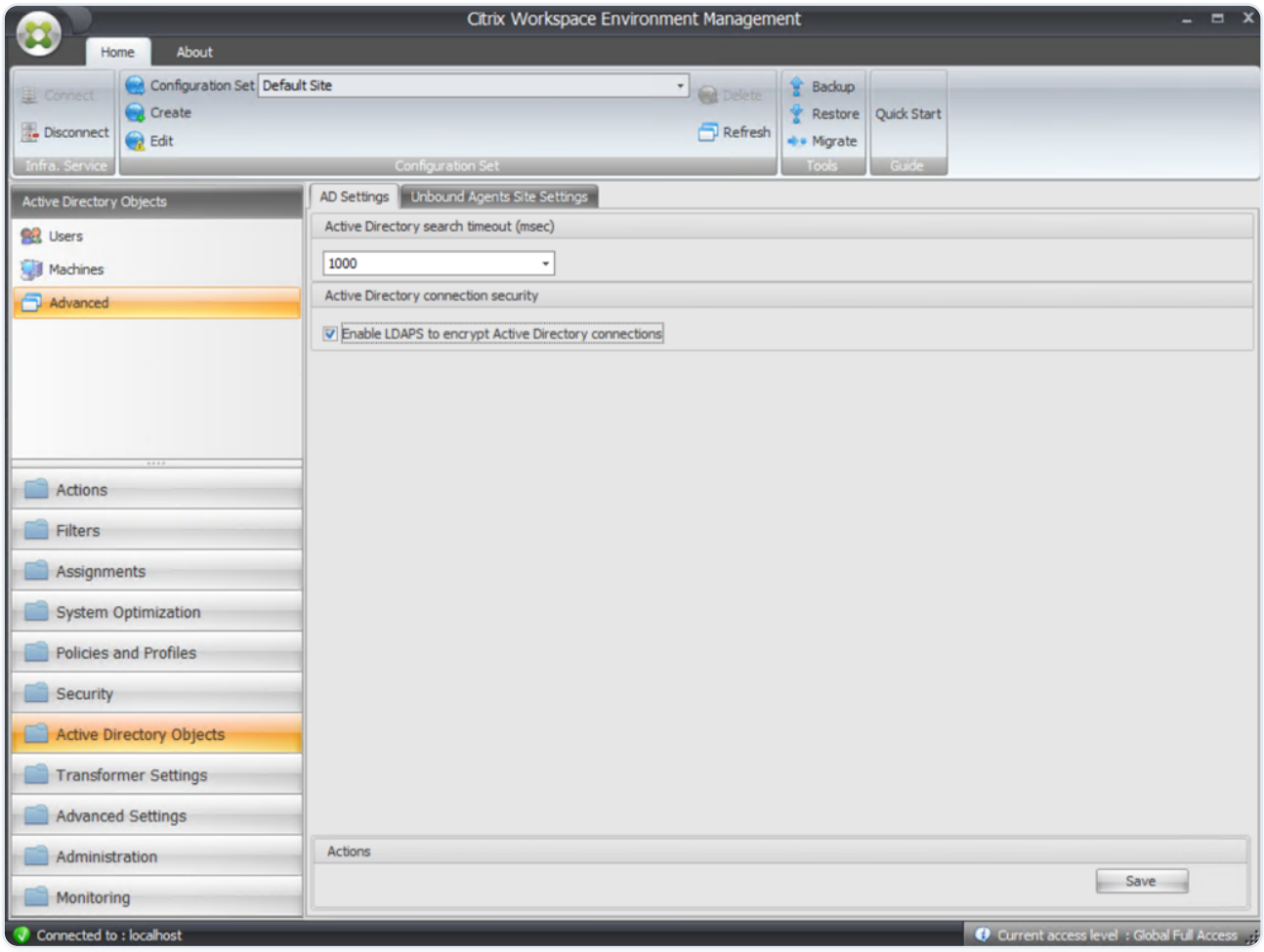


In the **Restore Wizard**, select the folder "Configuration Templates" containing the quickstart setting files, and then select all Setting Types.

Enforce LDAPS to encrypt Active Directory connections

By default, WEM uses *LDAP* for Active Directory queries. To enforce secure communication over *LDAPS*, select **Enable LDAPS to encrypt Active Directory connections** under **Advanced > Active Directory Objects**.

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



Web console service

The web console service provides HTTPS services to support the Workspace Environment Management (WEM) web console and communicate with the WEM infrastructure service.

Account: A specified domain user account that has the WEM global full access, and belongs to the administrator user group on the web console server where the web console service runs.

We recommend installing the web console service on the machine where the WEM infrastructure service runs.

Install the web console service

To install the web console service, run **Citrix Workspace Environment Management Web Console.exe**. By default, the infrastructure services install into the following folder: `C:\\Program Files (x86)\\Citrix\\Workspace Environment Management Web Console`.

You can customize your installation using the following arguments:

ApiLocation: The directory to install the web console service.

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

You can choose a silent installation or an upgrade of the infrastructure services. For example:

- .\Citrix Workspace Environment Management Web Console.exe `/quiet ApiLocation="C:\WEM\webconsole"`
- `.\setup.exe /quiet ApiLocation="path:\to\install" /log="path:\to\log"`
  - setup.exe. Lets you replace it with the file name of the installer.
  - `/quiet`. Indicates that no user interface appears during the installation.
  - `/log`. Indicates logging file location.
  - `ApiLocation="path:\to\install"`. Specifies where to install the web console service.

Configure the Web console service

You must configure the web console service by using the following tool in the installation path: `WEM Web Console Configuration.exe`.

Prerequisites

This release of web console service is compatible with WEM 2303 deployments and later.

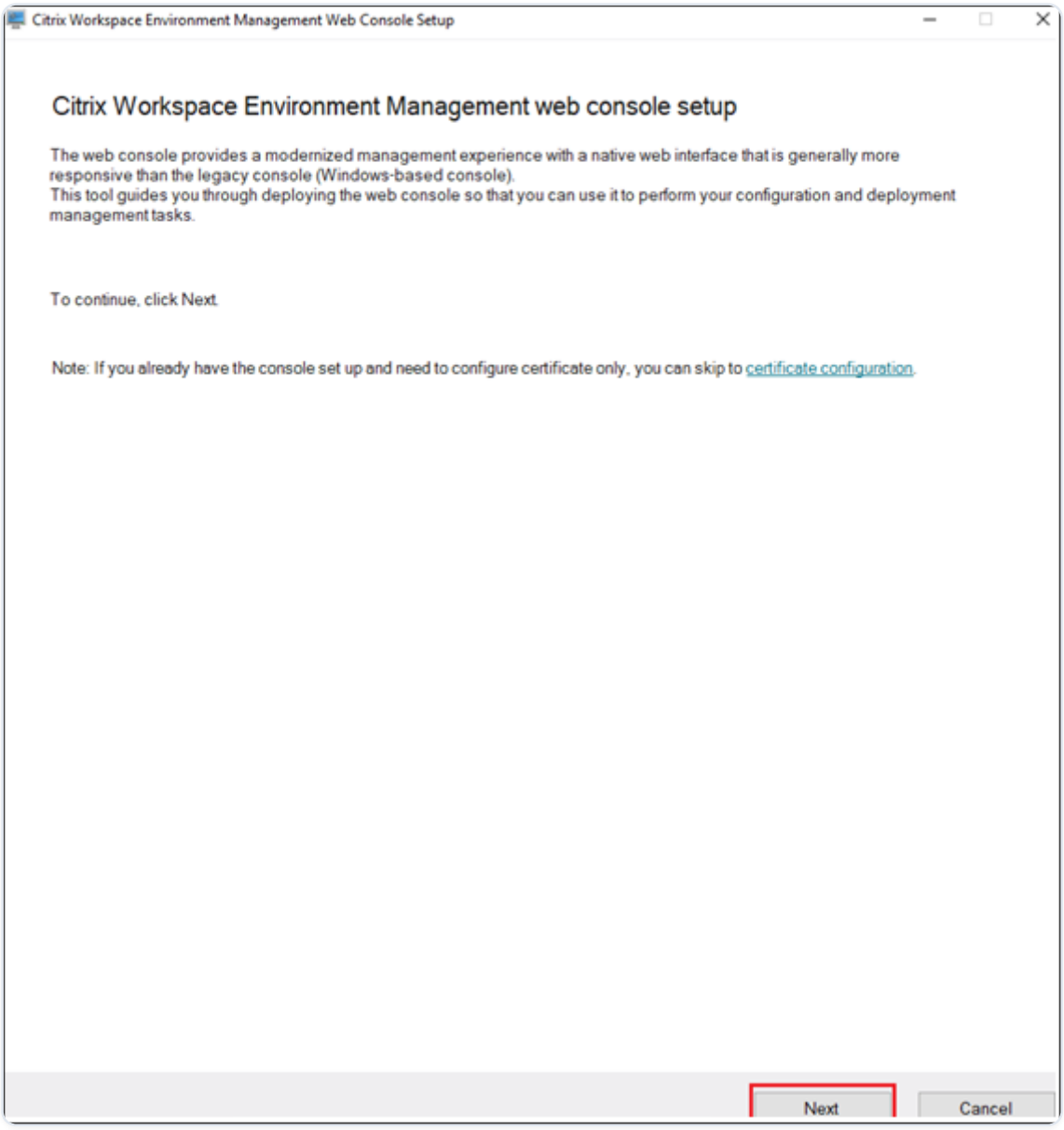
For deployments earlier than 2303, first, upgrade to 2303 and then configure the web console service.

Configure and start the Web console service

To configure and start the web console service, complete the following steps.

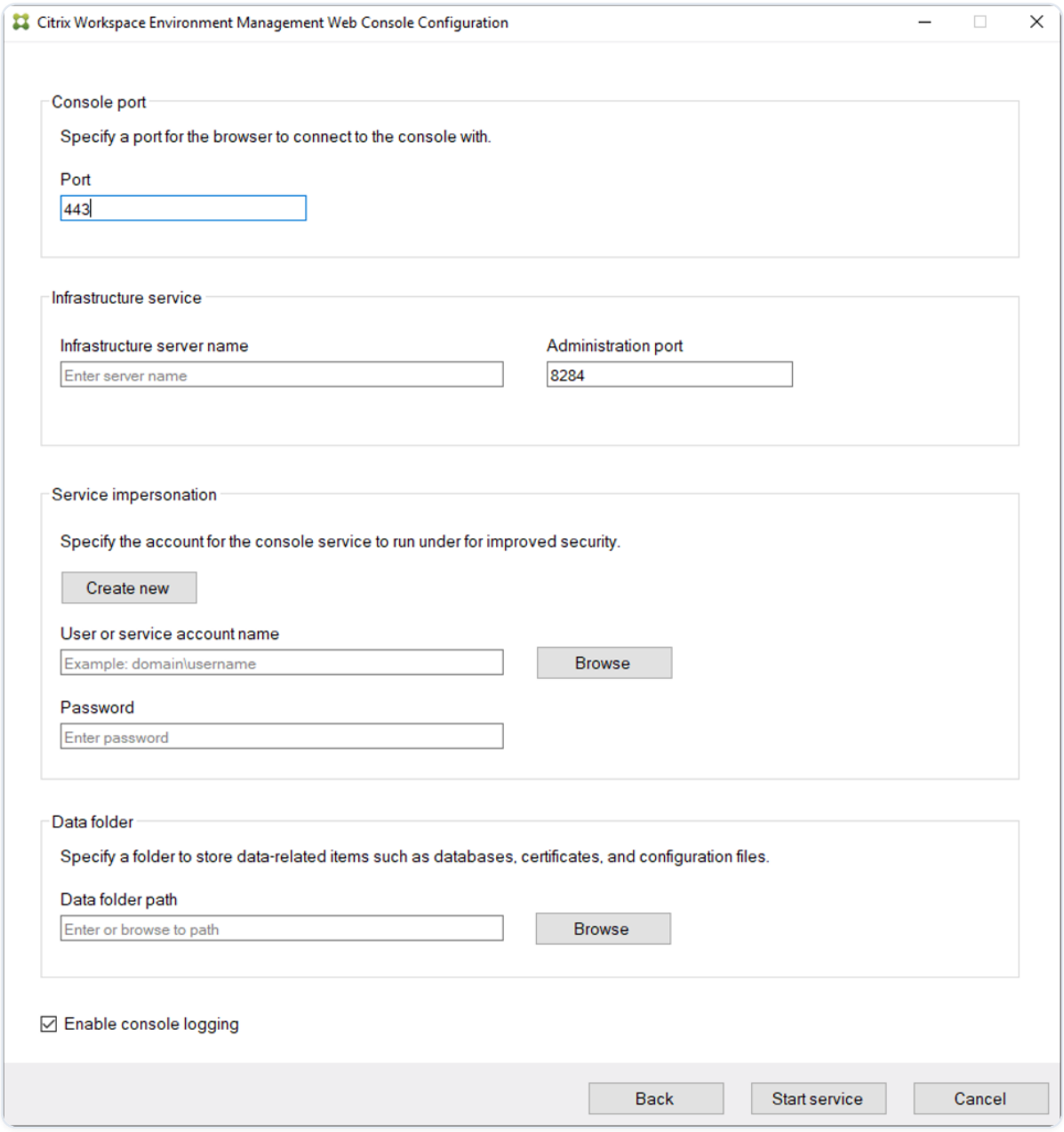
1. Launch the `WEM Web Console Configuration.exe` tool in the web console service folder and click **Next**.

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



2. Configure the console port by specifying a port for the browser to connect to the console. The default port is 443.
3. Configure the Infrastructure service by specifying the Infrastructure service information.
    - For the Infrastructure server name, type the machine name, fully qualified domain name, or IP address of the WEM infrastructure server.
    - For the Administration port, type the port on which the web console connects to the infrastructure service. The default port is 8284.

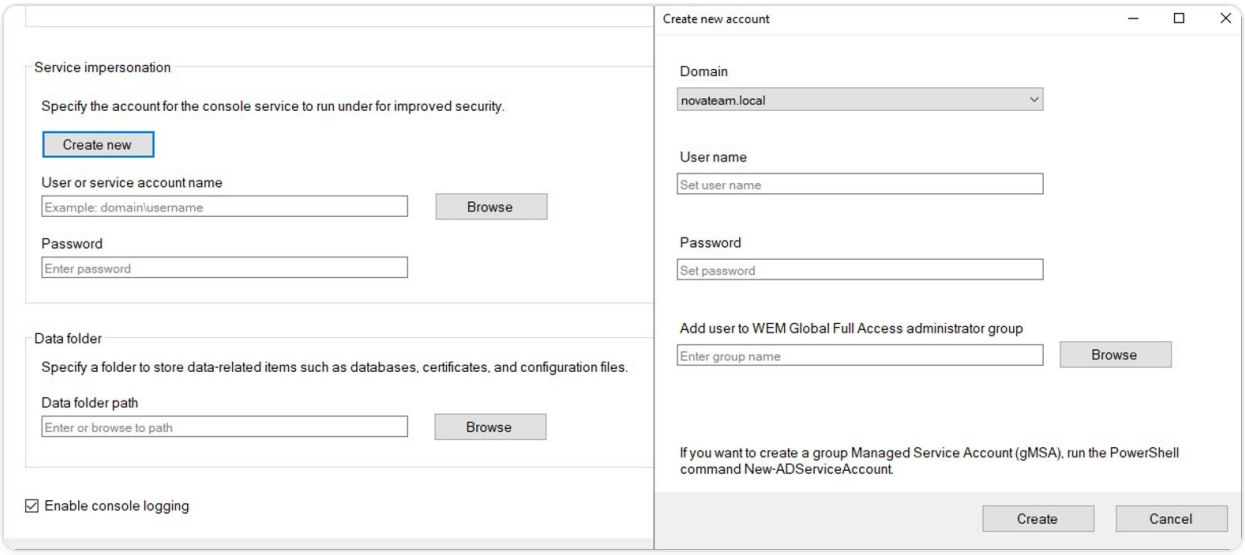
© 1997–2026 Citrix Systems, Inc. All rights reserved.



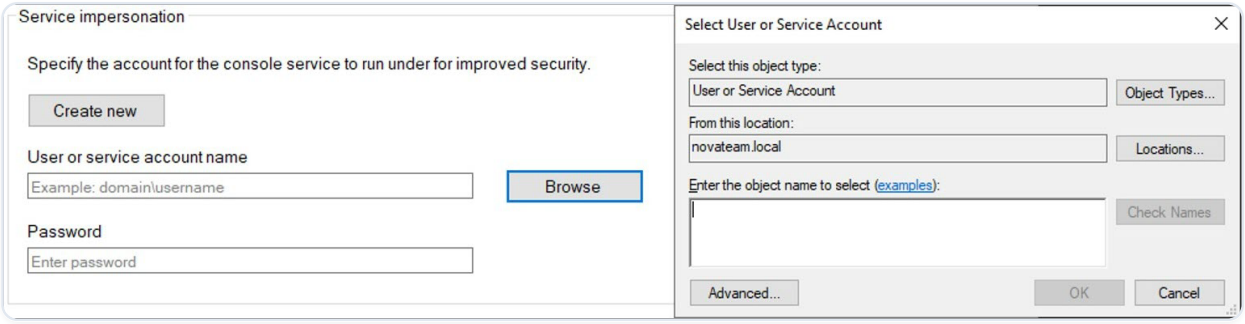
4. Configure **Service impersonation** when the web console service impersonates the specific account to improve security. You can create a new user or select an existing user.

    - Create a new user and add the user to the WEM global full-access administrator group.

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



- Select an existing user from the WEM global full-access administrator group.

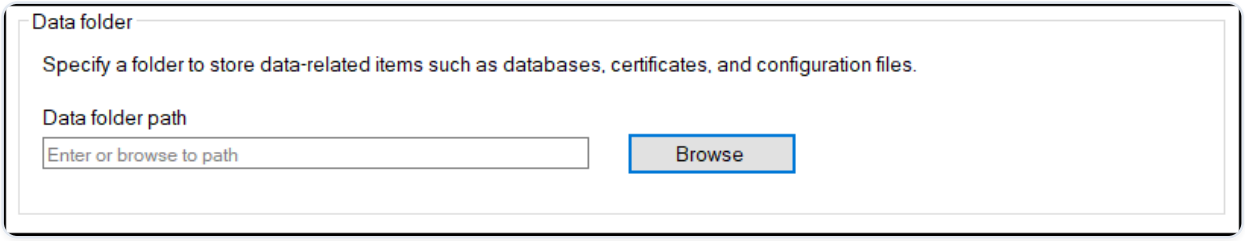


NOTE:

By default, *LDAP* is used when browsing the account. To enforce secure communication over *LDAPS*, add the following registry entry:

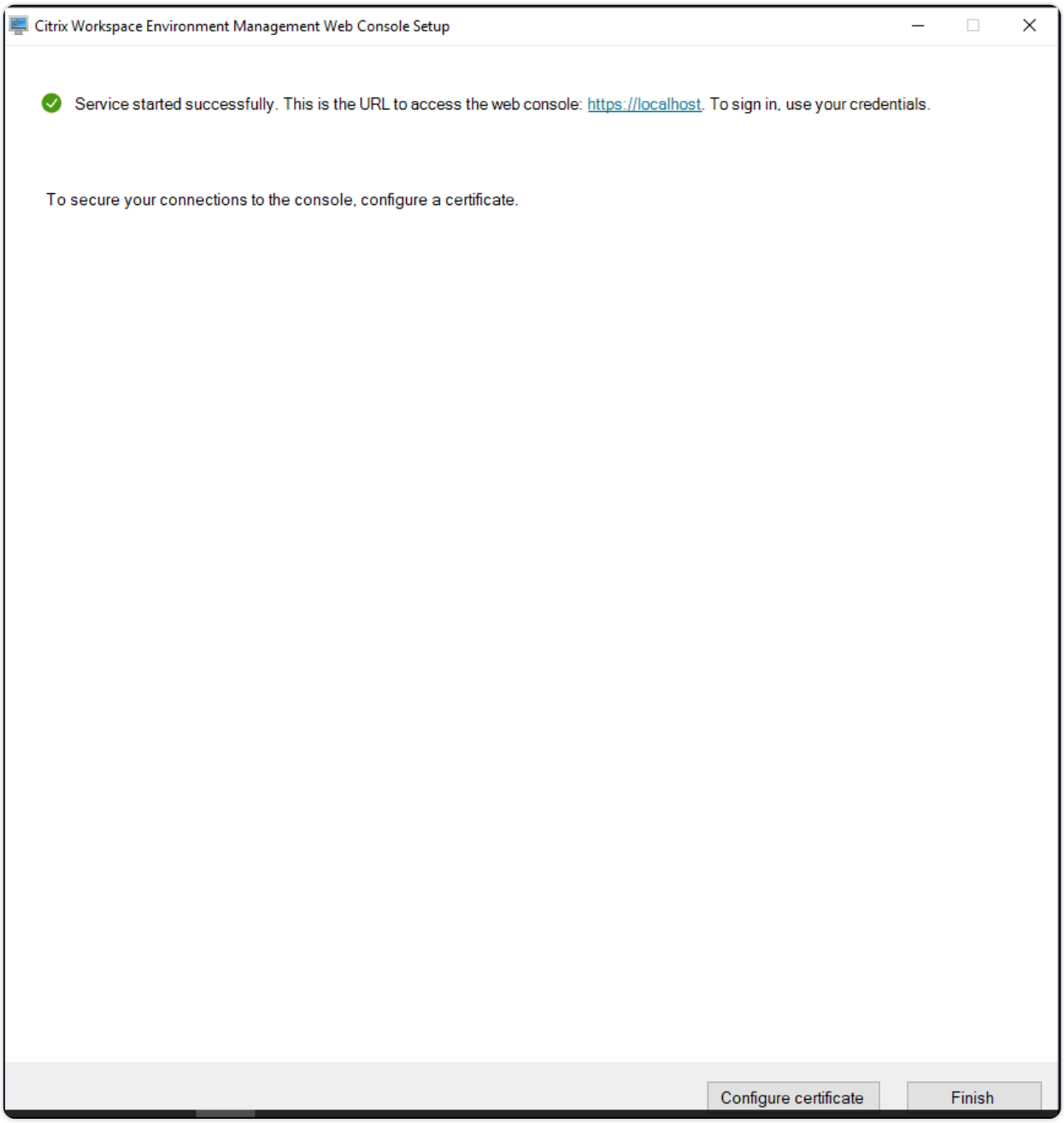
- Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\WEM`
- Name: `EnableLDAPS`
- Type: `REG_SZ`
- Value: `1`

5. Configure the **Data folder** by specifying a folder to share data-related items such as databases, and configuration files.



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

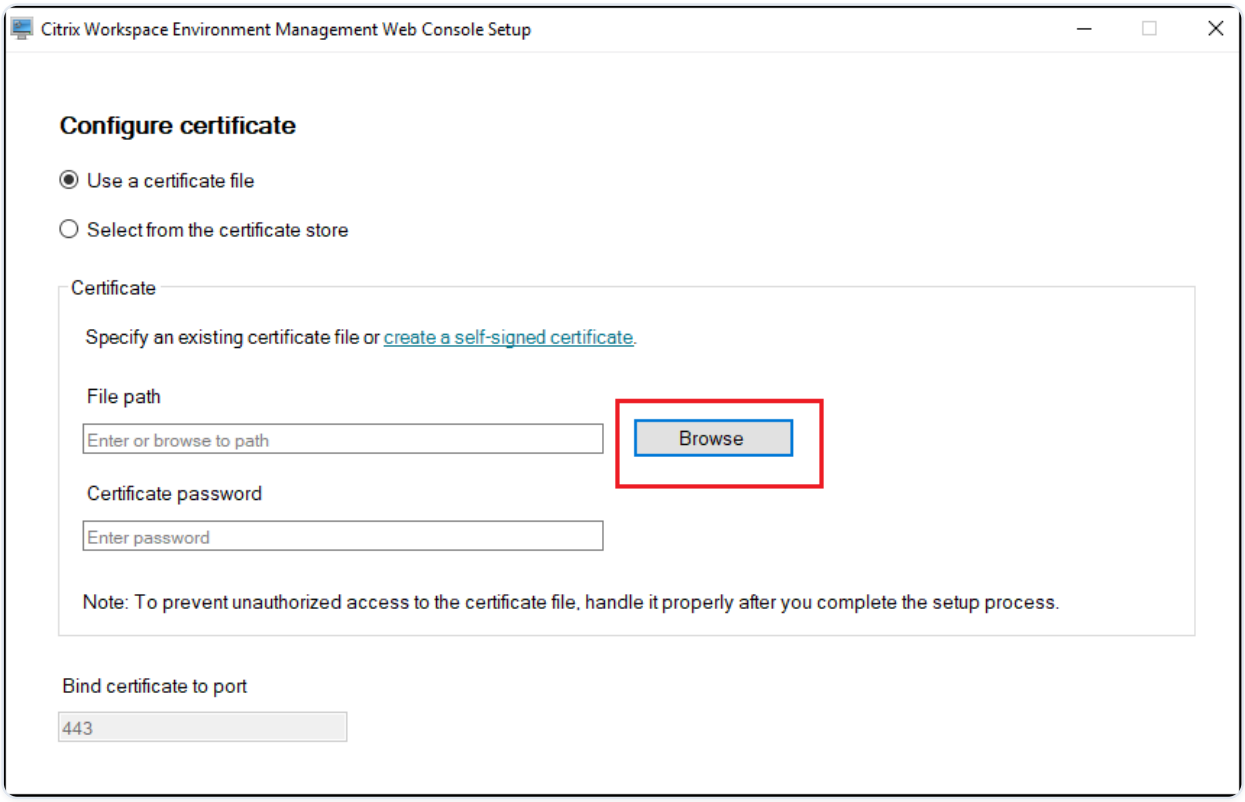
6. Click **Start service**.



7. After the successful start of the web console service, click **Configure certificate** to configure the certificate. There are two methods to configure the certificate.

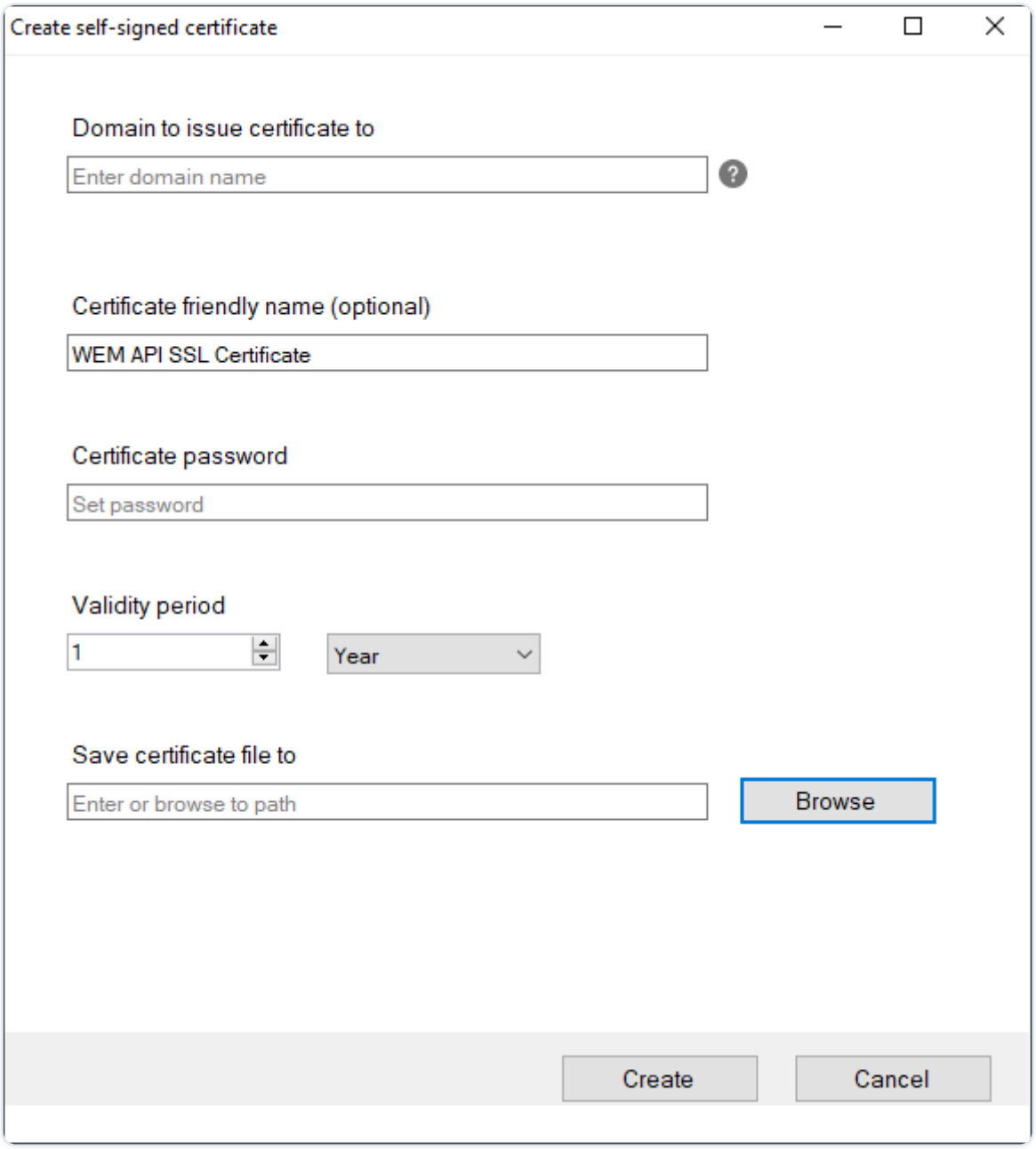
   - To use a certificate file, click **Browse**.

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



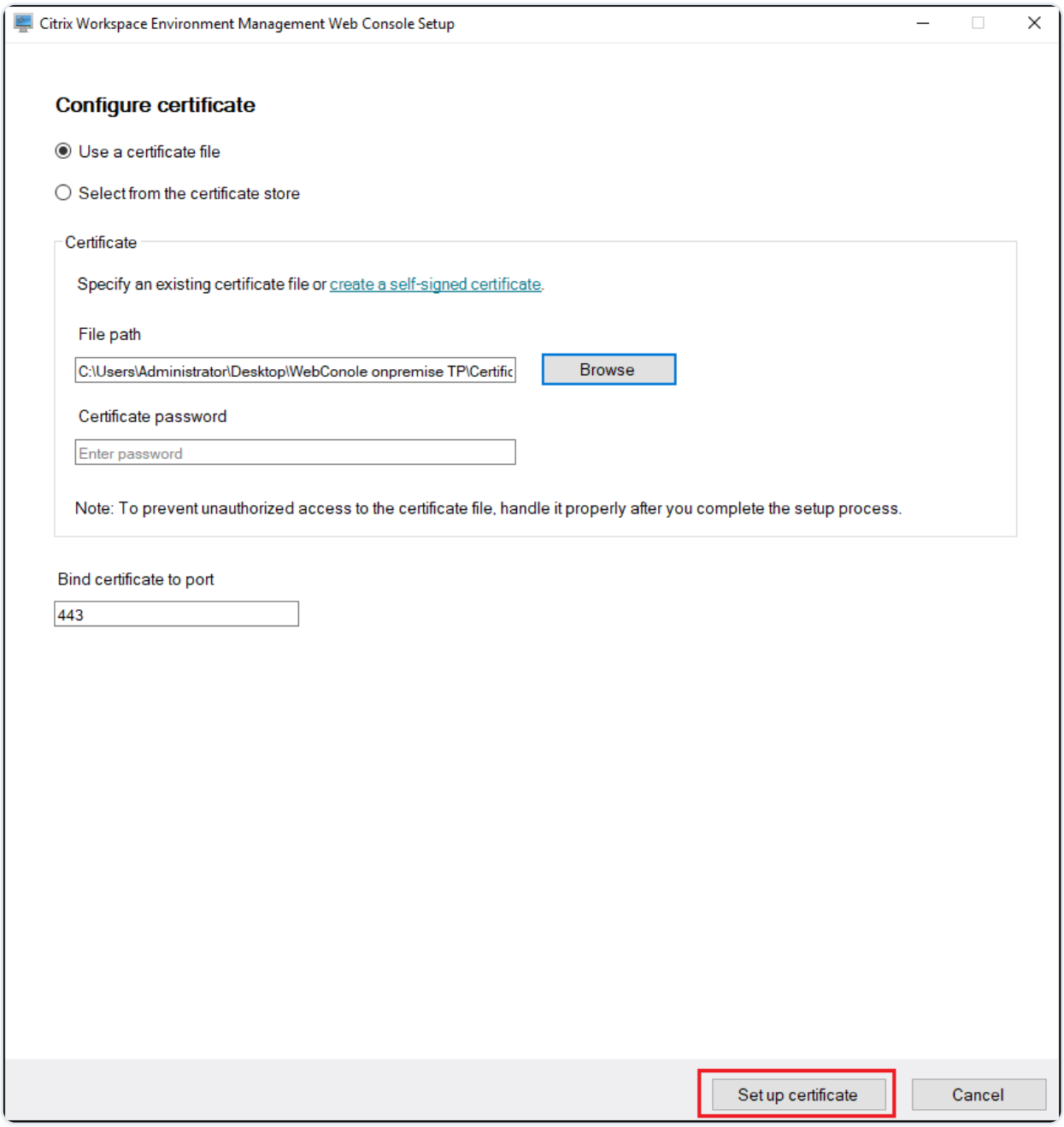
- To create a self-signed certificate, click **Create self-signed certificate**.

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



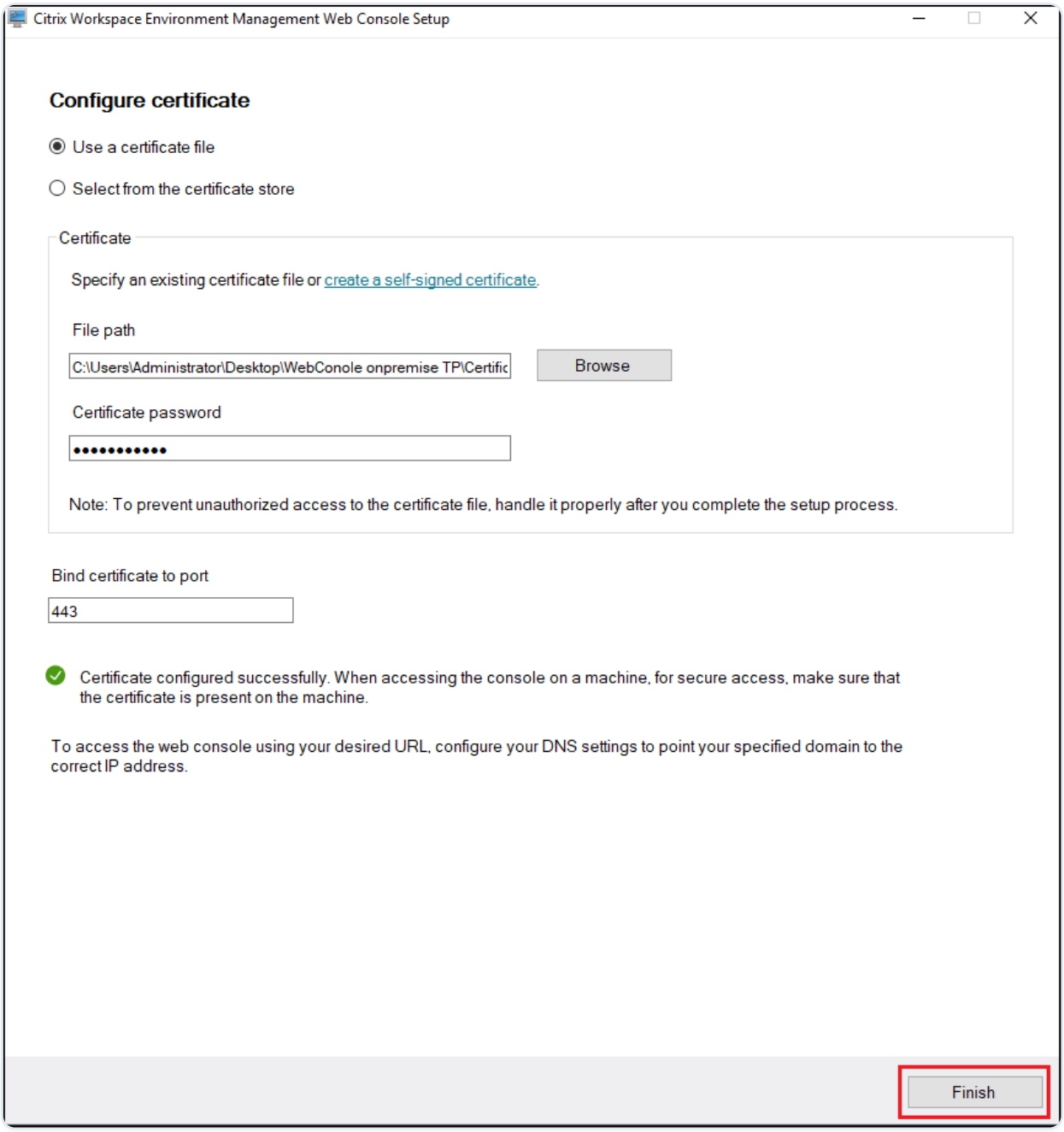
- Click **Set up certificate**.

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



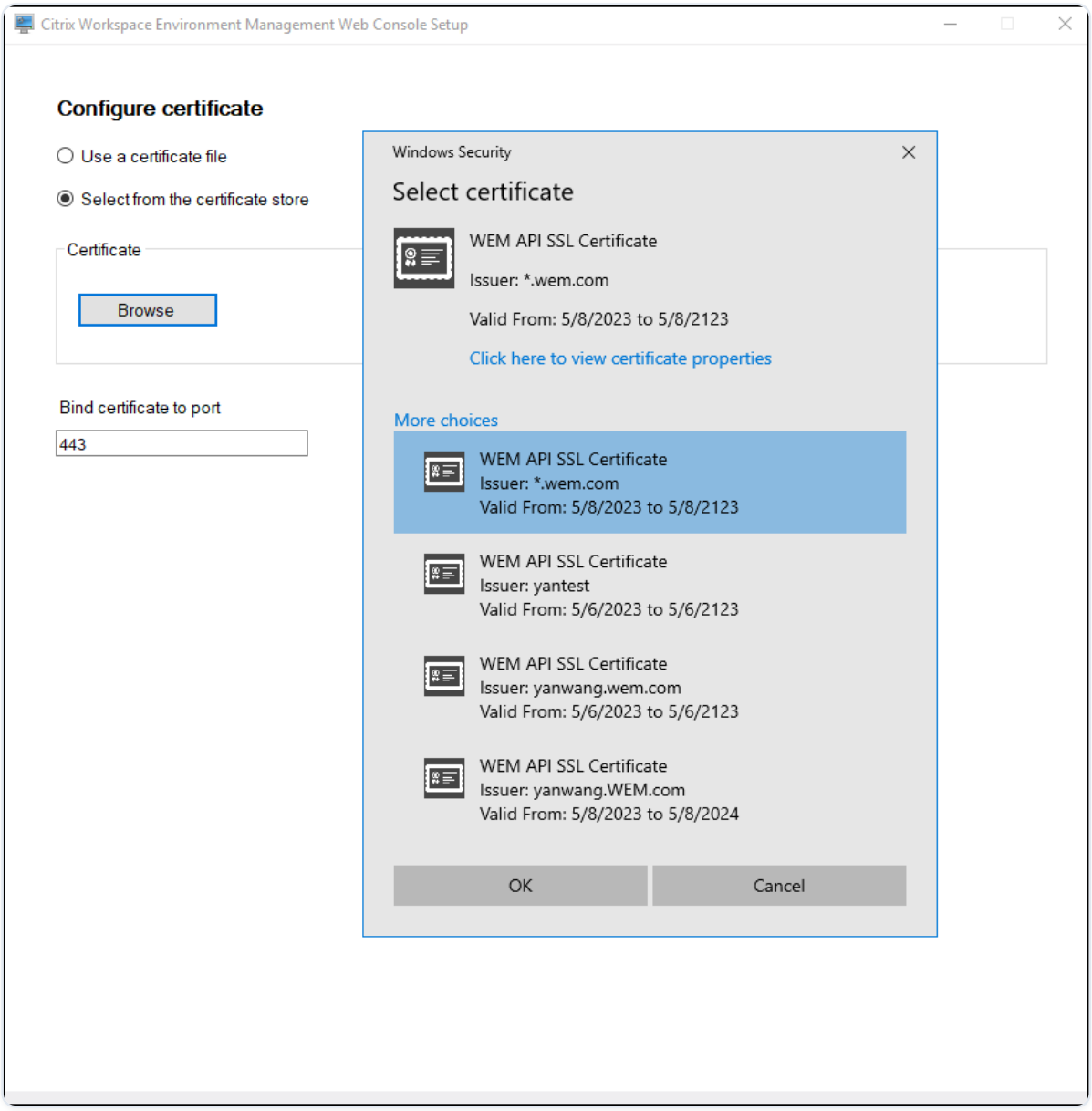
- After configuring the certificate successfully, click **Finish**.

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



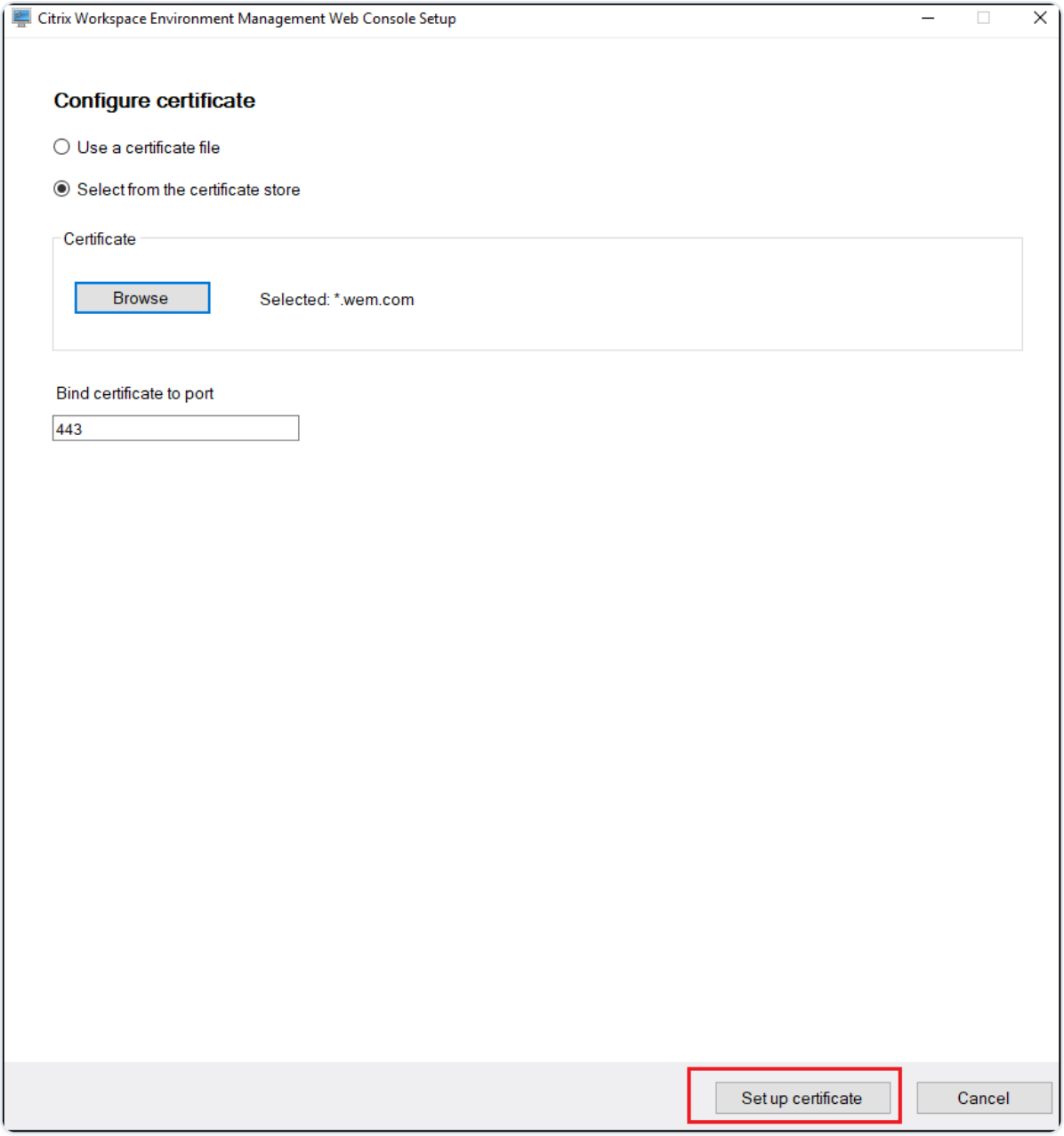
- To use a certificate from the certificate store, select the desired certificate.

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



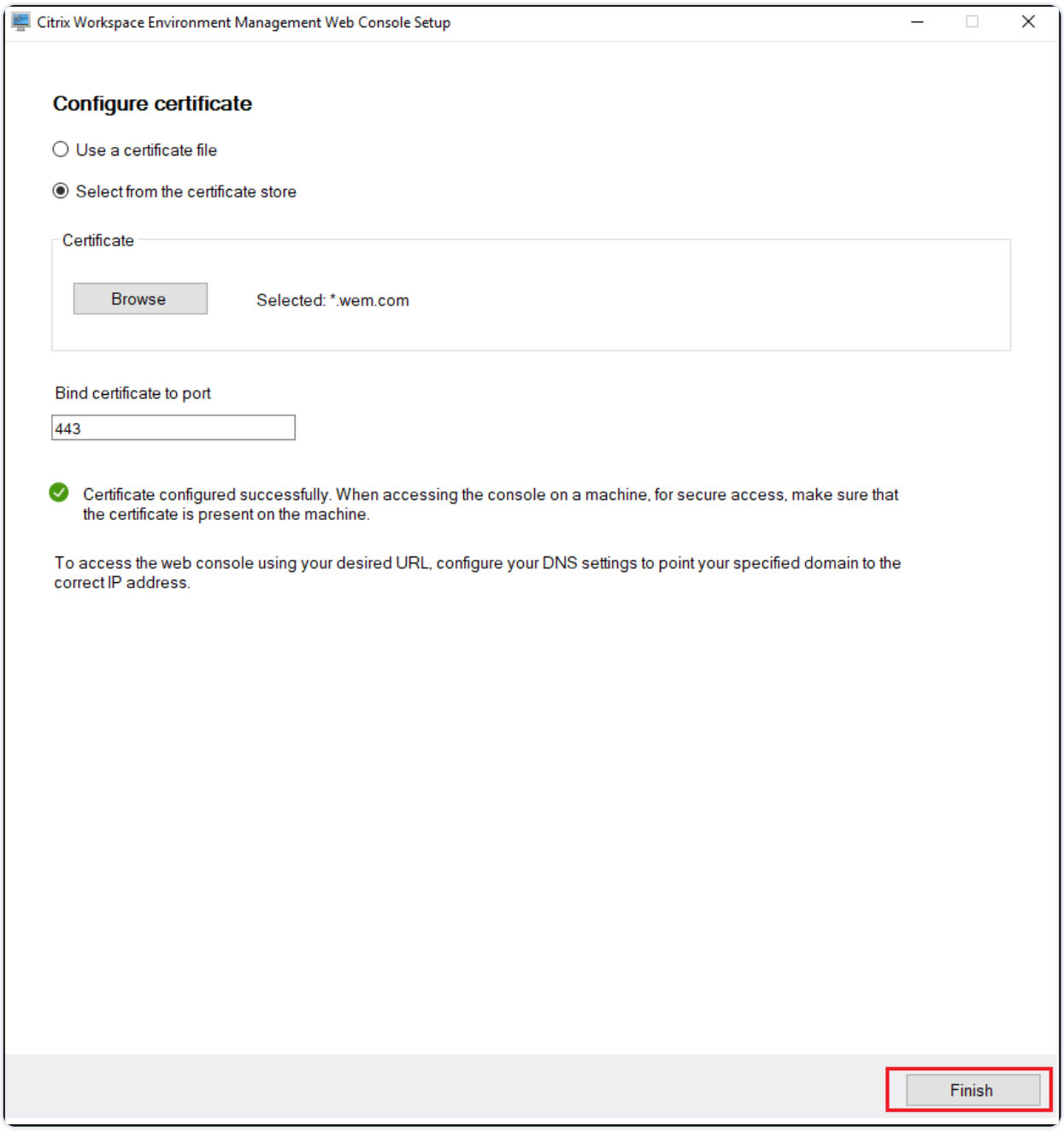
- Click **Set up certificate**.

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



- After configuring the certificate successfully, click **Finish**.

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



8. To create a global full-access account, go to the legacy console, and click **Administration** to manage permissions.

   NOTE:

   The Windows domain account must be a global full-access account.

   You must log in using a Windows domain account before using the web console.

   For more information about the WEM web console, see Manage (web console).

9. To use Template based GPO, Scripted task, Backup and restore, and files, you must set up a shared storage folder.

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

NOTE:

To set the permissions for the shared folder, follow these guidelines:

- Ensure that at least one user has full access to the shared folder, excluding the permissions to change permissions or take ownership.
- Verify that the shared folder is accessible from the machine hosting the web console service.
- If the configured user is the same user impersonated by the web console service, you can omit the credentials when configuring the shared folder in the web console. Otherwise, credentials must be specified. Using the impersonated user is the recommended approach. To enhance security and minimize access, limit the number of accounts with permissions to the shared folder as much as possible.

Go to the web console, click your account name in the top-right corner, click **Storage folder**, and configure the shared SMB path.

Set up licensing

Workspace Environment Management™ (WEM) validates your license entitlement through the Citrix License Server. Set up licensing for WEM based on the console you use:

- If you use the legacy console, set up licensing for the WEM infrastructure services.
- If you use the web console, set up licensing for both the WEM infrastructure services and the web console.

A WEM license entitlement does not affect WEM agent functionality. It only affects an administrator's ability to configure settings through the web console or the legacy console. Without a valid license, administrators cannot deploy new policies or modify existing ones through a console. Policies that have already been delivered to the agent are not affected.

NOTE:

WEM uses the Citrix® Licensing Activation Service (LAS) to validate entitlements. We recommend that you upgrade to:

- WEM version **2511** or later if you use the legacy console.
- WEM version **2603** or later if you use the web console.

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

Prerequisites

Before you set up licensing, ensure the following:

- A Citrix License Server with valid WEM entitlements is available.
- The WEM infrastructure server can reach the license server over HTTPS on the LAS port (default: **8083**).

> **NOTE:**
>
> If the license server is unreachable, license configuration and certificate acceptance fail. For more information about connectivity checks, see Troubleshoot WEM LAS issues.

Configure licensing for the infrastructure services

You can configure the WEM license for the infrastructure services in two ways:

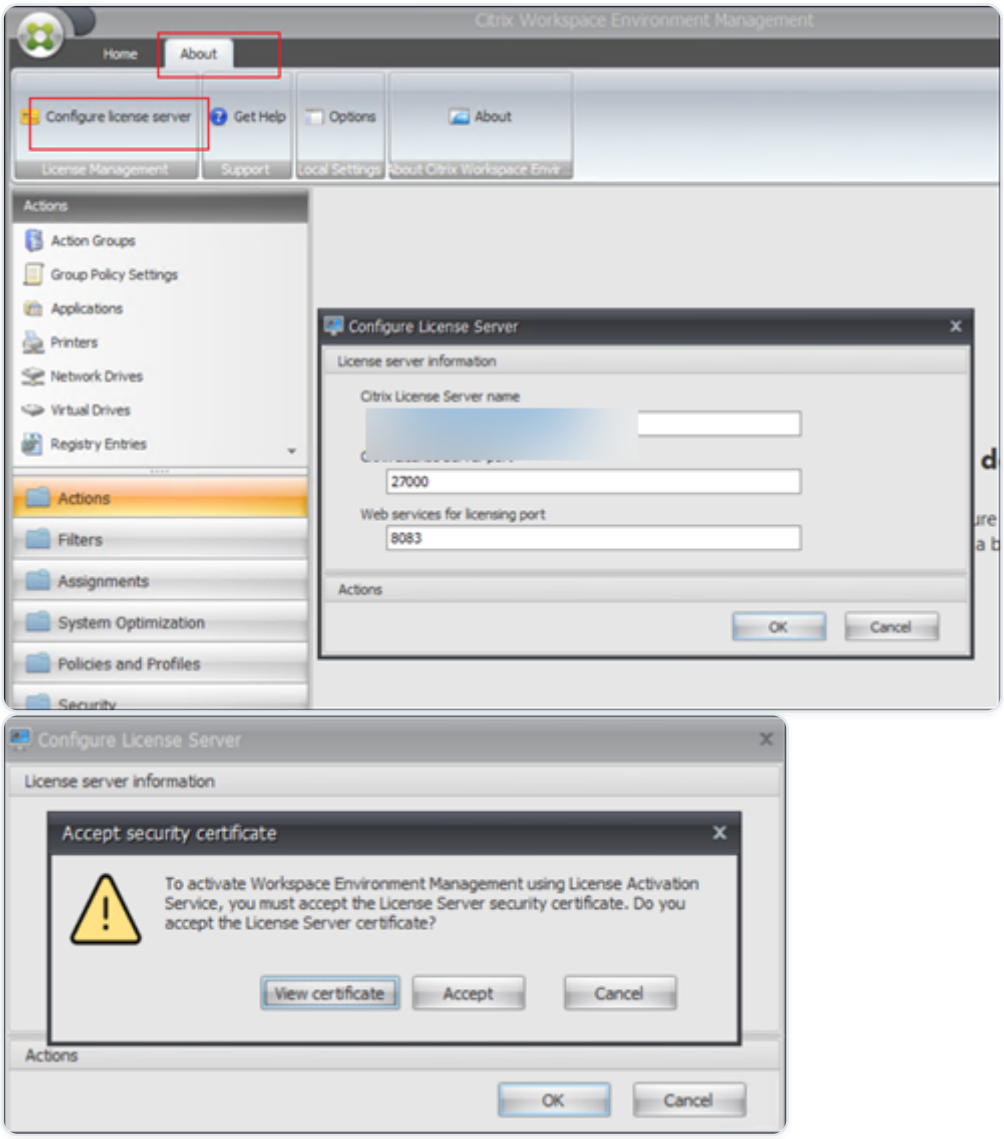
- Configure the license server globally for WEM infrastructure services
- Configure the license server for a single WEM infrastructure server

Configure the license server globally for WEM infrastructure services

If you have multiple WEM infrastructure servers, configure the license server **globally** in the WEM legacy console and apply the same settings to all servers.

1. In the WEM console, click **About** > **Configure License Server** to open the configuration dialog box.
2. Enter the license server information.
3. Click **OK**.
4. When the **Accept Security Certificate** dialog box appears, accept the certificate to complete the configuration.

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

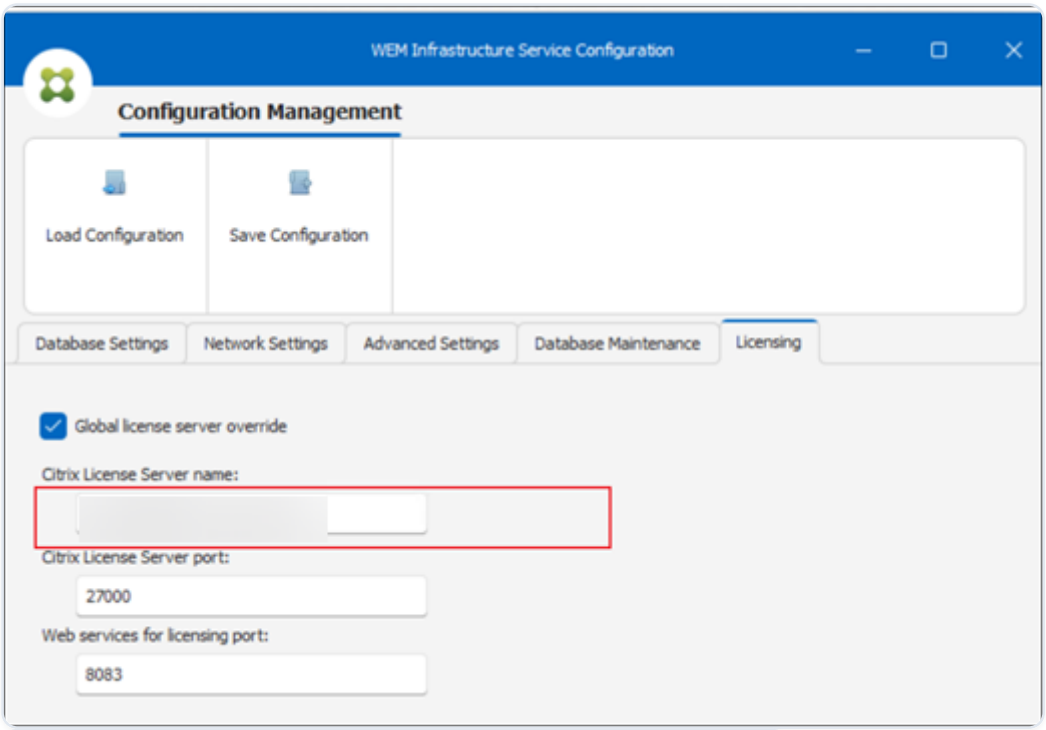


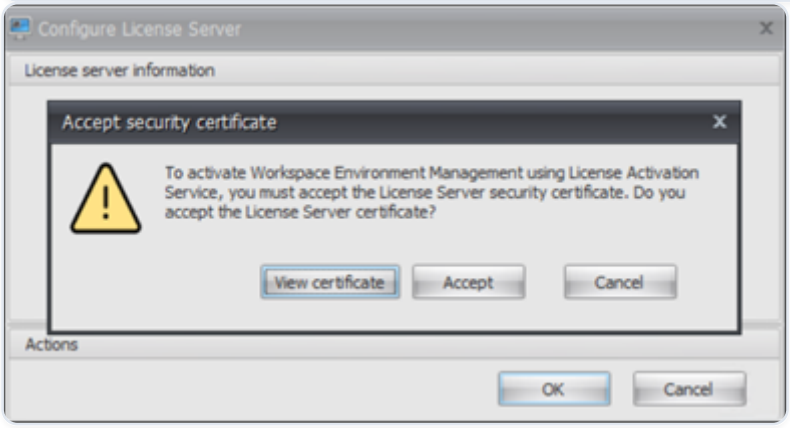
Configure the license server for a single WEM infrastructure server

Configure the license server for a specific WEM infrastructure server using the **WEM Infrastructure Service Configuration utility**.

1. Launch the **WEM Infrastructure Service Configuration utility**.
2. On the **Licensing** tab, enter the license server information.
3. Click **Save Configuration**.
4. When the **Accept Security Certificate** dialog box appears, accept the certificate to complete the configuration.

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





Configure licensing for the web console

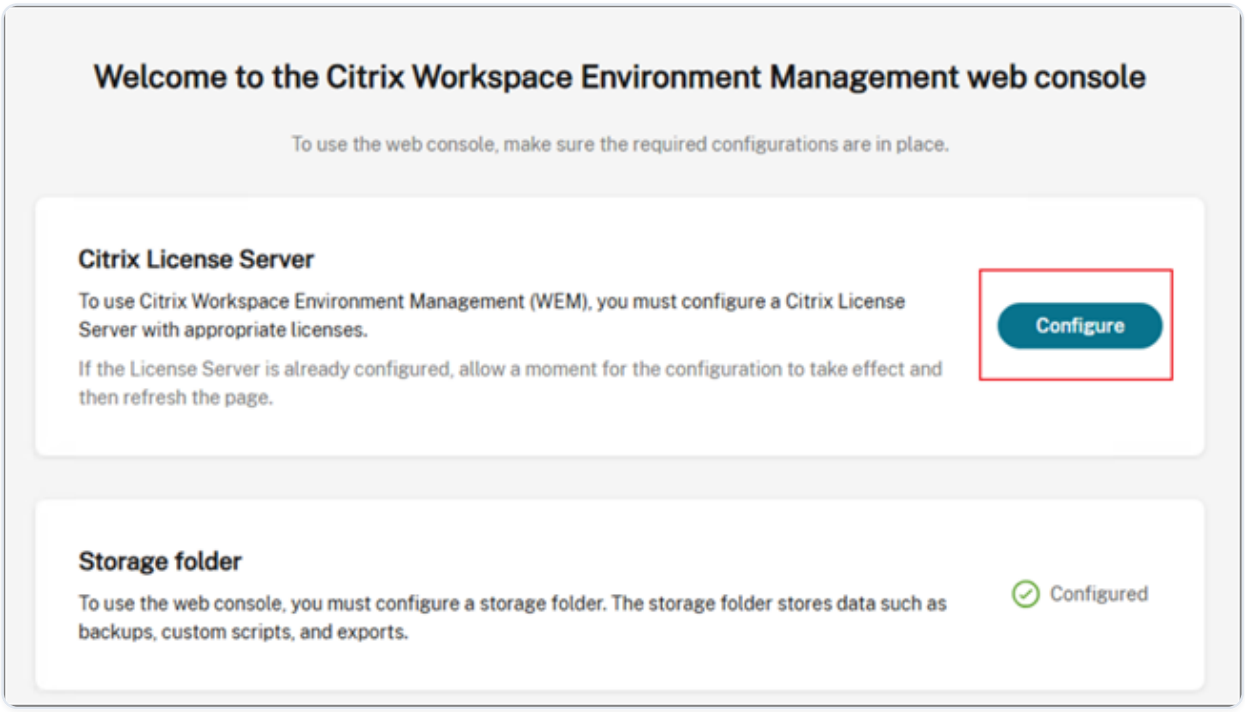
If you use the web console version **2603** or later, configure the license server for the web console after you configure licensing for the infrastructure services. Provide the Citrix License Server connection details, including the license server FQDN, port, and License Activation Service (LAS) port.

NOTE:

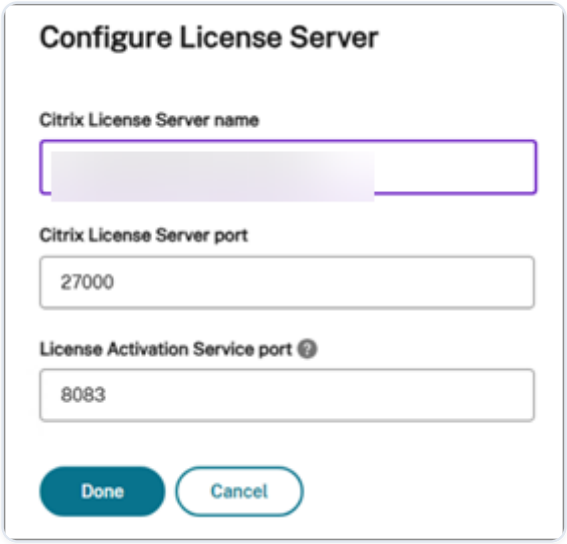
LAS simplifies the licensing experience by eliminating the need to download, upload, or manage license activation codes and product-specific license files. For more information, see License Activation Service.

1. Launch the web console. If no license server has been configured, a prompt appears.

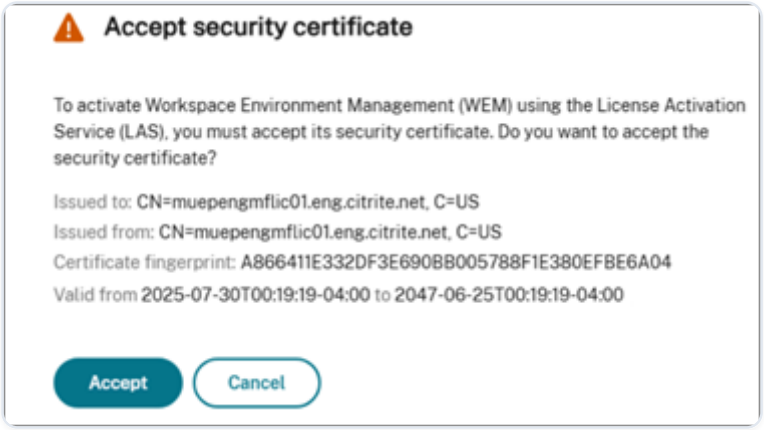
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Click **Configure**, and then enter the license server information.



3. When the **Accept Security Certificate** dialog box appears, accept the certificate to complete the configuration.



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

Re-accept the license server certificate

The first time you configure the license server, you accept the certificate as part of the configuration steps. You must re-accept the certificate under the following circumstances:

- You are upgrading WEM from a version that **did not support LAS** to a version that **supports LAS for the first time**.
- You have **renewed or replaced** the license server certificate.

NOTE:

If you have added the license server certificate to the machine's **Trusted Root Certification Authorities**, the dialog box does not appear. This is expected because LAS still works because the certificate is already trusted.

To re-accept the certificate, use the same method you used to configure the license server:

- **WEM Infrastructure Service Configuration utility**. Relaunch the utility and click **Save Configuration**. When the **Accept Security Certificate** dialog box appears, accept the certificate.
- **WEM console**. Reconfigure the license server in the WEM console. This action triggers the certificate acceptance process.

Verify that WEM LAS is working

After you configure the license server and accept the certificate, verify LAS based on the component you use:

- Check the activation log for the infrastructure service and legacy console
- Check the license status in the web console

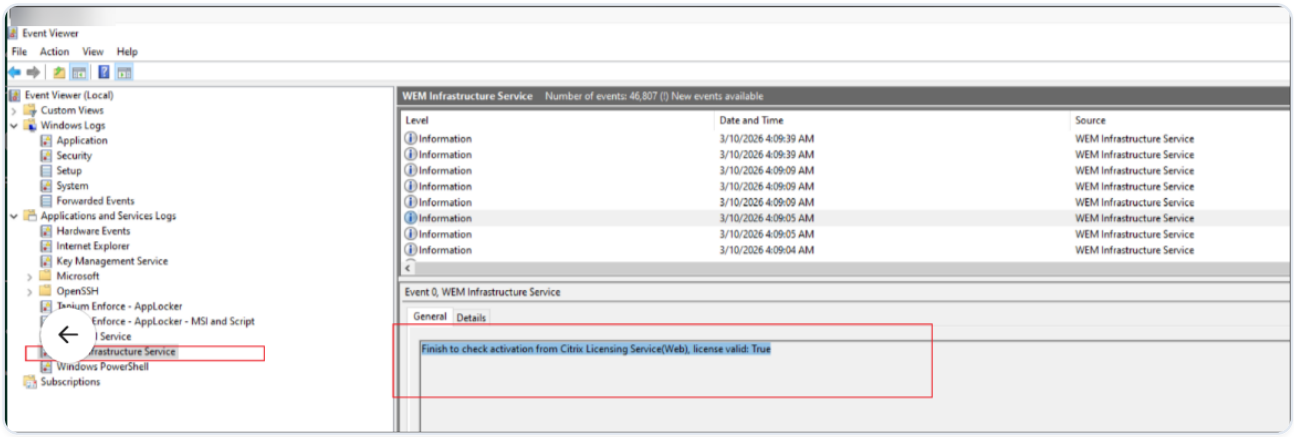
Verify LAS for the infrastructure service and legacy console

To verify that WEM is using LAS, check for the following log entry in **Event Viewer** or in the **Citrix WEM Infrastructure Service Debug.log**. To enable the log file, see View log files.

```
Finish to check activation from Citrix Licensing Service (Web), license
valid: True
```

If this log entry is present, WEM has been successfully activated using LAS.

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



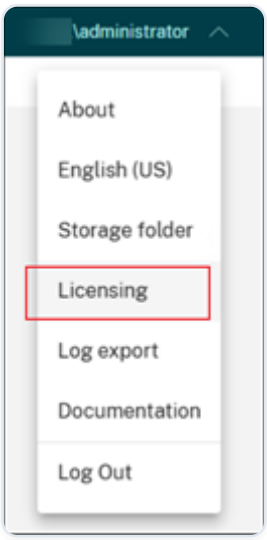
NOTE:

WEM switches to the legacy V6 license if LAS fails. In that case, the log entry includes `Citrix Licensing Service (Legacy)` instead.

Check license server information in the web console

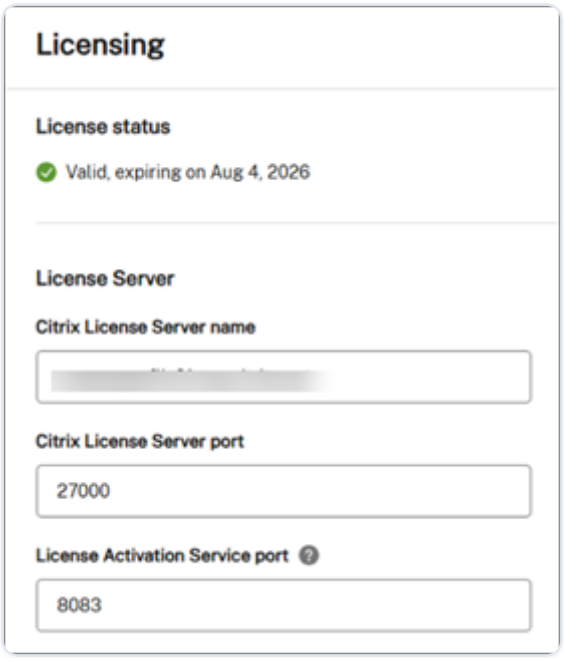
You can check the current license server information in the web console:

1. Click your name in the upper-right corner, and then select **Licensing**. A dialog box displays the current license information.



2. Check the license status and reconfigure the license server information if needed.

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



Troubleshoot license issues

If license configuration fails, or the certificate acceptance dialog box does not appear, see Troubleshoot WEM LAS issues for guidance on certificate errors, hostname mismatches, and connectivity checks.

Agent

Install and configure the agent

NOTE:

- Do not install the Workspace Environment Management™ (WEM) agent on the infrastructure server.
- Do not install the WEM agent and administration console on the same machine.
- If you intend to assign resources published in Citrix StoreFront stores as application shortcuts in WEM from the administration console, ensure that Citrix Workspace app for Windows is installed on the administration console and the agent host machines. For more information, see System requirements.

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

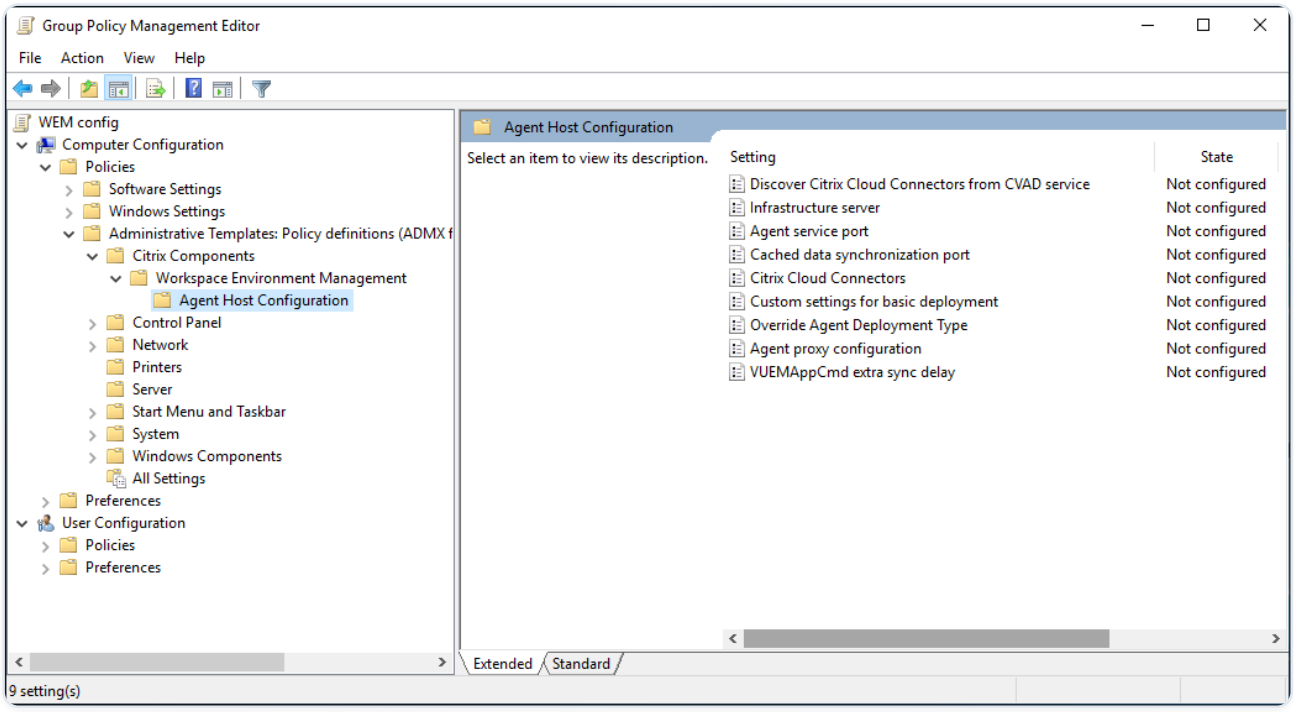
Step 1: Configure group policies (optional)

Optionally, you can choose to configure the group policies for the agent using the **Agent Group Policies** administrative template. The WEM installation package contains this template. The template files are divided into .admx files and language-specific .adml files. We recommend that you configure the group policies on the domain controller.

To add the Agent Host Configuration policy, complete these steps:

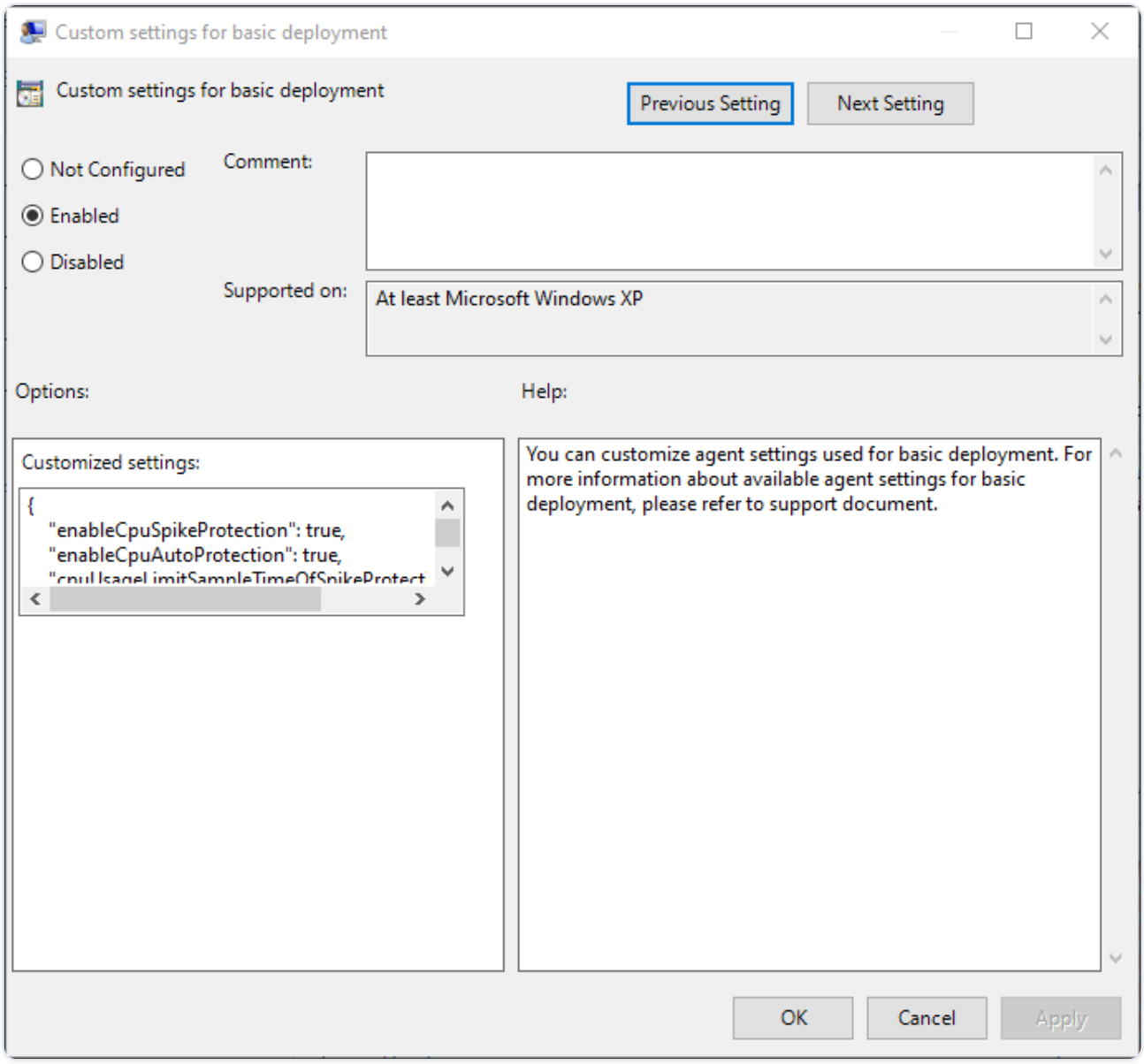
1. Copy the **Agent Group Policies** folder provided with the WEM installation package to your WEM domain controller.
2. Add the .admx files.
    a. Go to the **Agent Group Policies > ADMX** folder.
    b. Copy the two files (*Citrix Workspace Environment Management Agent Host Configuration.admx* and *CitrixBase.admx*).
    c. Go to the `<C:\Windows>\PolicyDefinitions` folder and then paste the files.
3. Add the .adml files.
    a. Go to the **Agent Group Policies > ADMX > en-US** folder.
    b. Copy the two files (*Citrix Workspace Environment Management Agent Host Configuration.adml* and *CitrixBase.adml*).
    c. Go to the `<C:\Windows>\PolicyDefinitions\en-US` folder and then paste the files.
4. In the **Group Policy Management Editor** window, go to **Computer Configuration > Policies > Administrative Templates > Citrix Components > Workspace Environment Management > Agent Host Configuration** and configure the following settings::

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



Custom settings for basic deployment. Customized agent settings used for deployment. For more information about available agent settings for basic deployment, see Manage Basic Deployment-agents.

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



Override Agent Deployment Type. Overrides the WEM agent deployment type. Choose one of the following options:

- **Cloud service deployment:** Connects the agent to the WEM service in Citrix Cloud, providing full WEM capabilities.
- **On-premises deployment:** Connects the agent to an on-premises WEM deployment, providing full WEM capabilities.
- **Basic deployment:** Runs the agent in a single-machine mode with limited functionality, without connecting to a WEM infrastructure.
- **Disabled:** Disables all WEM functions on the machine where the agent is installed.

Discover Citrix Cloud Connector™ from CVAD service. Not applicable to the on-premises versions of WEM. Leave the state Not Configured.

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

Infrastructure server. The address of the WEM infrastructure server. Type the name or IP address of the machine where the infrastructure service is installed.

Agent service port. The port on which the agent connects to the infrastructure server. The agent service port must be the same as the port you configured for the agent service port during the infrastructure services configuration. If unspecified, the port defaults to 8286.

Cached data synchronization port. (Applicable to Workspace Environment Management 1912 and later; replaces *Cache synchronization port* of Workspace Environment Management 1909 and earlier.) The port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server. The cached data synchronization port must be the same as the port you configured for the cached data synchronization port (**WEM Infrastructure Service Configuration > Network Settings**) during the infrastructure services configuration. The port defaults to 8288 and corresponds to the `CachedDataSyncPort` command-line argument. Alternatively, you can specify the port using a command-line option in the silent installation of the WEM agent. For example:

- `citrix_wem_agent_bundle.exe /quiet CachedDataSyncPort=9000`

Citrix Cloud™ Connectors. Not applicable to the on-premises versions of WEM. Leave the state **Not Configured**.

Agent proxy configuration. Not applicable to the on-premises versions of WEM. Leave the state **Not Configured**.

VUEMAppCmd extra sync delay. Specifies, in milliseconds, how long the agent application launcher (VUEMAppCmd.exe) waits before Citrix Virtual Apps and Desktops published resources are started. This ensures that the necessary agent work completes first. The recommended value is 100 through 200. The default value is 0.

Step 2: Install the agent

IMPORTANT:

Although the .NET Framework can be automatically installed during agent installation, we recommend that you install it manually before you install the agent. Otherwise, you need to restart your machine to continue with the agent installation, and it might take a long time to complete.

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

You can run **Citrix Workspace™ Environment Management Agent** in your user environment. You can also choose to install the agent using the command line. By default, the agent installs into one of the following folders, depending on your operating system:

- C:\Program Files (x86)\Citrix\Workspace Environment Management Agent (on 64-bit OS)
- C:\Program Files\ Citrix\Workspace Environment Management Agent (on 32-bit OS)

To install the agent interactively, complete these steps:

1. Run **Citrix Workspace Environment Management Agent.exe** on your machine.
2. Select **I agree to the license terms and conditions** and then click **Install**.
3. On the Welcome page, click **Next**.

   NOTE:

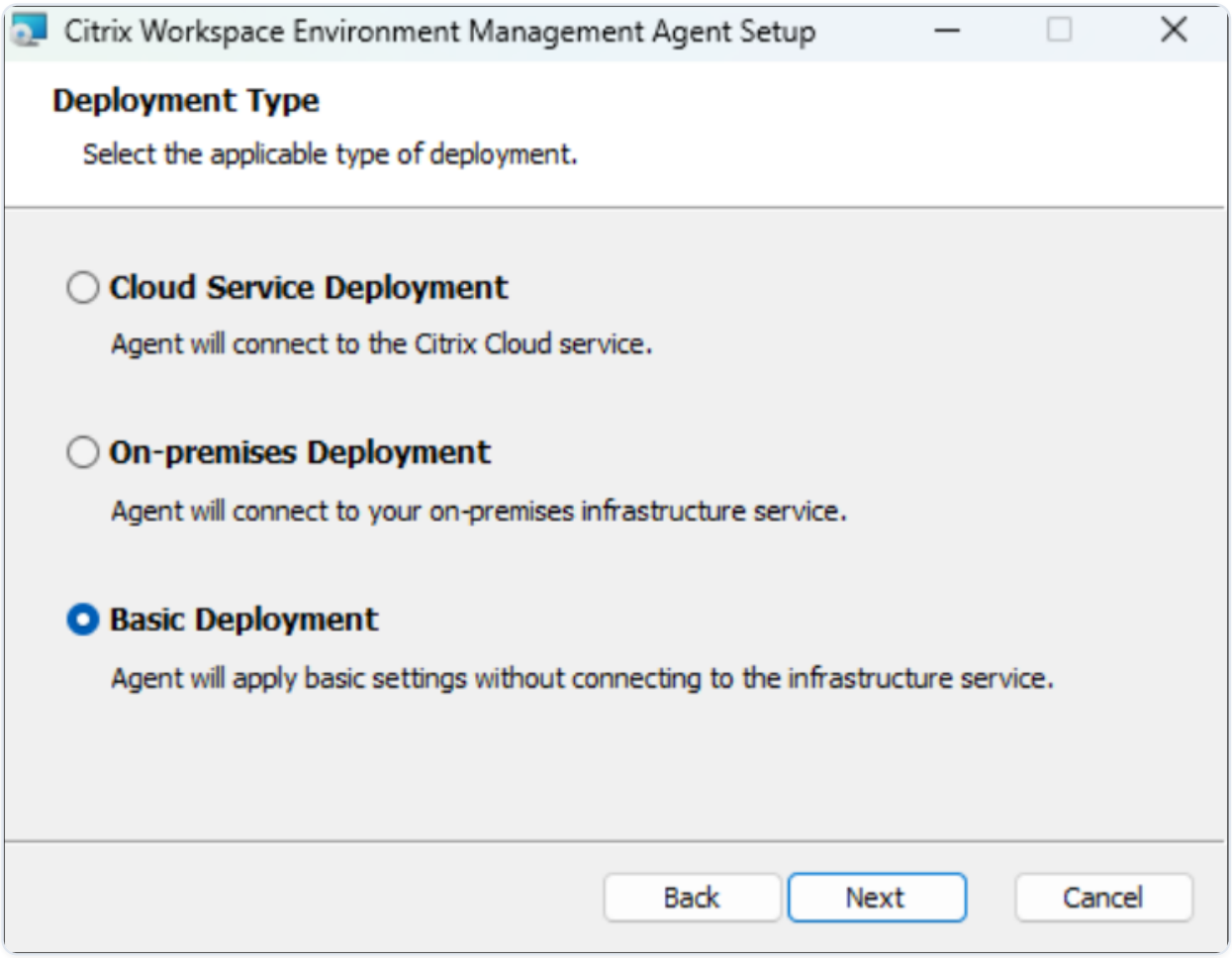
   The Welcome page can take some time to appear. This delay happens when the required software is missing and is being installed in the background.

4. On the Destination Folder page, click **Next**.

   - By default, the destination folder field is automatically populated with the default folder path. If you want to install the agent to another folder, click **Change** to navigate to the folder and then click **Next**.
   - If you already installed the WEM agent, the destination folder field automatically populates with the existing installation folder path.

5. On the Deployment Type page, select the applicable type of deployment and then click **Next**. In this case, select **On-premises Deployment**.
6. You can also select the **Basic Deployment** type. When you select **Basic Deployment** type, the agent turns on the default optimization settings without connecting to the infrastructure service.

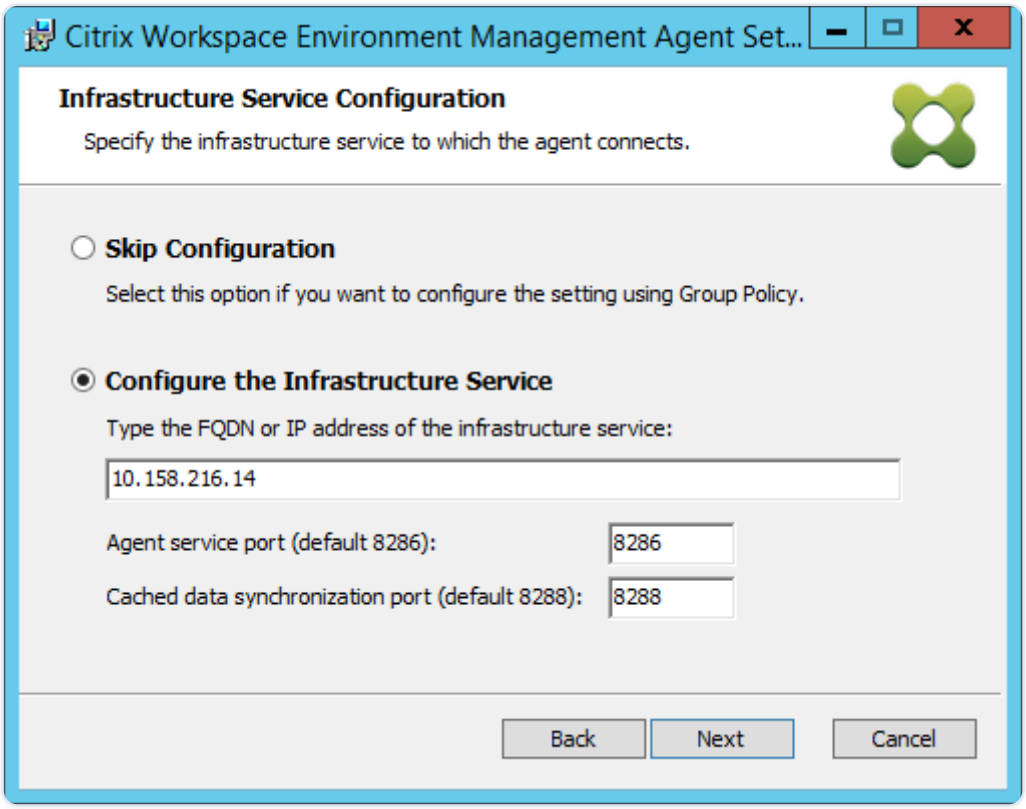
© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. On the Infrastructure Service Configuration page, specify the infrastructure service to which the agent connects and then click **Next**.

   - **Skip Configuration**. Select this option if you have already configured the setting using Group Policy.
   - **Configure the Infrastructure Service**. Lets you configure the infrastructure service by typing the FQDN or IP address of the infrastructure service.
   - **Agent service port**. By default, the value is 8286.
   - **Cached data synchronization port**. By default, the value is 8288.

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



8. On the Advanced Settings page, configure advanced settings for the agent and then click **Next**.

   - **Alternative Cache Location (Optional)**. Lets you specify an alternative location for the agent cache. Click **Browse** to navigate to the applicable folder. Alternatively, you can do that through the registry. To do that, first stop the Citrix WEM Agent Host Service and then modify the following registry key.

     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Agent Host

     Name: AgentCacheAlternateLocation

     Type: REG_SZ

     Value: Empty

     By default, the value is empty. The default folder is: `<WEM agent installation folder path>\Local Databases Set`. Specify a different folder path if necessary. For the changes to take effect, restart the Citrix WEM Agent Host Service. If the change takes effect, the following files appear in the folder: **LocalAgentCache.db** and **LocalAgentDatabase.db**.

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

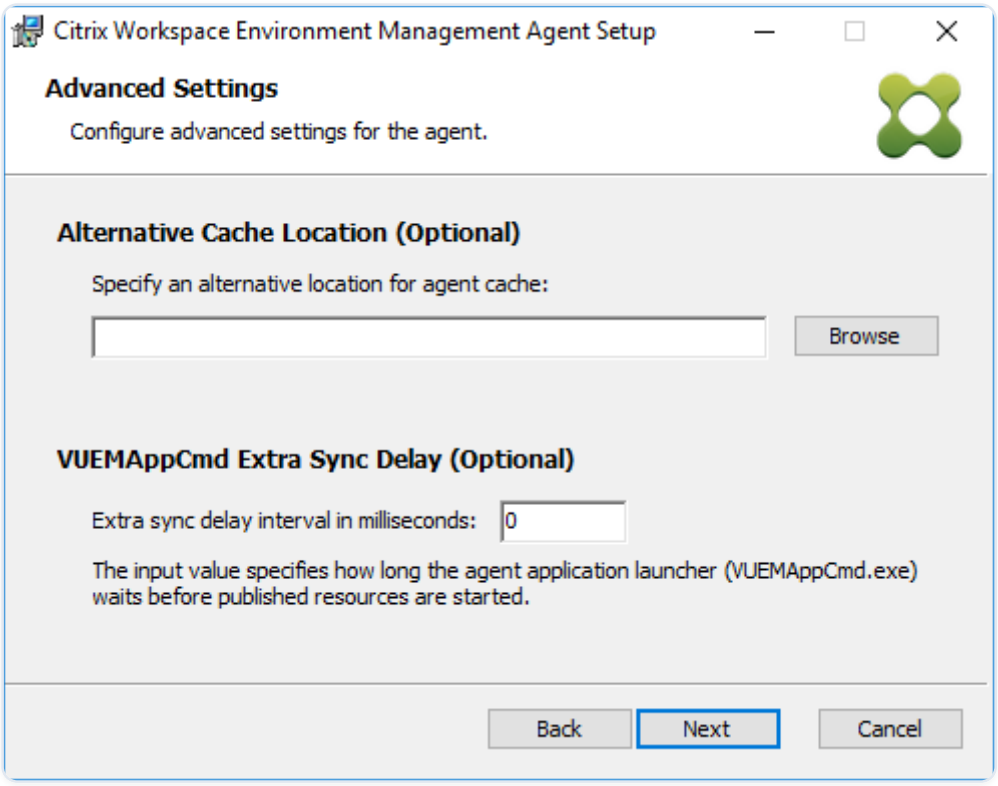
CAUTION:

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.

- **VUEMAppCmd Extra Sync Delay (Optional)**. Lets you specify how long the agent application launcher (VUEMAppCmd.exe) waits before published resources start. Setting this delay ensures that the necessary agent work completes first. The default value is 0.

NOTE:

The value you type for the extra sync delay interval must be an integer greater than or equal to zero.



9. On the Ready to install page, click **Install**.
10. Click **Finish** to exit the installalltion wizard.

Alternatively, you can choose a silent installation of the WEM agent. To do so, use the following command line:

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

- `"Citrix Workspace Environment Management Agent.exe" /quiet Cloud=0`

TIP:

- For agents running in an on-premises WEM deployment, enter `Cloud=0`. For agents running in a WEM service deployment, enter `Cloud=1`.
- You might want to consult the log files to troubleshoot the agent installation. By default, log files recording all actions that occur during installation are created in %TEMP%. You can use the `/log log.txt` command to designate a specific location for the log files to be saved.

You can also use command-line options to specify custom arguments. Doing so lets you customize the agent and system settings during the installation process. For more information, see Good to know.

After installation, the agent runs as *Citrix WEM Agent Host Service* (formerly Norskale Agent Host Service) and *Citrix WEM Agent User Logon Service*. The agent runs as account *LocalSystem*. We do not support changing this account. The service requires the **log on as a local system** permission.

Step 3: Restart the machine to complete the installation

Prerequisites and recommendations

To ensure that the WEM agent works properly, be aware of the following prerequisites and recommendations:

Prerequisites

Verify that the following requirements are met:

- The Windows service **System Event Notification Service** is configured to start automatically on startup.
- The WEM agent services **Citrix WEM Agent Host Service** and **Citrix WEM User Logon Service** are configured to start automatically on startup.
- The agent cache resides in a persistent location whenever possible. Using a non-persistent cache location can cause potential cache sync issues, excessive network data usage, performance issues, and so on.

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

Recommendations

Follow the recommendations in this section for a successful agent deployment:

- Do not manually operate **Citrix WEM Agent Host Service**, for example, using logon or startup scripts. Operations such as stopping or restarting **Citrix WEM Agent Host Service** can stop the Netlogon service from working, causing issues with other applications.
- Do not use logon scripts to launch UI-mode or CMD-mode agents. Otherwise, some functionalities might fail to work.

Agent startup behaviors

- **Citrix WEM Agent Host Service** automatically reloads Cloud Connector settings configured through Group Policy after the service starts.
- **Citrix WEM Agent User Logon Service** automatically starts **Citrix WEM Agent Host Service** if the agent host service does not start during the first logon. This behavior ensures that user configuration is processed properly.
- **Citrix WEM Agent Host Service** automatically performs checks on the following local database files on startup: `LocalAgentCache.db` and `LocalAgentDatabase.db`. If the virtual machine is provisioned and the local database files are from the base image, the database files are automatically purged.
- When **Citrix WEM Agent Host Service** starts, it automatically verifies that the agent local cache has been recently updated. If the cache has not been updated for more than two configured cache synchronization time intervals, the cache is synchronized immediately. For example, suppose the default agent cache sync interval is 30 minutes. If the cache was not updated in the past 60 minutes, it is synchronized immediately after **Citrix WEM Agent Host Service** starts.
- During installation, the WEM agent installer configures the Windows service **System Event Notification Service** to start automatically.
- The WEM agent installer automatically starts the Netlogon service after the WEM agent upgrade completes.

Agent cache utility options

Citrix WEM Agent Host Service handles setting refresh and cache sync automatically. Use the agent cache utility only in scenarios where there is a need to immediately refresh the settings and synchronize the cache.

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

Use the command line to run *AgentCacheUtility.exe* in the agent installation folder. The executable accepts the following command-line arguments:

- `-help`: Displays a list of allowed arguments.
- `-RefreshCache` or `-r`: Triggers a cache build or refresh.
- `-RefreshSettings` or `-S`: Refreshes agent host settings.
- `-Reinitialize` or `-I`: Reinitializes the agent cache when used together with the `-RefreshCache` option.

See the following examples for details about how to use the command line:

- Refresh agent host settings:
  - `AgentCacheUtility.exe -RefreshSettings`
- Refresh agent host settings and agent cache simultaneously:
  - `AgentCacheUtility.exe -RefreshSettings -RefreshCache`
- Reinitialize the agent cache:
  - `AgentCacheUtility.exe -RefreshCache -Reinitialize`

Good to know

The agent executable accepts custom arguments as described in the Agent settings and the System settings sections.

Agent settings

The WEM agent settings include:

- **AgentLocation**. Lets you specify the agent installation location. Specify a valid folder path.
- **AgentCacheLocation**. Lets you specify an alternative location for the agent cache. If configured, the agent local cache file is saved in the designated location instead of in the agent installation folder.
- **AgentCacheSyncPort**. Lets you specify the port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server.
- **AgentServicePort**. Lets you specify the port on which the agent connects to the infrastructure server.

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

- **InfrastructureServer**. Lets you specify the FQDN or IP address of the infrastructure server where the infrastructure service is running.
- **VUEMAppCmdDelay**. Lets you specify how long the agent application launcher (VUEMAppCmd.exe) waits before the Citrix Virtual Apps and Desktops published resources start. The default value is 0 (milliseconds). The value you type for the extra sync delay interval must be an integer greater than or equal to zero.

Be aware of the following:

- If you configure the settings through the command line, the WEM agent installer uses the configured settings.
- If you don't configure the settings through the command line and there are previously configured settings, the installer uses the settings that were previously configured.
- If you don't configure the settings through the command line and there are no previously configured settings, the installer uses the default settings.

System settings

The system settings associated with the agent host machine include:

- **GpNetworkStartTimeoutPolicyValue**. Lets you configure the value, in seconds, of the GpNetworkStartTimeoutPolicyValue registry key created during installation. This argument specifies how long Group Policy waits for network availability notifications during policy processing on logon. The argument accepts any whole number in the range of 1 (minimum) to 600 (maximum). By default, this value is 120.
- **SyncForegroundPolicy**. Lets you configure the SyncForegroundPolicy registry value during agent installation. This policy setting determines whether Group Policy processing is synchronous. Accepted values: 0, 1. If the value is not set or you set the value to 0, Citrix WEM Agent User Logon Service does not delay logons, and user Group Policy settings are processed in the background. If you set the value to 1, Citrix WEM Agent User Logon Service delays logons until the processing of user Group Policy settings completes. By default, the value does not change during installation.

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

> **IMPORTANT:**
>
> If Group Policy settings are processed in the background, Windows Shell (Windows Explorer) might start before all policy settings are processed. Therefore, some settings might not take effect the first time a user logs on. If you want all policy settings to be processed the first time a user logs on, set the value to 1.

- **WaitForNetwork**. Lets you configure the value, in seconds, of the **WaitForNetwork** registry key created during installation. This argument specifies how long the agent host waits for the network to be completely initialized and available. The argument accepts any whole number in the range of 0 (minimum) to 300 (maximum). By default, this value is 30.

The previous three keys ensure that the WEM agent service starts before the Windows logon screen appears. All three keys are created under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** during installation. The keys also ensure that the user environment receives the infrastructure server address GPOs before logon. In network environments where the Active Directory or Domain Controller servers are slow to respond, extra processing time before the logon screen appears might result. We recommend that you set the value of the **GpNetworkStartTimeoutPolicyValue** key to a minimum of 30 for it to have an impact.

- **ServicesPipeTimeout**. Lets you configure the value of the ServicesPipeTimeout registry key. The key is created during installation under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control**. This registry key adds a delay before the service control manager is allowed to report on the state of the WEM agent service. The delay prevents the agent from failing by keeping the agent service from launching before the network is initialized. This argument accepts any value, in milliseconds. If not specified, a default value of 60000 (60 seconds) is used.

> **NOTE:**
>
> If you don't configure the preceding settings using the command line, the WEM agent installer does not process them during installation.

Examples

You can configure the settings using the following command-line format:

- `"Citrix Workspace Environment Management Agent.exe" <key=value>`

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

For example:

- Choose a silent installation or upgrade of the WEM agent
  - `"Citrix Workspace Environment Management Agent.exe" /quiet Cloud=0`
- Set user logon network wait time to 60 seconds
  - `"Citrix Workspace Environment Management Agent.exe" WaitForNetwork=60`

Scale and size considerations for deployments

Workspace Environment Management™ (WEM) is designed for large-scale enterprise deployments. When evaluating WEM for sizing and scalability, you need to consider database performance, Active Directory setup, firewall rules, and more.

WEM scalability is based on the number of agents and users. The more infrastructure servers available, the more agents and users WEM can support. The infrastructure servers synchronize various back-end components (SQL Server and Active Directory) with front-end components (administration console and agent).

Suppose that the machine where the infrastructure server is running uses the following specification:

- 4 vCPUs, 8 GB RAM, and 80 GB of available disk space.

You can use the following formula to calculate the number of the infrastructure servers required for your deployment. The formula is developed based on statistics related to certain customers:

- Number of infrastructure servers = (number of agents/1,000) + (number of users/3,000)

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

NOTE:

- In scenarios with NTLM authentication, certain performance issues have been observed with Workspace Environment Management 2006 and earlier. Those issues have not been observed when Kerberos authentication is used.
- No performance differences between NTLM authentication and Kerberos authentication have been observed with Workspace Environment Management 2006 and later.
- Starting with WEM 2212, agents download configuration data only when needed. This enhancement can reduce bandwidth consumption and the load on infrastructure services by up to 50%. See What's new. We recommend that you upgrade your agents to 2212 or later so that you can reap the benefit.

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

Upgrade a deployment

Introduction

NOTE:

Starting with WEM 2212, agents download configuration data only when needed. This enhancement can reduce bandwidth consumption and the load on infrastructure services by up to 50%. See What's new. We recommend that you upgrade your agents to 2212 or later so that you can reap the benefit.

You can upgrade Workspace Environment Management™ (WEM) deployments to newer versions without having to first set up new machines or sites. This is called an in-place upgrade.

In-place upgrades from versions earlier than Workspace Environment Management 4.7 to version 1808 or later are not supported. To upgrade from any of those earlier versions, you need to upgrade to version 4.7 first and then upgrade to the target version. For details, see this table:

FROM	TO	IN-PLACE UPGRADE SUPPORTED
4.6 and earlier	4.7	Yes
4.6 and earlier	1808 or later	No (upgrade to version 4.7 before upgrading to the target version)
4.7	1808 or later	Yes

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

NOTE:

- The WEM database, infrastructure service, and administration console must all be of the same version.
- Keep the following in mind when you plan to upgrade a WEM deployment earlier than 2006 to 2209 or later: To avoid database upgrade failures, upgrade to 2103 first and then to 2209 or later.

The Workspace Environment Management components must be upgraded in the following order:

1. Upgrade the infrastructure services
2. Upgrade the database
3. Reconfigure the infrastructure services
4. Upgrade Administration console
5. Upgrade and reconfigure the web console service
6. Upgrade the Agent

Step 1: Upgrade the infrastructure services

To upgrade the Workspace Environment Management infrastructure services, run the new Workspace Environment Management infrastructure services setup on your infrastructure server. The upgrade procedure is otherwise identical to the installation procedure.

Upgrade the operating system of an infrastructure server

To upgrade the operating system of an infrastructure server, first install the infrastructure service on a different machine with the new operating system, manually configure it with identical infrastructure service settings, and then disconnect the "old" infrastructure server.

NOTE:

After you upgrade to Windows Server 2022, the WEM infrastructure service might fail to respond. As a workaround, reinstall the infrastructure service and configure it to connect to the WEM database.

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

Step 2: Upgrade the database

IMPORTANT:

The database upgrade process is not reversible. Ensure that you have a valid database backup before launching the upgrade process.

Tip:

You can also upgrade the database using the Workspace Environment Management PowerShell SDK module. For SDK documentation, see Citrix Developer Documentation.

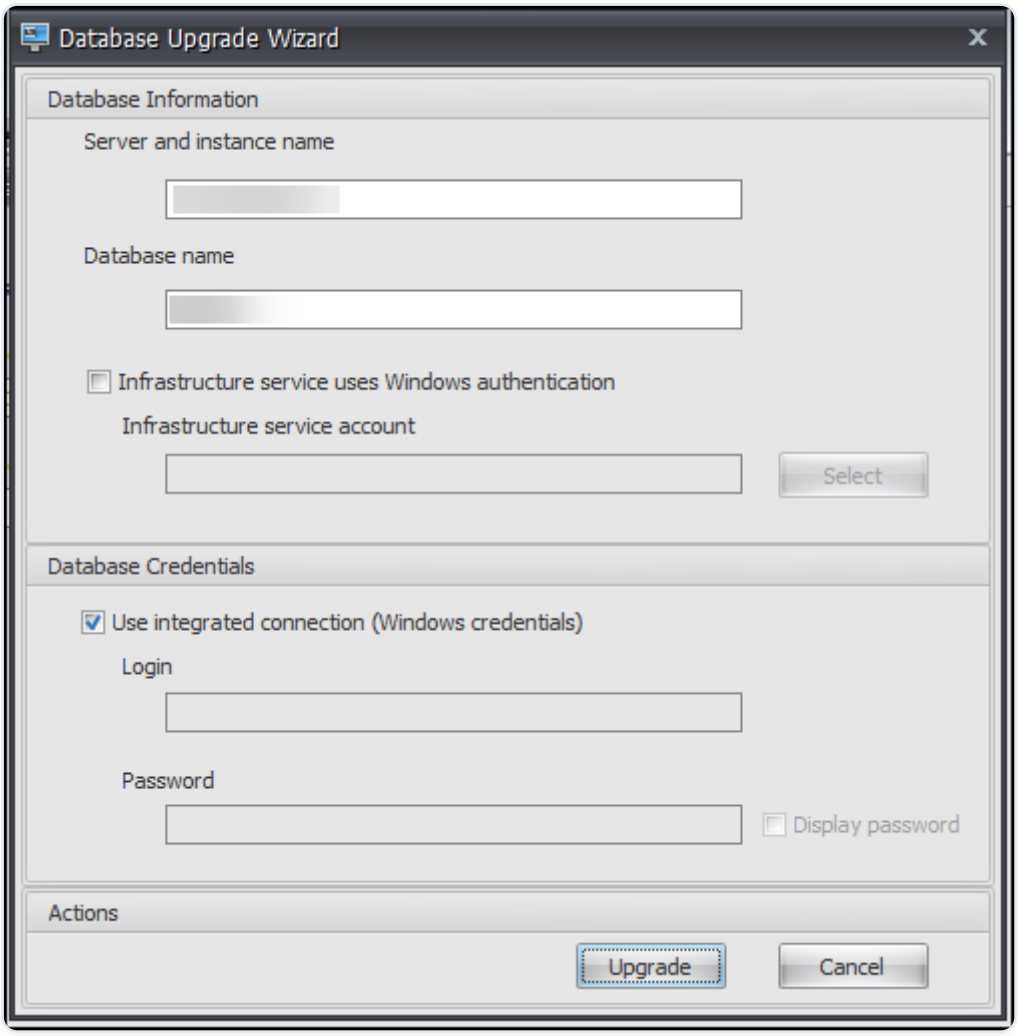
Use the **WEM Database Management Utility** to update the database. This is installed on your Workspace Environment Management infrastructure server during the infrastructure services installation process.

NOTE:

If you are using Windows authentication for your SQL Server, run the database upgrade utility under an identity that has sysadmin permissions.

1. From the **Start** menu, select **Citrix®>Workspace Environment Management > WEM Database Management Utility**.
2. Click **Upgrade Database**.
3. In the database upgrade wizard, type the required information.

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



- **Server and instance name**. Address of the SQL Server\\instance on which the database is hosted. It must be reachable exactly as entered from the infrastructure server.
- **Database name**. Name of the database to be upgraded.
- **Infrastructure service uses Windows authentication**. By default, this option is not selected. In this case, the infrastructure service connects to the database using the vuemUser SQL user account. (The vuemUser SQL user account is created during the installation process.) Verify that Mixed-Mode Authentication is enabled for the SQL instance.

  When selected, the infrastructure service connects to the database using a Windows account. In this case, the Windows account you select must not already have a login on the SQL instance. In other words, do not use the same Windows account that you used to create the database to run the infrastructure service.

  To select a gMSA, follow the same steps as selecting an AD user. Ensure that the gMSA has the **db-owner** role membership for the database.

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

- **Use integrated connection**. By default, this option is selected. The option lets the wizard use the Windows account of the identity under which the wizard is running to connect to SQL Server and to create the database. If this Windows account does not have sufficient permissions to create the database, run the database management utility as a Windows account with sufficient privileges, or clear this option and type a SQL account with sufficient privileges instead.

4. Click **Upgrade** to start the database upgrade process. After the database upgrade completes successfully, exit the wizard.

If errors occur during the database upgrade, check the **VUEM Database Management Utility Log** file available in your Workspace Environment Management infrastructure services installation folder.

Step 3: Reconfigure the infrastructure services

Reconfigure the Infrastructure Services using the WEM Infrastructure Service Configuration utility. See Configure the infrastructure service.

Step 4: Upgrade the administration console

NOTE:

All Workspace Environment Management settings configured with the Administration Console are stored in the database and are preserved during upgrade.

To upgrade the administration console, run the administration console setup executable. The procedure is otherwise identical to the installation procedure.

Step 5: Upgrade and reconfigure the web console service

1. Upgrade the web console service by running its setup executable. The procedure is otherwise identical to the installation procedure.
2. Reconfigure the web console service by running the WEM web console service configuration utility.

For more information, see Install and configure the web console service.

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

Step 6: Upgrade the agent

IMPORTANT:

- Before upgrading an agent, make sure that no users are logged in. This ensures that the upgrade process can modify the files on that machine.
- The version of the WEM infrastructure service must be equal to or greater than the version of the WEM agent. Citrix recommends that you upgrade the agent to the latest version so that you can use the most recent features.

To upgrade the agent, run the new agent setup executable on the target machine.

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

Home page

This page provides an overview of your Workspace Environment Management™ (WEM) deployment along with information necessary for you to get to know and get started with WEM quickly. The interface comprises the following four parts:

- **Overview**
- **Quick access**
- **Highlights**
- **Preview features**

Overview

Provides an overview of your WEM deployments, which includes the following information:

- a count of total agents for all configuration sets
- the number of agent machines users have recently logged on to
- VDA health status

To view agents in detail, click **View agent statistics** to go to **Monitoring > Administration > Agents**, where you can view agent information and perform administrative tasks such as refreshing the cache, customizing settings, and retrieving agent information. For more information, see WEM agents.

To view VDA health status in detail, click **View** under **Normal** to see reports about VDAs in normal state or click **View** under **Unusual** to see reports about VDAs in unusual state. For more information, see Reports.

Quick access

Provides quick access to a subset of the key features that WEM offers. The following features are available in the web console:

- **Optimize resource utilization**. Lets you reduce user logon times and make applications more responsive.

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

- **Gain insights**. Lets you gain insights into profile container and application behavior.
- **Configure scripted tasks**. Lets you customize scripted tasks to suit your unique environment management needs.

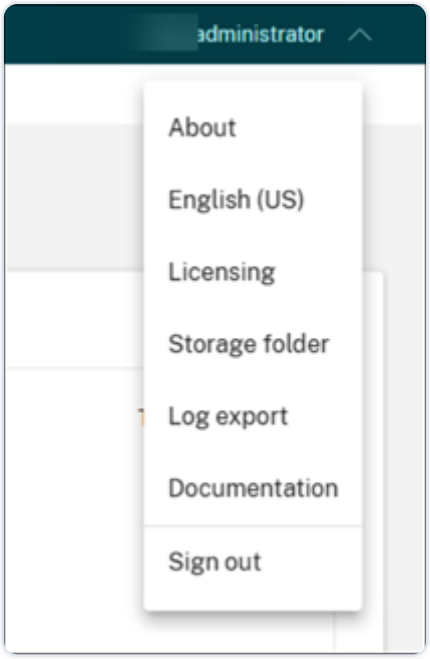
> **TIP:**
>
> When you click the quick access link, a window appears, prompting you to select the applicable configuration set. You are then directly taken to the feature page within the configuration set.

The following features are available in the legacy console:

- **Optimize profile management**. Lets you provide a unified experience across all user desktops.
- **Assign group policies**. Lets you assign Group Policy Objects to different Active Directory groups, just like you assign other actions.
- **Enforce enterprise security**. Lets you protect desktops by applying additional AppLocker rules.

Global configurations

Global configuration is a drop-down list located at the top right corner of the web console.



The functionalities and their descriptions are listed as follows:

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

- **About**. Lets you see the versions and the copyright of WEM.
- **English (US)**. Lets you switch the language.
- **Storage Folder**. To define a global storage folder, to use Template based GPO, Scripted task, Backup and restore, and files, you must set up a shared storage folder.
- **Licensing**. Lets you view or configure the Citrix License Server connection details.
- **Log export**. Lets you export your infrastructure service and web console logs to third-party platforms like Grafana and Splunk.

  To enable it, click **Create Destination**, enter the required information for the log platform. For example, URL, user name, and key. Then click **Done**.
- **Documentation**. Lets you view the documentation of WEM.
- **Sign out**. Lets you sign out the current account.

Highlights

Shows the key features that WEM offers. The following features are available in the web console:

- CPU management
- Scripted tasks

The following features are available in the legacy console:

- Privilege elevation
- External tasks

Preview features

Shows features that are currently in preview. To see preview features, click the preview features icon in the upper-right corner of the console. A red dot appears each time new preview features are available. You see the following tooltip when there are no preview features to show: `No preview features to show at the moment`.

Preview features might not be fully localized and are recommended for use in non-production environments. Issues found with preview features are not supported by Citrix Technical Support.

After you enable or disable preview features, refresh your browser window for the change to take effect.

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

Home page

This page provides an overview of your Workspace Environment Management™ (WEM) deployment along with information necessary for you to get to know and get started with WEM quickly. The interface comprises the following four parts:

- **Overview**
- **Quick access**
- **Highlights**
- **Preview features**

Overview

Provides an overview of your WEM deployments, which includes the following information:

- a count of total agents for all configuration sets
- the number of agent machines users have recently logged on to
- VDA health status

To view agents in detail, click **View agent statistics** to go to **Monitoring > Administration > Agents**, where you can view agent information and perform administrative tasks such as refreshing the cache, customizing settings, and retrieving agent information. For more information, see WEM agents.

To view VDA health status in detail, click **View** under **Normal** to see reports about VDAs in normal state or click **View** under **Unusual** to see reports about VDAs in unusual state. For more information, see Reports.

Quick access

Provides quick access to a subset of the key features that WEM offers. The following features are available in the web console:

- **Optimize resource utilization**. Lets you reduce user logon times and make applications more responsive.
- **Gain insights**. Lets you gain insights into profile container and application behavior.
- **Configure scripted tasks**. Lets you customize scripted tasks to suit your unique environment management needs.

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

TIP:

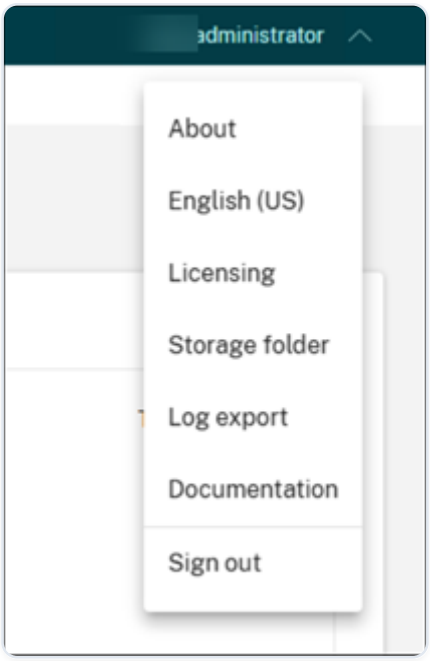
When you click the quick access link, a window appears, prompting you to select the applicable configuration set. You are then directly taken to the feature page within the configuration set.

The following features are available in the legacy console:

- **Optimize profile management**. Lets you provide a unified experience across all user desktops.
- **Assign group policies**. Lets you assign Group Policy Objects to different Active Directory groups, just like you assign other actions.
- **Enforce enterprise security**. Lets you protect desktops by applying additional AppLocker rules.

Global configurations

Global configuration is a drop-down list located at the top right corner of the web console.



The functionalities and their descriptions are listed as follows:

- **About**. Lets you see the versions and the copyright of WEM.
- **English (US)**. Lets you switch the language.
- **Storage Folder**. To define a global storage folder, to use Template based GPO, Scripted task, Backup and restore, and files, you must set up a shared storage folder.

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

- **Licensing**. Lets you view or configure the Citrix License Server connection details.
- **Log export**. Lets you export your infrastructure service and web console logs to third-party platforms like Grafana and Splunk.

  To enable it, click **Create Destination**, enter the required information for the log platform. For example, URL, user name, and key. Then click **Done**.
- **Documentation**. Lets you view the documentation of WEM.
- **Sign out**. Lets you sign out the current account.

Highlights

Shows the key features that WEM offers. The following features are available in the web console:

- CPU management
- Scripted tasks

The following features are available in the legacy console:

- Privilege elevation
- External tasks

Preview features

Shows features that are currently in preview. To see preview features, click the preview features icon in the upper-right corner of the console. A red dot appears each time new preview features are available. You see the following tooltip when there are no preview features to show: `No preview features to show at the moment`.

Preview features might not be fully localized and are recommended for use in non-production environments. Issues found with preview features are not supported by Citrix Technical Support.

After you enable or disable preview features, refresh your browser window for the change to take effect.

Configuration Sets

This page lets you manage your configuration sets. A configuration set is a logical container used to organize a set of Workspace Environment Management™ (WEM) configurations. You can perform the following operations:

- Add a configuration set

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

- Edit or delete a configuration set
- Add configuration sets to favorites
- Configure settings for a configuration set
- Save a backup copy of your current configuration
- Revert to a previously backed up version of your WEM service configuration
- Search for a configuration set using the search box
- Refresh the configurtion list

There are two built-in configuration sets:

- **Default Site**. A built-in WEM configuration set.
- **Unbound Agents**. A built-in WEM configuration set. Available for use only with agents that are not bound to any configuration set. To apply the settings of this configuration set to those agents, go to **Directory Objects > Advanced settings**.

NOTE:

- For **Default Site**, you cannot delete it. You can change its name and description if necessary.
- For **Unbound Agents**, you cannot delete or edit it. The **Edit configuration set** option is unavailable.

Add a configuration set

You create a configuration set to apply settings to directory objects (users, machines, groups, and OUs). To do so, perform the following steps:

1. On the **Configuration sets** node, click **Add configuration set**.
2. Enter a name for the configuration set.
3. Enter a description to help identify the configuration set.
4. Click **Save**.

Edit or delete a configuration set

To edit or delete a configuration set, perform the following steps:

1. On the **Configuration sets** node, locate the configuration set.

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

2. Click the configuration set. The details view of the configuration set appears.
3. In the upper right corner, click **Edit configuration set**.
4. Edit the name and description or click **Delete configuration set**.

Add configuration sets to favorites

To add a configuration set to favorites, perform the following steps:

1. On the **Configuration sets** node, locate the configuration set.
2. Click the configuration set.
3. In the upper right corner, click **Add to favorites**.

NOTE:

- You can favorite up to five configuration sets.
- Favorites are saved on a per-administrator basis.

Configure settings for a configuration set

To configure settings for a configuration set, perform the following steps:

1. On the **Configuration sets** node, locate the configuration set.
2. Click the configuration set.
3. Configure settings as needed.

You can configure the following settings for a configuration set:

- System Optimization
- Advanced Settings
- Scripted Task Settings

Back up and restore

The **Backup and restore** page displays a list of your existing backups. There are two types of backups: automatic backup and manual backup (configuration set and settings). You can differentiate automatic backups from manual backups by the **Content type** column.

For each backup, you can perform the following operations:

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

- **Restore**. Lets you restore a configuration from the backup. Restoring a configuration from a backup replaces all settings related to the selected configuration set with those from the backup.

  NOTE:

  - To restore Profile Management settings to a configuration set, you can also use the quick setup feature on the **Profiles > Profile Management Settings** page under that configuration set.
  - When restoring Profile Management settings from a backup, the SMB shares selected for relevant services to use are also restored.

- **Download.** Lets you save a copy of the backup to your local machine. The backup is saved to the default download location of your browser. The backup file is in JSON format.
- **Delete**. Lets you delete an existing backup.

You can also perform the following operations:

- Click the Refresh icon next to the **Upload** button to refresh the current page
- Upload a configuration file
- Manage automatic backup
- Back up a configuration set
- Back up Profile Management settings

Upload a configuration file

You can upload a JSON file used to revert to a previous backup. A JSON file can contain a configuration set or Profile Management settings.

To upload a file, perform the following steps:

1. Click **Upload**. The **Upload backup file** wizard appears.
2. Click **Browse**, browse to the file you want to upload, select the file, and then click **Open**. You are returned to the **Upload backup file** wizard.
3. Specify a name for your file.
4. Click **Upload** to start the upload.

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

NOTE:

- You can upload only JSON files.
- You can upload only files whose size is smaller than 5 MB.

Manage automatic backup

You can save a backup of a configuration set automatically. The feature supports storing up to 25 backup files for each configuration set before starting to overwrite the oldest existing file. You cannot back up the following items related to a configuration set:

- Directory objects related to machines (single machines, machine groups, and OUs)
- Monitoring data (statistics and reports)
- Process management
- Agents registered with the configuration set

To configure automatic backup, perform the following steps:

1. Click **Manage automatic backup**. The **Manage automatic backup** wizard appears.
2. Locate the configuration set you want to back up automatically.
3. Select one of the following three options for that configuration set.
    - **Not configured**. If selected, WEM does not back up automatically.
    - **Daily**. If selected, WEM performs backups on a daily basis.
    - **Weekly**. If selected, WEM performs backups every Monday.
4. Repeat the steps of locating the configuration set and selecting one of the above three options for other configuration sets if needed.
5. Click **Save** to save your changes and to exit the wizard.

Back up a configuration set

IMPORTANT:

We limit the number of manual backups to 25 per account. If you have reached the limit, delete existing backups and try again.

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

You can save a backup copy of your configuration set and then use the backup for restore purposes. You can back up the following items related to a configuration set:

- Actions
- Application security, privilege elevation, and process hierarchy control
- Assignments (related to actions and action groups)
- Filters
- Scripted task settings
- Users
- WEM settings

You cannot back up the following items related to a configuration set:

- Directory objects related to machines (single machines, machine groups, and OUs)
- Monitoring data (statistics and reports)
- Process management
- Agents registered with the configuration set

To back up a configuration set, perform the following steps:

1. Click **Back up**. The **Back up** wizard appears.
2. Select the target configuration set.
3. Select from the list the configuration set you want to back up.
4. Specify a name for your backup.
5. Optionally, select **Save a copy of the backup to your local machine** to save the backup locally.

   NOTE:

   The backup is saved to the default download location of your browser.

6. Click **Back up** to start the backup.

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

Back up Profile Management settings

IMPORTANT:

We limit the number of manual backups to 25 per account. If you have reached the limit, delete existing backups and try again.

To back up Profile Management settings, perform the following steps:

1. Click **Back up**. The **Back up** wizard appears.
2. Select the target configuration set.
3. Select **Settings** from the **What to back up** list.
4. Select **Profile Management settings**.
5. Specify a name for your backup.
6. Optionally, select **Save a copy of the backup to your local machine** to save the backup locally.

   NOTE:

   The backup is saved to the default download location of your browser.

7. Click **Back up** to start the backup.

Actions

TIP:

- You can use dynamic tokens to extend WEM actions to make them more powerful.
- To paste data copied from Citrix Environment Tool Hub into the web console, ensure that the browser allows data copying. Example: For Microsoft Edge, be sure to have the **Site permissions > Clipboard > Ask when a site wants to see text and images copied to the clipboard** option enabled.

Workspace Environment Management™ (WEM) streamlines the workspace configuration process by providing you with easy-to-use actions. You can use assignments to make actions available to users. WEM also provides you with filters to contextualize your assignments.

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

Group Policy settings

IMPORTANT:

- Workspace Environment Management (WEM) currently supports adding and editing only Group Policy settings associated with the `HKEY_LOCAL_MACHINE` and the `HKEY_CURRENT_USER` registry hives.

Rather than relying on an Active Directory administrator to use the **Group Policy Management** console to manage Group Policy Objects (GPOs), you can deploy GPOs through WEM.

Before you start, add or import your **Group Policy** settings. You then deploy your settings by assigning them to your users in the form of GPOs. You can manage the assignments for each GPO by specifying the targets you want to assign it to.

When the feature is enabled:

- You can configure your settings.
- The WEM agent can process Group Policy settings.

When the feature is disabled:

- You cannot configure Group Policy settings.
- The WEM agent does not process Group Policy settings even if they are already assigned to users or user groups.

NOTE:

For WEM agents to process and apply Group Policy settings properly, verify that Citrix WEM User Logon Service is enabled on them.

Registry-based settings

Use this tab to configure settings for Windows by configuring registry operations.

In **Actions > Group Policy Settings > Registry-based** under a configuration set, you can do the following operations:

- Import registry-based Group Policy settings into WEM.
- Create a GPO

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

- Refresh the GPO list
- View a GPO
- Edit a GPO
- Manage assignments for a GPO
- Clone a GPO
- Delete a GPO

WARNING:

Editing, adding, and deleting registry-based settings incorrectly can prevent the settings from taking effect in the user environment.

IMPORT GROUP POLICY SETTINGS

You can import GPOs from a zip file containing your GPO backups or exported registry files.

When importing settings from registry files, you can convert registry values that you export using the Windows Registry Editor into GPOs for management and assignment. Before you start, be aware of the following:

- When importing settings from a zip file, the file can contain one or more registry files.
- Each .reg file will be converted into a GPO. You can treat each converted GPO as a set of registry settings.
- The name of each converted GPO is generated based on the name of the corresponding .reg file. Example: If the name of the .reg file is `test1.reg`, the name of the converted GPO is `test1`.
- The feature supports converting delete operations associated with registry keys and values that you define in .reg files. For information about deleting registry keys and values by using a .reg file, see `<https://support.microsoft.com/en-us/topic/how-to-add-modify-or-delete-registry-subkeys-and-values-by-using-a-reg-file-9c7f37cf-a5e9-e1cd-c4fa-2a26218a1a23>`.
- Descriptions of converted GPOs are empty.

To import your Group Policy settings, complete the following steps:

1. In the action bar, click **Import**.
2. Select the file type.

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

- **GPO backup file**. Select this option if you want to import settings from GPO backup files. For information on how to back up Group Policy settings, see Back up Group Policy settings.
- **Exported registry file**. Select this option if you want to import settings from registry files you export using the Windows Registry Editor.

3. Click **Browse** to navigate to your zip file.

> **NOTE:**
>
> You can upload only files whose size doesn't exceed 10 MB.

4. Choose whether to overwrite existing GPOs with the same name.
5. Click **Import** to start the import process.

After the import completes successfully, imported GPOs appear on the **Registry-based** tab.

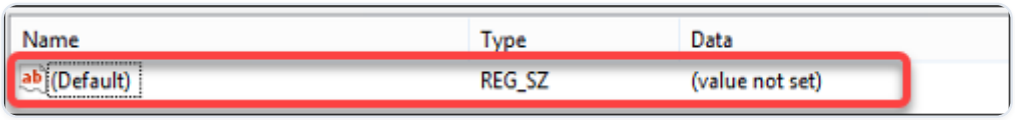
CREATE A GPO

To create a GPO, complete the following steps:

1. In the action bar, click **Create GPO**.
2. Specify a name for the GPO.
3. Optionally, specify additional information to help you identify the GPO.
4. Click **Add** to add registry operations. The following settings become available:
   - **Action**. Lets you specify the type of action for the registry key.
     - **Set value**. Lets you set a value for the registry key.
     - **Delete value**. Lets you delete a value for the registry key.
     - **Create key**. Lets you create the key as specified by the combination of the root key and the subpath.
     - **Delete key**. Lets you delete a key under the registry key.
     - **Delete all values**. Lets you delete all values under the registry key.
   - **Root Key**. Supported values: `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`.
   - **Subpath**. The full path of the registry key without the root key. For example, if `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows` is the full path of the registry key, `Software\Microsoft\Windows` is the subpath.

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

- **Name**. Lets you specify a name for the registry value. The highlighted item in the following diagram as a whole is a registry value. Leaving the **Name** field blank sets it as the default value for that key.



- **Type**. Lets you specify the data type for the value.
  - **REG_SZ**. This type is a standard string used to represent human readable text values.
  - **REG_EXPAND_SZ**. This type is an expandable data string that contains a variable to be replaced when called by an application. For example, for the following value, the string "%SystemRoot%" will be replaced by the actual location of the folder in an operating system.
  - **REG_BINARY**. Binary data in any form.
  - **REG_DWORD**. A 32-bit number. This type is commonly used for Boolean values. For example, *0* means disabled and *1* means enabled.
  - **REG_DWORD_LITTLE_ENDIAN**. A 32-bit number in little-endian format.
  - **REG_QWORD**. A 64-bit number.
  - **REG_QWORD_LITTLE_ENDIAN**. A 64-bit number in little-endian format.
  - **REG_MULTI_SZ**. This type is a multistring used to represent values that contain lists or multiple values. Each entry is separated by a null character.
  - **REG_NONE**. Lets you configure registry values that do not fit into predefined data type categories.
- **Data**. Lets you type data corresponding to the registry value. For different data types, you might need to type different data in different formats.

5. After you finish, click:
   - **Done**. This action completes the GPO creation.
   - **Save and Assign**. This action completes the GPO creation and opens the **Assignment** page, where you can continue to assign the created GPO.

VIEW A GPO

You can view the WEM Group Policy settings and GPO summaries in read-only mode without editing the GPO. This implementation eliminates the risk of misconfiguration while reviewing the existing settings.

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

To view a GPO, complete the following steps:

1. Select the GPO and then click **View** in the action bar.
2. View the name, description, and registry operations.
3. After you finish, click **Close**.

EDIT A GPO

To edit a GPO, complete the following steps:

1. Select the GPO and then click **Edit** in the action bar.
2. Edit the name and description. When you create or update a registry key value, leaving the **Name** field blank sets it as the default value for that key.
3. Do the following as needed:
    - Click **Add** to add a registry operation
    - Select a registry operation and then edit it
    - Select a registry operation and then delete it
    - Move a registry operation down or up. Alternatively, select a registry operation, click the six-dot icon, and then drag it to the desired position.
4. After you finish, click **Done**.

NOTE:

If a GPO is already assigned to users, editing it will impact those users.

MANAGE ASSIGNMENTS FOR A GPO

You can assign a GPO to different AD groups. A group can contain users and machines. Machine-level settings take effect if the related machine belongs to the group. User-level settings take effect if the current user belongs to the group.

TIP:

For machine-level settings to take effect immediately, restart the Citrix WEM Agent Host Service. For user-level settings to take effect immediately, users must log off and log back on.

To manage assignment for a GPO, complete the following steps:

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

1. After creating a GPO, click the **Save and Assign** button to complete the creation and continue with the following steps.
2. Select the GPO and then click **Manage assignments** in the action bar.
3. Select assignment targets (users, groups, and OUs) to assign the GPO to.

   NOTE:

   When assigning GPOs to machines, make sure that the machines reside either in OUs or in relevant security groups.

   - To add a new target, click **Add new target**. For more information, see Add an assignment target.
4. Use filters to contextualize the assignment and then set the priority of the GPO for each target.

   TIP:

   For information about adding filters, see Filters. Group Policy settings comprise user and machine settings. Some filter conditions apply only to user settings. If you apply those conditions to machine settings, the WEM agent skips them when evaluating the filter before assigning the settings. For a complete list of conditions that do not apply to machine settings, see Conditions not applicable to machine settings.
5. Click the ellipsis icon on each tile and do the following as needed:
   - **Copy configuration**. Lets you copy the configuration of the assignment.
   - **Paste configuration**. Lets you paste the configuration you copied from other configuration.
   - **Apply this configuration to all targets**. Lets you apply the configuration of the assignment to all targets.
6. After you finish, click **Save**.

CLONE A GPO

To clone a GPO, complete the following steps:

1. Select the GPO and then click **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the GPO to.

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

4. Click **Clone** to start the clone process.

DELETE A GPO

To delete a GPO, select it and then click **Delete** in the action bar.

> **NOTE:**
>
> If a GPO is already assigned to users, deleting it will impact those users.

Template-based settings

Use this tab to configure settings for Windows by using Group Policy Administrative Templates. You can configure GPOs at a machine and user level.

In **Actions > Group Policy Settings > Template-based** under a configuration set, you can perform the following operations:

- Create a GPO with a template.
- Manage templates.
- Import templates.
- Refresh the GPO list.
- Edit a GPO.
- Manage assignments for a GPO.
- Clone a GPO.
- Delete a GPO.

CREATE A GPO WITH A TEMPLATE

To create a GPO with a template, complete the following steps:

1. In the action bar, click **Create GPO**.
2. In **Basic information**:
    - Specify a name for the GPO.
    - Optionally, specify additional information to help you identify the GPO.
3. In **Computer configuration**, configure policies that you want to apply to machines (regardless of who logs on to them).
4. In **User configuration**, configure policies that you want to apply to users (regardless of which machine they log on to).

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

5. In **Summary**, review the changes you made.
6. After you finish, click **Done**.

In **Computer configuration** and **User configuration**, select a setting to configure it. You can show policies in tree view and list view. In list view, policies are sorted alphabetically, and you can search for desired policies.

To configure a setting, you first enable it. A setting might have multiple items that can be configured. Depending on the type of input needed, the setting can be a check box, input box (text or number as input), selection, list, or a combination.

For information about the settings, download a GPO reference sheet from Microsoft.

MANAGE TEMPLATES

To manage templates, complete the following steps:

1. In the action bar, click **Manage template**.
2. In the **Manage template** wizard:

- Select **Computer configuration** to configure policies that you want to apply to machines (regardless of who logs on to them).
- Select **User configuration** to configure policies that you want to apply to users (regardless of which machine they log on to).

1. After you finish, click **Done**.

In **Computer configuration** and **User configuration**, select a setting to configure it. You can show policies in tree view and list view. In list view, policies are sorted alphabetically, and you can search for desired policies.

To configure a setting, you first enable it. A setting might have multiple items that can be configured. Depending on the type of input needed, the setting can be a check box, input box (text or number as input), selection, list, or a combination.

For information about the settings, download a GPO reference sheet from Microsoft.

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

IMPORT TEMPLATES

IMPORTANT:

When importing ADMX files to WEM for use as templates, ensure that all .adml files in the zip file are of the same language.

You can import ADMX files to WEM for use as templates. You then create GPOs with those templates. To import templates, complete the following steps:

1. In the action bar, click **Manage template**.
2. In the **Manage template** wizard, click **Import**.
3. Browse to the zip file that contains your ADMX files and decide what to do if the file contains a template with the same name as an existing template:
    - **Do not import**. Cancels the import.
    - **Skip the template and import the rest**.
    - **Overwrite the existing template**. Overwriting might change associated settings originating from existing templates. Existing GPOs created with the templates are not affected. However, when you edit those GPOs, associated settings are lost.
4. Click **Start import** to start the import process.
5. After you finish, click **Done** to return to the **Manage template** wizard.
6. Manage templates there or click **Done** to exit.

For information on how to manage your imported template files, see Files. When managing them there, consider the following:

- Deleting GPO administrative template files will remove the associated settings from your current template. Existing GPOs created with the templates are not affected. However, when you edit those GPOs, associated settings are lost.

VIEW A GPO

You can view the WEM Group Policy settings and GPO summaries in read-only mode without editing the GPO. This implementation eliminates the risk of misconfiguration while reviewing the existing settings.

To view a GPO, complete the following steps:

1. Select the GPO and then click **View** in the action bar.

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

2. View the name, description, and configurations.
3. After you finish, click **Close**.

EDIT A GPO

To edit a GPO, complete the following steps:

1. Select the GPO and then click **Edit** in the action bar.
2. In **Basic information**, edit the name and description.
3. In **Computer configuration**, edit machine policies.
4. In **User configuration**, edit user policies.
5. In **Summary**, review the changes you made.
6. After you finish, click **Save**.

NOTE:

If a GPO is already assigned to users, editing it will impact those users.

MANAGE ASSIGNMENTS FOR A GPO

You can manage assignments for GPOs created using templates, just like you do for registry-based GPOs. For more information, see Manage assignments for a GPO.

CLONE A GPO

To clone a GPO, complete the following steps:

1. Select the GPO and then click **Clone** in the action bar.
2. Decide whether to clone the GPO as a registry-based GPO or a template-based GPO.

   NOTE:

   When cloned as registry-based, the GPO is converted to registry values and appears on the **Registry-based** tab. You can treat each converted GPO as a set of registry settings.

3. Edit the name and description.
4. Select the configuration set you want to clone the GPO to.
5. Click **Clone** to start the clone process.

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

DELETE A GPO

To delete a GPO, select it and then click **Delete** in the action bar.

NOTE:

If a GPO is already assigned to users, deleting it will impact those users.

Applications

This feature lets you add applications to assign to your users. When assigned, those applications have their shortcuts created on the desktop, Start menu, or taskbar, depending on your configuration.

TIP:

You can use the Full Configuration management console of Citrix DaaS to edit the application settings and then add an executable file path that points to **VUEMAppCmd.exe**. **VUEMAppCmd.exe** ensures that the Workspace Environment Management agent finishes processing an environment before Citrix DaaS and Citrix Virtual Apps and Desktops published applications are started. For more information, see Editing application settings using the Full Configuration management interface.

You can perform the following operations:

- Add an application.
- Refresh the application list.
- Edit an application to manage its properties.
- Manage assignments for an application.
- Clone an application.
- Delete an application.
- Switch to the Start menu view.
- Specify how the agent processes applications.

A general workflow to add and assign an application is as follows:

1. In the web console, go to the relevant configuration set, navigate to **Actions > Applications**, and click **Add application**. See Add an application.

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

2. Select the application you added and click **Manage assignments** in the action bar. See Manage assignments for an application.

The assignment takes some time to take effect, depending on the value you specified for SQL Settings Refresh Delay in Advanced Settings. For the assignment to take effect immediately, complete the following steps:

1. Go to **Web Console > Monitoring > Administration > Agents > Statistics** and select the agent.
2. Click **More** in the action bar and select **Agent > Refresh agent host settings**.

IMPORTANT:

- For the agent to process actions, verify that the following settings are enabled:
  - Launch agent on logon (for processing actions on logon)
  - Launch agent on reconnection (for processing actions on reconnection)
  - Enable desktop compatibility mode
- You can find these settings in Legacy Console > Advanced Settings > Configuration > Main Configuration > Agent Service Actions.

Add an application

To add an application, complete the following steps:

1. In **Applications**, click **Add application**.
2. On the **Basic information** page, configure the following settings:
   - **Name**. Specify a name to help you identify the application.
   - **Description**. Specify additional information about the application.
   - **State**. Enable or disable the application or put it into maintenance mode. When in maintenance mode, the application is unavailable for use. Its shortcut icon contains a warning sign, indicating that it is unavailable.
   - **Application type**. Specify the type of application the shortcut opens. The user interface differs depending on your selection.
     - **Installed application**. Create a shortcut that opens an application installed on the user's machine. If selected, prompts you to complete the following:

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

    - **Application path**. Type the full path of the application that resides on the user's machine.
    - **Working folder**. Type the full path to a folder on the user's machine as a working folder for the application. This field populates automatically after you type the full path in the **Application path** field.
    - **Parameters**. Type launch parameters for the application if needed.

- **File or folder**. Lets you create a shortcut that opens the target file or folder on the user's machine when a user clicks the shortcut icon. If selected, prompts you to complete the following:
    - **Path**. Type the full path to the target file or folder.
- **URL**. Lets you add the URL of an application. If selected, prompts you to complete the following:
    - **Application URL**. Type the URL of an application.
- **Citrix Workspace™ resource**. Lets you add an application from Citrix Workspace. If selected, prompts you to complete the following:
    - **Store URL**. Type the URL of a StoreFront™ or Workspace store that contains the resource you want to start from the application shortcut.

      NOTE:

      You can't open SaaS apps or certain applications of the **Citrix Workspace (Storefront) resource** type on the agent machine.

    - **Resource**. Use **Citrix Environment Tool Hub > Application Assistant** to browse to the target Workspace resource. Copy the resource information and paste it here by clicking **Paste resource info**. Click **Open Application Assistant** to open Citrix Environment Tool Hub (if installed). To download Citrix Environment Tool Hub, go to **Citrix Cloud > WEM service > Utilities**. For more information, see Citrix Environment Tool Hub.

3. On the **Options** page, configure the following settings:

- **Application icon**. Click **Change** to select a different icon or add a new icon.

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

    - To add a new icon, browse to an .ico file or paste the icon data copied from **Citrix Environment Tool Hub > Application Assistant**. WEM supports saving up to 100 icons. For more information, see Citrix Environment Tool Hub.

- **Set icon location on user's desktop**. Specify the target location of the application shortcut on the user's desktop. Values are in pixels. If moved, the shortcut reverts to the specified location on next logon.
- **Display name**. Specify the name of the shortcut. The name appears in the user environment.
- **Start menu integration**. Click **Change** to specify where to create the application shortcut on the left side of the Start menu. By default, a new shortcut is created in **Programs**. In the **Start menu integration** window, you can do the following:

    - Create a custom folder for the shortcut.
    - Specify where the application shortcut resides in the Start menu folder.
    - Rename a custom folder.

    NOTE:

    To delete custom folders, go to **Start menu view** in **Applications**. See Switch to the Start menu view.

- **Window style**. Specify whether the application opens in a minimized (minimized to taskbar), normal (normal screen view), or maximized (full-screen view) window on the user's machine.
- **Hotkey**. To set a hotkey, click the input field and press the key combination. Or enter the combination in the following format (for example): Ctrl + Alt + S
- **Enable automatic restore**. If enabled, the agent automatically recreates the shortcut (if moved or deleted) on refresh.
- **Hide application from agent menu**. Specify whether to show or hide the application in the agent menu accessible from the user's machine.
- **Create shortcut in user's Favorites folder**. Specify whether to create an application shortcut in the user's Favorites folder.

4. When you finish, click **Done** to save and exit.

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

Edit an application

To edit an application, complete the following steps:

1. In **Applications**, select the application. If needed, use the search box to quickly find the application.
2. Click **Edit** in the action bar.
3. On the **Basic information** and **Options** pages, make changes as needed.
4. After you finish, click **Save**.

Manage assignments for an application

To manage assignments for an application, complete the following steps:

1. Select the application and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign the application to.

- To add a new target, click **Add new target**. For more information, see Add an assignment target.
- Configure a target to specify which filter to use and where to create the application shortcut:
  - Create desktop shortcut
  - Add to Start menu
  - Pin to Start menu
  - Add to Quick Launch
  - Add to Windows startup
  - Pin to taskbar

1. Use filters to contextualize the assignment.
   - For information about adding filters, see Filters.
2. After you finish, click **Done**.

Clone an application

NOTE:

Assignments are not cloned.

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

To clone an application, complete the following steps:

1. Select the application and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the application to.
4. Click **Clone** to start the clone process.

Delete an application

To delete an application, select it and then select **Delete** in the action bar.

> **NOTE:**
>
> If an application is already assigned to users, deleting it will impact those users.

Switch to the Start menu view

To switch to the **Start menu view**, click **Start menu view**. The view shows where each application resides in the Start menu folder. You can do the following:

- Create a custom folder.
- Move an application to a desired folder.
- Rename a custom folder.
- Delete a custom folder. When you delete a custom folder, the applications in the folder will also be deleted.

Specify how the agent processes applications

Processing:

- Process applications on logon and refresh
- Process applications on reconnection
- Delete applications from desktops when unassigned
- Enforce processing of applications
- Enforce processing of filters for applications

StoreFront:

- Add a StoreFront URL and enter a description for it if needed. You need the URL when adding an application of type "Citrix Workspace resource." See Add an application.

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

External tasks

TIP:

External tasks work at a user session level. To run tasks at a machine level, use Scripted Tasks instead.

This feature lets you create external tasks to assign to your users. External tasks work at a user session level and can be scripts or applications. Make sure that the target agent machines have the necessary programs to run them. Commonly used scripts include: **.vbs** and **.cmd** scripts.

You can specify when to run an external task so that you can manage your user environments precisely and effectively.

You can perform the following operations:

- Create an external task
- Edit, clone, and delete an external task
- Manage assignments for an external task
- Refresh the external task list
- Enable and view reports for script-based external tasks

TIP:

You can quickly enable or disable an external task by using the toggle in the **State** column. To enable a task, configure at least 1 trigger for it.

Create an external task

To create a task, complete the following steps:

1. In **External Tasks**, click **Create external task**.
2. On the **Task** tab, configure the following settings.
    - **Name**. Specify a name to help you identify the task.
    - **Description**. Specify additional information about the task.
    - **Enable this task**. Controls whether the task is enabled or disabled. When disabled, the agent does not process the task even if the task is assigned to users.

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

- **Task details**
  - **Run script**. Supported script types (file types) are **.ps1**, **.vbs**, **.cmd**, **.bat**, **.py**. You can view the script by selecting **View content** or even replace the script by clicking **Replace**. However, an error is thrown if the script is larger than 1 MB and if you select an invalid or unsupported file/script format.
    - **Program to run script with**. Enter the path to the program to run the script with. This field appears only when the uploaded script is a python script with the **.py**. file extension.
    - **Arguments**. Enter arguments. This entry is optional.
    - **Working folder**. Enter the working folder. This entry is also optional.
  - **Run command**.
    - **Path**. Enter the path to the task or browse to the task. The path resolves in the user environment. Make sure that:
      - The path you specified here is consistent with the target agent machine.
      - The target agent machine has the corresponding program to run the task.
    - **Arguments**. Specify launch parameters or arguments. You can type a string. The string contains arguments to pass to the target script or application. For examples about using the **Path** and **Arguments** fields, see External task examples. This entry is optional.
    - **Working folder**. Enter the working folder. This entry is also optional.
- **Task settings**
  - **Run hidden**. If selected, the task runs in the background and is not visible to users.
  - **Run once**. If selected, WEM runs the task only once regardless of which options you select in **Triggers** and regardless of whether agents restart.
  - **Execution order**. Use this option when you have multiple tasks assigned to users and some tasks rely on others to run successfully. Tasks with an execution order value of 0 (zero) run first, then those with a value of 1, then those with a value of 2, and so on.
  - **Wait for task to complete**. Specify how long the agent waits for the task to complete. By default, the **Wait timeout** value is 30 seconds. If the task is script-based, you can select **Collect task output report** to collect output data from the task.

3. On the **Triggers** tab, select triggers that you want to associate with the task.

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

NOTE:

Not all triggers can be associated with external tasks. See Considerations.

- **Create new trigger**. See Create a trigger.
- **Show only triggers that apply to this task**. Filter out triggers that do not apply to the task.

4. When you finish, click **Done** to save and exit.

CONSIDERATIONS

External tasks work at a session level. You can associate only the following triggers with external tasks. See the following Supportability matrix for triggers table that lists the triggers that are supported for the tasks.

	SCRIPTED TASK	EXTERNAL TASK
Agent refresh		X
Reconnect		X
Logon		X
Logoff		X
Disconnect		X
Lock		X
Unlock		X
Machine startup	X	
Machine shutdown	X	
Scheduled	X	X
Process started		X
Process ended		X
Windows event	X	X

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

	SCRIPTED TASK	EXTERNAL TASK
Cloud Health Check result	X	
Profile Management health check result	X	
Custom scripted task	X	

- Built-in triggers:
  - **Agent refresh**
  - **Reconnect**
  - **Logon**
  - **Logoff**
  - **Disconnect**
  - **Lock**
  - **Unlock**
  - **Machine startup**
  - **Machine shutdown**
- Windows triggers:
  - **event**
- Schedulded triggers:
- User process triggers:
  - **Process started**
  - **Process ended**

When using the **Reconnect** built-in trigger, consider the following:

- If the WEM agent is installed on a physical Windows device, this option is not applicable.

When using the Disconnect, Lock, and Unlock triggers, consider the following:

- The implementation of disconnect, lock, and unlock is based on Windows events. In some environments, these options might not work as expected. For example, in desktops running on

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

Windows 10 or Windows 11 single-session VDAs, the disconnect option does not work. Instead, use the lock option. (In this scenario, the action we receive is "lock.")

- We recommend that you use these triggers with the UI agent. Two reasons:
  - When you use them with the CMD agent, the agent starts in the user environment each time the corresponding event occurs, to check whether the external task runs.
  - The CMD agent might not work optimally in concurrent task scenarios.

With user process triggers, you can define external tasks to supply resources only when certain processes are running and to revoke those resources when the processes end. Using processes as triggers for external tasks lets you manage your user environments more precisely compared with processing external tasks on logon or logoff. Before using user process triggers, verify that the following prerequisites are met:

- The WEM agent launches and runs in UI mode.
- The specified processes run in the same user session as the logged-on user.
- To keep the configured external tasks up to date, be sure to select **Enable Automatic Refresh** on the **Advanced Settings > Configuration > Advanced Options** tab.

When using the Windows event trigger, consider the following:

- Only the Windows event, with the user name recorded, can be used to trigger an external task.
- The WEM agent opens and runs in UI mode.

Edit an external task

To edit a task, perform the following steps:

1. In **External Tasks**, select the task. If needed, use the search box to quickly find the task.
2. Click **Edit** in the action bar.
3. On the **Task** and **Triggers** tabs, make changes as needed.
4. After you finish, click **Done**.

Manage assignments for an external task

To manage assignments for an external task, complete the following steps:

1. Select the task and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign the task to.

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

- To add a new target, click **Add new target**. For more information, see Add an assignment target.

3. Use filters to contextualize the assignment.
   - For information about adding filters, see Filters.
4. After you finish, click **Done**.

Clone an external task

NOTE:

Trigger associations and assignments are not cloned.

To clone a task, complete the following steps:

1. Select the task and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the task to.
4. Click **Clone** to start the clone process.

Delete an external task

To delete a task, select it and then select **Delete** in the action bar.

NOTE:

If an external task is already assigned to users, deleting it will impact those users.

Enable and view reports for script-based external tasks

NOTE:

For external tasks, reporting is available only for script-based tasks.

You can configure Workspace Environment Management to generate and display reports for a script-based external task. Two types of reports are available: **Action Processing Results** and **Action Processing Events**.

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

ENABLE EXTERNAL TASK REPORTING

To enable reporting for a script-based external task, complete the following setup:

1. Go to **Advanced Settings > Monitoring Preferences > Action Processing Results**, and select **External Tasks**.
2. When creating this external task, enable both **Wait for Task to Complete** and **Collect task output report**.

VIEW PROCESSING RESULTS OF EXTERNAL TASKS

The **Action processing results** report shows the final status of each script-based external task with reporting enabled, indicating whether it completed successfully or encountered an error.

To view the report:

1. Go to **Monitoring > Reports**.
2. Apply the **Event type Is Action processing results** filter.
3. On the **Action Processing Results** page that appears, select the **External Tasks** tab.

VIEW EVENT DETAILS OF EXTERNAL TASKS

The **Action processing events** report provides detailed information for each script-based external task with reporting enabled. Details include:

- Task result
- Agent that ran the task
- User who triggered the task
- Configuration set name
- Captured console output

To view the report:

1. Go to **Monitoring > Reports**.
2. Apply the **Event type Is Action processing events** filter.

Printers

This feature lets you add printers as assignable actions. When assigned, those printers are available for use within the user’s desktop.

You can perform the following operations:

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

- Add a printer.
- Add printers from a print server.
- Refresh the printer list.
- Edit a printer.
- Manage assignments for a printer.
- Clone a printer.
- Delete a printer.
- Specify how the agent processes printers.

A general workflow to add and assign a printer is as follows:

1. In the web console, go to the relevant configuration set, navigate to **Actions > Printers**, and click **Add printer**. See Add a printer.
2. Select the printer you added and click **Manage assignments** in the action bar. See Manage assignments for a printer.

The assignment takes some time to take effect. For immediate effect, see Make assignments take effect immediately.

Add a printer

To add a printer, complete the following steps:

1. In **Printers**, click **Add printer**.
2. Specify the action type. The interface differs based on the selected action type.
    - **Map network printer.**
        - **Name**. Specify a name to help you identify the printer.
        - **Description (optional)**. Specify additional information about the printer.
        - **Enable this printer**. Enable or disable the printer. When disabled, it is not processed by the agent even if assigned to a user.
        - **Printer path**. Specify the path to the printer as it resolves in the user environment.
        - **Connect using specific credentials**. By default, the agent uses the Windows account under which it runs to connect to the printer. Select this option if users must specify different credentials for the connection.
        - **Display name**. Specify the name of the printer. The name appears in the user environment.

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

- **Enable automatic restore**. If enabled, the agent automatically recreates the printer (if removed) on refresh.

- **Use printer mapping file**.
  - **Name**. Specify a name to help you identify the printer.
  - **Description (optional)**. Specify additional information about the printer.
  - **Enable this printer**. Enable or disable the printer. When disabled, it is not processed by the agent even if assigned to a user.
  - **File path**. You can configure printers for your users using an XML printer list file. Place the file on the agent machine that you use as an image. When the agent refreshes, it parses the XML file for printers to add to the action queue. See XML printer list configuration.

3. When you finish, click **Done** to save and exit.

Add printers from a print server

To add printers from a network print server, look for desired printers in **Citrix Environment Tool Hub > Printer Assistant**, copy their information, and then paste it. See Citrix Environment Tool Hub.

Edit a printer

To edit a printer, complete the following steps:

1. In **Printers**, select the printer. If needed, use the search box to quickly find the printer.
2. Click **Edit** in the action bar.
3. Make changes as needed.
4. After you finish, click **Save**.

Manage assignments for a printer

To manage assignments for a printer, complete the following steps:

1. Select the printer and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign the printer to.
   - To add a new target, click **Add new target**. For more information, see Add an assignment target.
   - Configure a target to specify which filter to use and whether to set it as the default printer. For information about adding filters, see Filters.

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

3. After you finish, click **Done**.

Clone a printer

NOTE:

Assignments are not cloned.

To clone a printer, complete the following steps:

1. Select the printer and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the printer to.
4. Click **Clone** to start the clone process.

Delete a printer

To delete a printer, select it and then select **Delete** in the action bar.

NOTE:

If a printer is already assigned to users, deleting it will impact those users.

Specify how the agent processes printers

Processing options:

- Process printers on logon and refresh
- Process printers on reconnection
- Delete printers from desktops when unassigned
- Enforce processing of printers
- Enforce processing of filters for printers
- Process printers asynchronously (if enabled, the agent processes printers asynchronously, without awaiting the completion of the processing of other actions)

Network drives

This feature lets you add network drives as assignable actions. When assigned, those network drives are available for use within the user's desktop.

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

You can perform the following operations:

- Add a network drive.
- Refresh the network drive list.
- Edit a network drive.
- Manage assignments for a network drive.
- Clone a network drive.
- Delete a network drive.
- Specify how the agent processes network drives.

A general workflow to add and assign a network drive is as follows:

1. In the web console, go to the relevant configuration set, navigate to **Actions > Network Drive**, and click **Add network drive**. See Add a network drive.
2. Select the network drive you added and click **Manage assignments** in the action bar. See Manage assignments for a network drive.

The assignment takes some time to take effect. For immediate effect, see Make assignments take effect immediately.

Add a network drive

To add a network drive, complete the following steps:

1. In **Network Drives**, click **Add network drive**.
2. Configure the following settings:
    - **Name**. Specify a name to help you identify the network drive.
    - **Description (optional)**. Specify additional information about the network drive.
    - **Enable this network drive**. Enable or disable the network drive. When disabled, it is not processed by the agent even if assigned to a user.
    - **Target path**. Specify the path to the network drive as it resolves in the user environment.
    - **Connect using specific credentials**. By default, the agent uses the Windows account under which it runs to connect to the network drive. Select this option if users must specify different credentials for the connection.
    - **Display name**. Specify the name of the network drive. The name appears in the user environment.

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

- **Enable automatic restore**. If enabled, the agent automatically recreates the network drive (if removed) on refresh.
- **Set as home drive**. If enabled, the network drive is set as the home drive.

3. When you finish, click **Done** to save and exit.

Edit a network drive

To edit a network drive, complete the following steps:

1. In **Network Drives**, select the network drive. If needed, use the search box to quickly find the network drive.
2. Click **Edit** in the action bar.
3. Make changes as needed.
4. After you finish, click **Save**.

Manage assignments for a network drive

To manage assignments for a network drive, complete the following steps:

1. Select the network drive and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign the network drive to.
   - To add a new target, click **Add new target**. For more information, see Add an assignment target.
   - Configure a target to specify which filter and drive letter to use. For information about adding filters, see Filters.
3. After you finish, click **Done**.

Clone a network drive

NOTE:

Assignments are not cloned.

To clone a network drive, complete the following steps:

1. Select the network drive and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the network drive to.

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

4. Click **Clone** to start the clone process.

Delete a network drive

To delete a network drive, select it and then select **Delete** in the action bar.

> **NOTE:**
>
> If a network drive is already assigned to users, deleting it will impact those users.

Specify how the agent processes network drives

Processing options:

- Process network drives on logon and refresh
- Process network drives on reconnection
- Delete network drives from desktops when unassigned
- Enforce processing of network drives
- Enforce processing of filters for network drives
- **Process network drives asynchronously**. If enabled, the agent processes network drives asynchronously, without awaiting the completion of the processing of other actions.

Drive letter:

- **Drive letters not to be used for assignment**. Any selected drive letter is excluded from the drive letter selection when assigning a drive resource.
- **Allow drive letter reuse in assignment**. If enabled, a drive letter used in an assignment is still available for use by other drives assigned to the same target.

Virtual drives

This feature lets you add virtual drives as assignable actions. When assigned, those virtual drives are available for use within the user's desktop.

You can perform the following operations:

- Add a virtual drive.
- Refresh the virtual drive list.
- Edit a virtual drive.
- Manage assignments for a virtual drive.

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

- Clone a virtual drive.
- Delete a virtual drive.
- Specify how the agent processes virtual drives.

A general workflow to add and assign a virtual drive is as follows:

1. In the web console, go to the relevant configuration set, navigate to **Actions > Virtual Drive**, and click **Add virtual drive**. See Add a virtual drive.
2. Select the virtual drive you added and click **Manage assignments** in the action bar. See Manage assignments for a virtual drive.

The assignment takes some time to take effect. For immediate effect, see Make assignments take effect immediately.

Add a virtual drive

To add a virtual drive, complete the following steps:

1. In **Virtual Drives**, click **Add virtual drive**.
2. Configure the following settings:
    - **Name**. Specify a name to help you identify the virtual drive.
    - **Description (optional)**. Specify additional information about the virtual drive.
    - **Enable this virtual drive**. Enable or disable the virtual drive. When disabled, it is not processed by the agent even if assigned to a user.
    - **Target path**. Specify the path to the virtual drive as it resolves in the user environment.
    - **Set as home drive**. If enabled, the network drive is set as the home drive.
3. When you finish, click **Done** to save and exit.

Edit a virtual drive

To edit a virtual drive, complete the following steps:

1. In **Virtual Drives**, select the virtual drive. If needed, use the search box to quickly find the virtual drive.
2. Click **Edit** in the action bar.
3. Make changes as needed.
4. After you finish, click **Save**.

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

Manage assignments for a virtual drive

To manage assignments for a virtual drive, complete the following steps:

1. Select the virtual drive and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign the virtual drive to.
    - To add a new target, click **Add new target**. For more information, see Add an assignment target.
    - Configure a target to specify which filter and drive letter to use. For information about adding filters, see Filters.

    IMPORTANT:

    The **Next available** and **No letter assigned** options apply only to network drives.
3. After you finish, click **Done**.

Clone a virtual drive

NOTE:

Assignments are not cloned.

To clone a virtual drive, complete the following steps:

1. Select the virtual drive and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the virtual drive to.
4. Click **Clone** to start the clone process.

Delete a virtual drive

To delete a virtual drive, select it and then select **Delete** in the action bar.

NOTE:

If a virtual drive is already assigned to users, deleting it will impact those users.

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

Specify how the agent processes virtual drives

Processing options:

- Process virtual drives on logon and refresh
- Process virtual drives on reconnection
- Delete virtual drives from desktops when unassigned
- Enforce processing of filters for virtual drives
- Enforce processing of filters for virtual drives

Drive letter:

- **Drive letters not to be used for assignment**. Any selected drive letter is excluded from the drive letter selection when assigning a drive resource.
- **Allow drive letter reuse in assignment**. If enabled, a drive letter used in an assignment is still available for use by other drives assigned to the same target.

Registry Entries

This feature lets you create, set, delete registry values, and assign them to create or modify registries. You can add tags to registry entries and assign multiple registry entries at the same time.

You can perform the following operations:

- Add a registry entry
- Refresh the registry entry list
- Edit a registry entry or entries
- Manage assignments for a registry entry or entries
- Clone a registry entry
- Import registry entries by **reg** file
- Delete a registry entry
- Remove tags

A general workflow to add and assign a registry entry is as follows:

1. In the web console, go to the relevant configuration set. Navigate to **Actions** > **Registry entries**, and click **Add registry entry**. For more details, see Add a registry entry.

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

2. Select the registry entry that you added and click **Manage assignments** in the action bar. For more details, see Manage assignments for a registry entry or multiple registry entries.

The assignment takes some time to take effect. For immediate effect, see Make assignments take effect immediately.

Add a registry entry

To add a registry entry, complete the following steps:

1. In registry entries, click **Add registry entry**.
2. Configure the following settings:
    - **Action type**. Describes the type of action of the resource.
    - **Name**. Specify a name to help you identify the registry entry. When you create a registry key value, leaving the **Name** field blank sets it as the default value for that key.
    - **Description** (optional). Specify additional information about the registry entry.
    - **Tags**. You can create new tags or select existing tags for the registry entry and then you can batch and manage registry entries with the tags.
    - **Enable this action**. Enable or disable the registry entry. When disabled, it is not processed by the agent even if assigned to a user or machine.
    - **Registry path**. Specify a registry path for the registry entry.
    - **Value name**. The name of your registry value as it appears in the registry (for example, **NoNtSecurity**).
    - **Type**. The type of registry entry that might be created.
    - **Data**. The value of the registry entry once created (for example, `0` or `C:\Program Files`)
    - **Run once**. If selected, WEM runs the action only once.
3. When you finish, click **Done** to save and exit.

Edit a registry entry or registry entries

To edit a registry entry or registry entries, complete the following steps:

1. In registry entries, select the registry entry or entries. If needed, use the search box or tag the list to quickly find the registry entry.
2. Click **Edit** in the action bar.
3. Make changes as needed.

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

4. After you finish, click **Save**.

Manage assignments for a registry entry or multiple registry entries

To manage assignments for a registry entry or multiple registry entries, complete the following steps:

1. Select the registry entry or registry entries and then select **Manage assignments** in the action bar. If needed, use the search box or tag list to quickly find the registry entry or registry entries.

> **NOTE:**
>
> To manage assignments for multiple registry entries, review the registry entries list and then click **Next**.

1. Select assignment targets (users and groups) to assign the registry entry.
   - To add a new target, click **Add new target**. For more information, see Add an assignment target.
   - Configure a target to specify which filter to use. For information about adding filters, see Filters.
2. After you finish, click **Done**.

Clone a registry entry

> **NOTE:**
>
> Assignments are not cloned.

To clone a registry entry, complete the following steps:

1. Select the registry entry and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set where you want to clone the registry entry.
4. Click **Clone** to start the clone process.

Import registry entries by `reg` file

You can convert your registry file into registry entries for an assignment. This feature has the following limitations:

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

- It supports only registry values under `HKEY_CURRENT_USER`. With the registry entries feature, you can assign only registry settings under `HKEY_CURRENT_USER`.
- It does not support registry values of the `REG_BINARY` and `REG_MULTI_SZ types`.

To avoid the limitations, we recommend that you import your registry files to WEM by using the **Import Group Policy settings** in **Group Policy Settings**. For more information, see, Import Group Policy settings.

To import registry entries, complete the following steps:

1. Select **Import** in the action bar.
2. Browse local `reg` file.
3. Click **Import** to load registry entries to the page.
4. Select the **Options** for the loaded registry entries.
5. Select **overwrite rule** for the loaded registry entries.
6. Click **Import** to start the import process.

Delete a registry entry

To delete a registry entry, select the registry entry and then select **Delete** in the action bar.

Remove tags

To remove tags for registry entries, complete the following steps:

1. Select the registry entries and then select **Remove tags** in the action bar.
2. Click **Remove** to begin the removal process.

Environment variables

This feature lets you add environment variables as assignable actions. When assigned, those environment variables are created or set in the user environment.

You can perform the following operations:

- Add an environment variable.
- Refresh the environment variable list.
- Edit an environment variable.
- Manage assignments for an environment variable.
- Clone an environment variable.

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

- Delete an environment variable.
- Specify how the agent processes environment variables.

A general workflow to add and assign an environment variable is as follows:

1. In the web console, go to the relevant configuration set, navigate to **Actions > Environment Variable**, and click **Add environment variable**. See Add an environment variable.
2. Select the environment variable that you added and click **Manage assignments** in the action bar. See Manage assignments for an environment variable.

The assignment takes some time to take effect. For immediate effect, see Make assignments take effect immediately.

Add an environment variable

To add an environment variable, complete the following steps:

1. In **Environment Variables**, click **Add environment variable**.
2. Configure the following settings:
    - **Name**. Specify a name to help you identify the environment variable.
    - **Description (optional)**. Specify additional information about the environment variable.
    - **Enable this environment variable**. Enable or disable the environment variable. When disabled, it is not processed by the agent even if assigned to a user.
    - **Variable name**. The functional name of the environment variable.
    - **Variable value**. The environment variable value.
    - **Execution order**. Use this option to determine the order in which the agent processes the variables. The agent first processes variables with an execution order value of 0 (zero), then those with a value of 1, then those with a value of 2, and so on. When conflicts occur, variables processed last overwrite those processed earlier.
3. When you finish, click **Done** to save and exit.

Edit an environment variable

To edit an environment variable, complete the following steps:

1. In **Environment Variables**, select the environment variable. If needed, use the search box to quickly find the environment variable.
2. Click **Edit** in the action bar.

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

3. Make changes as needed.
4. After you finish, click **Save**.

Manage assignments for an environment variable

To manage assignments for an environment variable, complete the following steps:

1. Select the environment variable and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign the environment variable to.
    - To add a new target, click **Add new target**. For more information, see Add an assignment target.
    - Configure a target to specify which filter to use. For information about adding filters, see Filters.
3. After you finish, click **Done**.

Clone an environment variable

NOTE:

- Assignments are not cloned.

To clone an environment variable, complete the following steps:

1. Select the environment variable and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the environment variable to.
4. Click **Clone** to start the clone process.

Delete an environment variable

To delete an environment variable, select it and then select **Delete** in the action bar.

NOTE:

- If an environment variable is already assigned to users, deleting it will impact those users.

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

Specify how the agent processes environment variables

Processing options:

- Process environment variables on logon and refresh
- Process environment variables on reconnection
- Delete environment variables from desktops when unassigned
- Enforce processing of filters for environment variables
- Enforce processing of filters for environment variables

More information

Make assignments take effect immediately

Typically, an assignment takes effect after the period of time that you specified for **SQL Settings Refresh Delay** in Advanced Settings. For the assignment to take effect immediately, complete the following steps:

1. Go to **Web Console > Monitoring > Administration > Agents > Statistics** and select the agent.
2. Click **More** in the action bar and select **Agent > Refresh agent host settings**.

IMPORTANT:

- For the agent to process actions, verify that the following settings are enabled:
  - Launch agent on logon (for processing actions on logon)
  - Launch agent on reconnection (for processing actions on reconnection)
  - Enable desktop compatibility mode
- You can find these settings in **Legacy Console > Advanced Settings > Configuration > Main Configuration > Agent Service Actions**.

Back up Group Policy settings

To back up your Group Policy settings, complete the following steps on your domain controller:

1. Open the Group Policy Management Console.
2. In the **Group Policy Management** window, right-click the GPO you want to back up and then select **Back Up**.

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

3. In the **Back Up Group Policy Object** window, specify the location where you want to save the backup. Optionally, you can give the backup a description.
4. Click **Back Up** to start the backup and then click **OK**.
5. Navigate to the backup folder and then compress it into a zip file.

NOTE:

WEM supports importing zip files that contain multiple GPO backup folders.

Configure FSLogix Profile Container using WEM GPO

For an example of how to configure settings for Windows by using Group Policy Administrative Templates, see Configure FSLogix Profile Container using WEM GPO.

Application launcher

Application launcher aggregates all applications you assigned to your users through the administration console. Using the tool, users can launch all assigned applications in one place.

TIP:

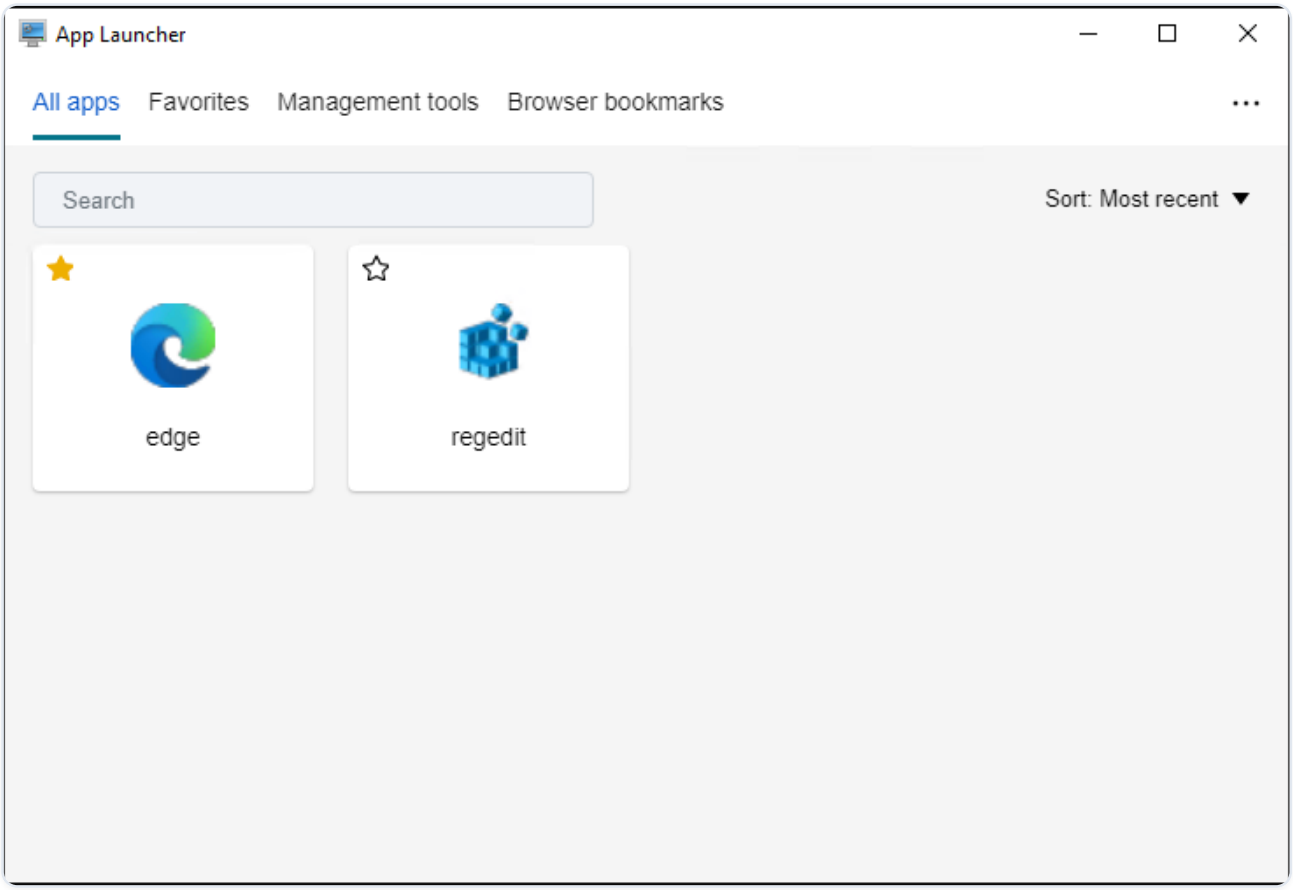
We recommend that you publish this tool as a Citrix virtual app.

This feature provides the following benefits:

- Assigned applications can be launched faster.
- Users can launch all applications assigned to them in one place.
- Users can quickly access their bookmarked websites. With Profile Management, browser bookmarks can be roamed.

Your users can directly open the application launcher tool (AppLauncherUtil.exe) in their environment. The tool is available in the agent installation folder: `%ProgramFiles%\Citrix\Workspace Environment Management Agent\ AppLauncherUtil.exe`. After opening the tool, users see the following, reflecting the applications assigned to them:

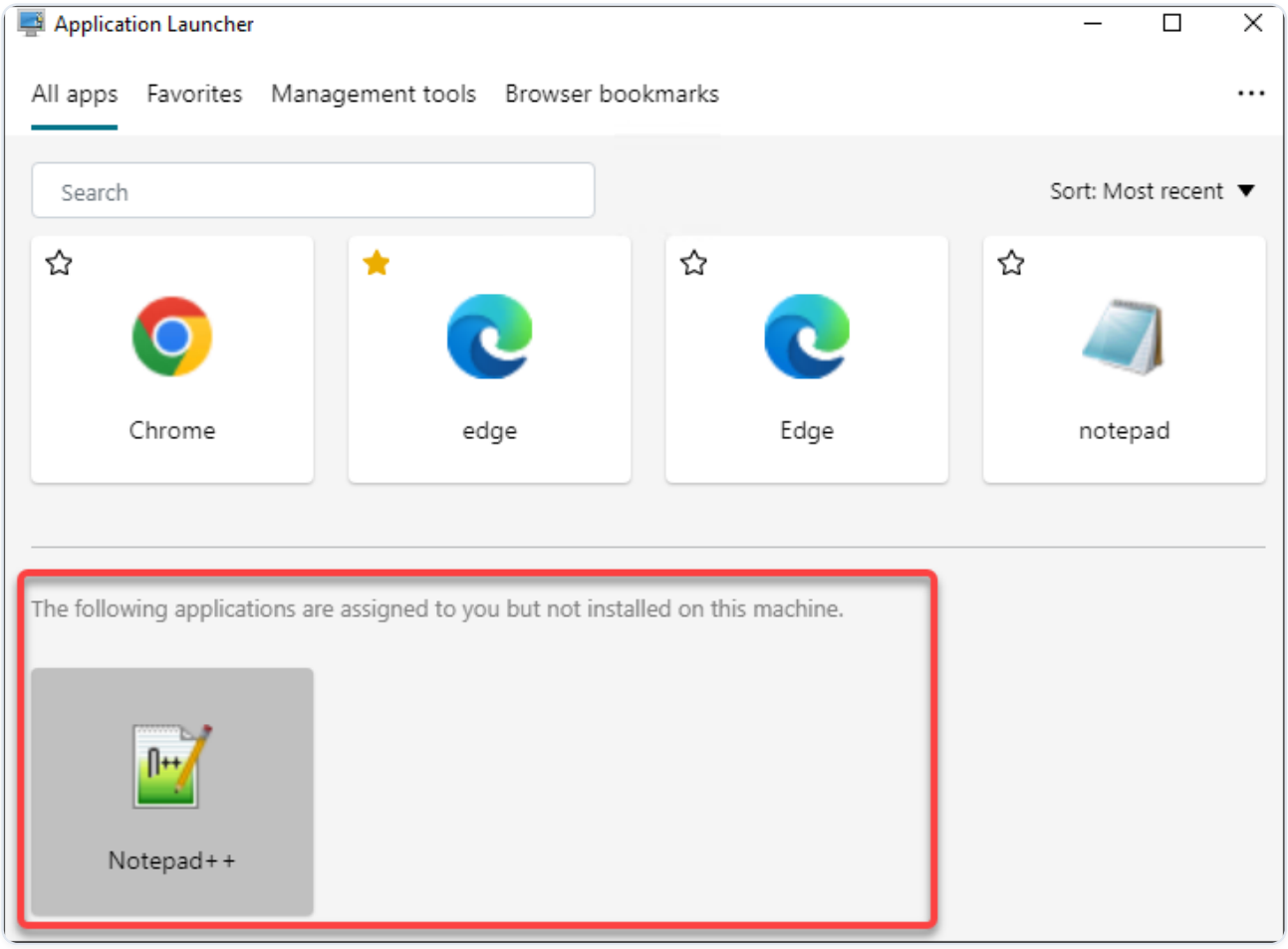
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **All apps**. Shows all assigned applications. Available sorting options: **Most recent**, **A-Z**, and **Z-A**.
- **Favorites**. Shows applications marked as favorites.
- **Management tools**. Shows the following two tools:
  - **Taskmgr**. Opens Task Manager.
  - **VUEMUIAgent**. Launches the WEM UI agent.
- **Browser bookmarks**. Shows websites saved in browser bookmarks. By clicking a bookmark, users can quickly open the browser and get to the target website. Bookmarks can be grouped by browser. This feature supports only Google Chrome and Microsoft Edge. Available sorting options: **Most recent**, **A-Z**, and **Z-A**.
- **Ellipsis icon**. There is a **Sign out** option that lets users sign out of their sessions.

Make sure that the assigned applications are present on the agent machine. If an assigned application is not installed on the agent machine, the application is shown but unavailable for launch.

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



For an example of how to use this feature, see Aggregate assigned applications in one place.

External task examples

For a script (for example, PowerShell script):

- If neither the folder path nor the script name contains blank spaces:
  - In the **Path** field, type the following: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.
  - In the **Arguments** field, type the following: `C:\<folder path>\<script name>.ps1`.

  Alternatively, you can type the path to the script file directly in the **Path** field. For example: `C:\<folder path>\<script name>.ps1`. In the **Arguments** field, specify arguments if needed. However, whether the script file runs or opens with a different program depends on file type associations configured in the user environment. For information about file type associations, see File Associations.
- If the folder path or the script name contains blank spaces:
  - In the **Path** field, type the following: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.

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

- In the **Arguments** field, type the following: `-file C:\<folder path>\<script name>.ps1`.

For an application (for example, iexplore.exe):

- In the **Path** field, type the following: `C:\Program Files\"Internet Explorer"\iexplore.exe`.
- In the **Arguments** field, type the URL of the website to open: `https://docs.citrix.com/`.

File System Operations

Controls the copying of folders and files into the user's environment.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

File system operations list

A list of your existing file and folder operations. You can use **Find** to filter the list by name or ID against a text string.

ADD A FILE SYSTEM OPERATION

1. Use the context menu **Add** command.
2. Enter details in the **New File System Operation** dialog tabs, then click **OK**.

FIELDS AND CONTROLS

Name. The display name of the file or folder operation, as it appears in the list.

Description. Lets you specify additional information about the resource. This field appears only in the edition or creation wizard.

Filesystem Operation State. Controls whether the file system operation is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Source Path. The path to the source file or folder that is copied.

Target Path. The destination path for the source file or folder that is copied.

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

Overwrite Target if Existing. Controls whether the file or folder operation overwrites existing files or folders with the same names in the target location. If cleared, and a file or folder with the same name already exists at the target location, the affected files are not copied.

Run Once. By default, Workspace Environment Management runs a file system operation every time the agent refreshes. Select this option to let Workspace Environment Management run the operation only once, rather than on every refresh. This speeds up the agent refresh process, especially if you have many file system operations assigned to your users.

Action Type. Describes what type of action this file or folder action is: **Copy**, **Delete**, **Move**, **Rename** or **Symbolic Link** operation. For symbolic link creation, you need to give users the `SeCreateSymbolicLinkPrivilege` privilege for Windows to allow symbolic link creation.

Execution order. Determines the running order of operations, letting certain operations run before others. Operations with an execution order value of 0 (zero) run first, then those with a value of 1, then those with a value of 2, and so on.

File Type Associations

IMPORTANT:

File type associations (FTAs) that you configure become default associations automatically. However, when you open an applicable file, the “How do you want to open this file?” window might still appear, prompting you to select an application to open the file. Click **OK** to dismiss the window. If you do not want to see a similar window again, do the following: Open the Group Policy Editor and enable the **Do not show the ‘new application installed’ notification** policy (**Computer Configuration > Administrative Templates > Windows Components > File Explorer**).

Controls the creation of FTAs in the user environment.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

This feature lets you add FTAs as assignable actions.

You can perform the following operations:

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

- Add FTAs
- Refresh FTAs
- Edit FTAs
- Manage assignments
- Clone FTAs
- Delete FTAs

To add FTAs

1. Use the context menu **Add association** command.
2. Enter details in the **Add file type association** dialog box.

Action Type. Describes what type of action this resource is.

Name. The display name of the file association, as it appears in the file association list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

File Association State. Toggles whether the file association is Enabled or Disabled. When disabled, it is not processed by the agent even if assigned to a user.

File Extension. The extension used for this file type association. If you select a file name extension from the list, the **ProgID** field automatically populates (if the file type is present on the machine where the administration console is running). You can also type the extension directly. However, for browser associations, you *must* type the extension directly. For more information, see Browser association.

ProgID. The programmatic identifier associated with an application (COM). This value automatically populates when you select a file extension from the list. You can also type the ProgID directly. To discover the ProgID of an installed application, you can use the OLE/COM Object Viewer (oleview.exe), and look in Object Classes/Ole 1.0 Objects. For more information about ProgID, see Programmatic identifier (ProgID).

Action. Lets you select the action type: open, edit, or print.

Target application. Lets you specify the executable used with this file name extension. Type the full path of the executable. For example, for UltraEdit Text Editor: `C:\Program Files\IDM Computer Solutions\UltraEdit\uedit64.exe`

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

Command. Lets you specify action types that you want to associate with the executable. For example:

- For an open action, type `“%1”`.
- For a print action, type `/p"%1"`.

Set as Default Action. Toggles whether the association is set as a default for that file name extension.

Overwrite. Toggles whether this file association overwrites any existing associations for the specified extension.

Run Once. By default, Workspace Environment Management (WEM) creates a file association every time the agent refreshes. Select this option to create the file association once, rather than on every refresh. This speeds up the agent refresh process, especially if you have many file associations assigned to your users.

TIP:

You can use File Type Association Assistant data to add them as assignable actions in the management console.

For more information, see Good to know.

Edit a file type association

To edit a file type association, complete the following steps:

1. In **File Type Associations**, select the required association. If needed, use the search box to quickly find the required file type association.
2. Click **Edit** in the action bar.
3. Make changes as needed.
4. After you finish, click **Save**.

Manage assignments

To manage assignments for a file type association, complete the following steps:

1. Select the file type association and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign the association to.

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

- To add a new target, click **Add new target**. For more information, see Add an assignment target.
- Use filters to contextualize the assignment. If necessary, set the priority of the required association for each target.
- Click the three ellipses associated with the assignment to copy the configuration.
- You can also apply the copied configuration to all the targets by choosing the respective option associated with the assignment.

Clone file type association

To clone a file type association, complete the following steps:

1. Select the file type association and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the file type association to.
4. Click **Clone** to start the clone process.

Delete a file type association

To delete a file type association, select it and then select **Delete** in the action bar.

Specify how the agent processes file type associations

Processing options:

- Process file type associations on logon and refresh
- Process FTAs on reconnection
- Enforce processing of filters for FTAs
- Delete FTAs from desktops when unassigned

JSON files

This feature lets you add JSON objects and assign them to create or modify JSON files. Using this feature, you can apply personalized settings to applications with a JSON configuration file (for example, Microsoft Teams).

You can perform the following operations:

- Add a JSON object.
- Refresh the JSON object list.
- Add a JSON object to the Windows 11 Start menu layout

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

- Edit a JSON object.
- Manage assignments for a JSON object.
- Clone a JSON object.
- Delete a JSON object.
- Control whether to process JSON objects.

A general workflow to add and assign a JSON object is as follows:

1. In the web console, go to the relevant configuration set, navigate to **Actions > JSON object**, and click **Add JSON object**. See Add a JSON object.
2. Select the JSON object that you added and click **Manage assignments** in the action bar. See Manage assignments for a JSON object.

The assignment takes some time to take effect. For immediate effect, see Make assignments take effect immediately.

Add a JSON object

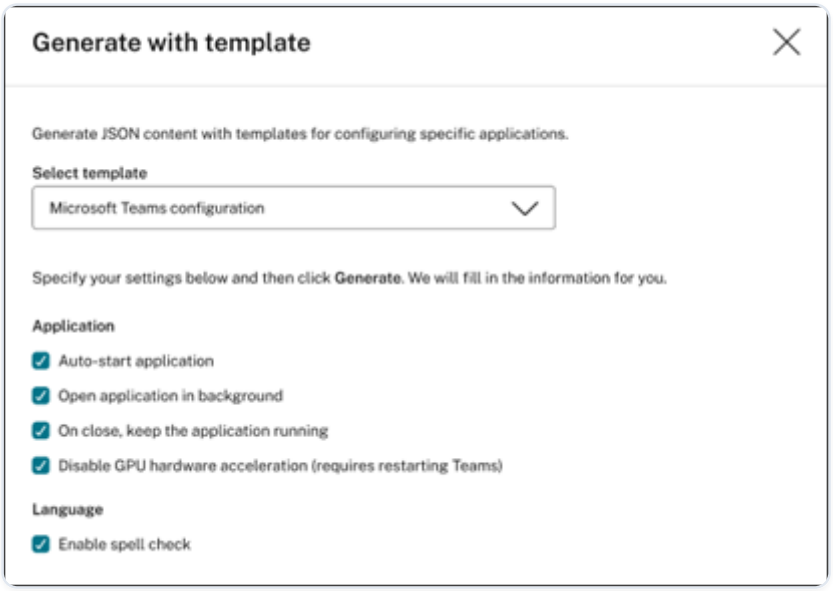
To add a JSON object, complete the following steps:

1. In **JSON objects**, click **Add JSON object**.
2. Configure the following settings:

    - **Name**. Specify a name to help you identify the JSON object.
    - **Description (optional)**. Specify additional information about the JSON object.
    - **Enable this action**. Enable or disable the JSON object. When disabled, it is not processed by the agent even if assigned to a user or machine.
    - **File path and content**. Specify the path to the JSON file that you want the object to modify. The specified content is merged with the existing content in the target file. To understand how content is merged, see JSON content merge example.

    If you don’t want to enter the path and content manually, click **Generate with template**. The **Generate with template** feature lets you generate JSON content with templates for configuring specific applications. Currently, the feature applies only to Microsoft Teams.

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



- **Create file if it does not exist**. This is a failsafe option ensuring that the object works as expected. For example, in the case of Microsoft Teams, the “desktop-config.json” file does not exist until Microsoft Teams is launched for the first time.
- **Back up the original file**. When selected, the agent automatically saves a backup of the target file in the same location. The backup inherits the name of the original and has a suffix “-WEMCopy.”
- **Processing mode**
  - **User-level processing**. Process the action when the user logs on or when the agent refreshes.
  - **Machine-level processing**. Process the action when the machine starts or when the agent refreshes its SQL connection settings.
- **Run once**. If selected, WEM runs the action only once.

3. When you finish, click **Done** to save and exit.

JSON CONTENT MERGE EXAMPLE

The following example illustrates how the specified content is merged with the existing content in the target JSON file.

Example of content in the target file:

```
{

    "value": "value1",

    "array": ["test1", "test2"],
```

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

```
    "object": {"key1": "value1", "key2":  "value2"}

}
```

Example of specified content:

```
{

    "value": "value2",

    "array": ["test2", "test3"],

    "object": { "key1": "changed", "key3": "value3", "key4": "value4" },

    "new": 1

}
```

Example of merged result:

```
{

    "value": "value2",

    "array": ["test1", "test2", "test3"],

    "object": {"key1": "changed", "key2": "value2", "key3": "value3",
"key4": "value4" },

     "new": 1

}
```

Add a JSON object to the Windows 11 Start menu layout

To add a JSON object to the Windows 11 Start menu layout, complete the following steps.

1. Click **Add a new JSON object**.
2. Select **Start menu configuration for Windows 11**.
3. Paste the configuration in the **Add JSON object** page.

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

4. Click **Done**.

For more information, see Customize the Start menu layout for Windows 11.

Edit a JSON object

To edit a JSON object, complete the following steps:

1. In **JSON objects**, select the JSON object. If needed, use the search box to quickly find the JSON object.
2. Click **Edit** in the action bar.
3. Make changes as needed.
4. After you finish, click **Save**.

Manage assignments for a JSON object

To manage assignments for a JSON object, complete the following steps:

1. Select the JSON object and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign the JSON object to.
   - To add a new target, click Add new target. For more information, see Add an assignment target.
   - Configure a target to specify which filter to use. For information about adding filters, see Filters.
3. After you finish, click **Done**.

Clone a JSON object

NOTE:

- Assignments are not cloned.

To clone a JSON object, complete the following steps:

1. Select the JSON object and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you want to clone the JSON object to.
4. Click **Clone** to start the clone process.

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

Delete a JSON object

To delete a JSON object, select it and then select **Delete** in the action bar.

NOTE:

- If a JSON object is already assigned to users, deleting it will impact those users.

INI Files

Controls the creation of **.ini** file operations, allowing you to modify **.ini** files.

Ini files operation list

A list of your existing **.ini** file operations. You can use **Find** to filter the list by name or ID against a text string.

TO ADD INI FILE OPERATION

1. Use the context menu **Add** command.
2. Enter details in the **Add INI File Operation** page and click **OK**.

FIELDS AND CONTROLS

Name. The display name of the .ini file operation, as it appears in the **Ini File Operations** list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

.ini File Operation State. Toggles whether the .ini file operation is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Target Path. Specifies the location of the .ini file that will be modified as it resolves in the user's environment.

NOTE:

While using a non-domain-joined agent, WEM might not work if the **Target Path** is a network share.

Target Section. Specifies which section of the .ini file this operation targets. If you specify a non-existent section, then it will be created.

Target Value Name. Specifies the name of the value that will be added.

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

Target Value. Specifies the value itself.

Run Once. By default, Workspace Environment Management performs an .ini file operation every time the agent refreshes. Select this checkbox to make the Workspace Environment Management operate only once, rather than at every refresh. This operation speeds up the agent refresh process, especially if you have many .ini file operations assigned to your users.

Action Type. Describes what type of action this resource is.

EDIT AN INI FILE OPERATION

To edit, complete the following steps:

1. Click **Edit** in the action bar.
2. Make changes as needed.
3. After you finish, click **Save**.

MANAGE ASSIGNMENTS

To manage assignments, complete the following steps:

1. Select the INI file and then select **Manage assignments** in the action bar.
2. Select assignment targets (users and groups) to assign this INI file to.
3. Use filters to contextualize the assignment.
4. Set the priority of the selected INI file for each target.
5. After you finish, click **Save**.

CLONE INI FILE OPERATION

To clone, complete the following steps:

1. Select the INI file and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you need to clone.
4. Click **Clone** to start the clone process.

DELETE INI FILE

To delete an INI file, select it and then select **Delete** in the action bar.

Ports

Lets you add port mappings as assignable actions. The Ports feature allows client COM port mapping. You can also use Citrix Studio policies to enable automatic connection of COM ports. If

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

you use the Ports feature to manually control the mapping of each port, remember to enable the Client COM port redirection policies in Citrix Studio. By default, COM port redirection is prohibited.

Ports list

A list of your existing ports. You can use **Find** to filter the list by name or ID.

ADD A PORT

1. Select **Add port mapping** from the context menu.
2. Enter details on the **Add port mapping** dialog tab, then click **OK**.

FIELDS AND CONTROLS

Name. The display name of the port, as it appears in the port list.

Description. Appears only in the edition/creation wizard and allows you to specify additional information about the resource.

Port State. Toggles whether the port is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Port Name. The functional name of the port.

Port Target. The target port.

OPTIONS TAB

Action Type. Describes what type of action this resource performs.

For example, you can configure the port settings as follows:

- **Port name**: Select “COM3:”
- **Port target**: Enter `\\Client\COM3:`

EDIT PORT MAPPING

To edit port mapping, complete the following steps:

1. Click **Edit** in the action bar.
2. Make changes as needed.
3. After you finish, click **Save**.

MANAGE ASSIGNMENTS

To manage assignments, complete the following steps:

1. Select a port mapping and then select **Manage assignments** in the action bar.

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

2. Select assignment targets (users and groups) to assign this port to.
3. Use filters to contextualize the assignment.
4. Set the priority of the selected port mappings for each target.
5. After you finish, click **Save**.

CLONE PORT MAPPING

To clone, complete the following steps:

1. Select the port and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you need to clone.
4. Click **Clone** to start the clone process.

DELETE PORT MAPPING

To delete port mapping, select it and then select **Delete** in the action bar.

User DSNs

Controls the creation of user DSNs.

User DSN list

A list of your existing user DSNs. You can use **Find** to filter the list by name or ID against a text string.

ADD A USER DSN

1. Use the context menu **Add** command.
2. Enter details in the **Add User DSN** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the user DSN, as it appears in the user DSN list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

User DSN State. Toggles whether the user DSN is enabled or disabled. When disabled, it will not be processed by the agent even if assigned to a user.

Data source name. The functional name of the user DSN.

Driver. The DSN driver. At present, only SQL server DSNs are supported.

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

Server Name. The name of the SQL server to which the user DSN is connecting.

Database Name. The name of the SQL database to which the user DSN is connecting.

Run Once. By default, Workspace Environment Management will create a user DSN every time the agent refreshes. Tick this box to make Workspace Environment Management only create the user DSN once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many DSNs assigned to your users.

Action Type. Describes what type of action this resource is.

EDIT A USER DSN

To edit a user DSN, complete the following steps:

1. Click **Edit** in the action bar.
2. Make changes as needed.
3. After you finish, click **Save**.

MANAGE ASSIGNMENTS FOR A USER DSN

To manage assignments for a user DSN, complete the following steps:

1. Select a user DSN and then select **Manage assignments** in the action bar.
2. Select assignment targets (users, groups, and OUs) to assign the user DSN to.
3. Use filters to contextualize the assignment.
4. Set the priority of the selected user DSN for each target.
5. After you finish, click **Save**.

CLONE A USER DSN

To clone a user DSN, complete the following steps:

1. Select the user DSN and then select **Clone** in the action bar.
2. Edit the name and description.
3. Select the configuration set you need to clone.
4. Click **Clone** to start the clone process.

DELETE A USER DSN

To delete a user DSN, select it and then select **Delete** in the action bar.

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

Security

Application security

Application security feature allows you to define rules to control which applications and files the users can run. You can configure application security rules in the web console and provide a tool to retrieve information needed for rule configuration. Also, you can use this feature to create assignment groups with security rules.

Configuration

When the **Process application rules** and **Process DLL rules** are enabled, the **Overwrite** mode is turned on by default. In **Overwrite** mode, the rules that are processed in the end overwrite rules that were processed earlier. We recommend that you apply this mode to only single-session machines. This feature also allows you to create the following rules:

- Executable rules
- Windows installer rules
- Script rules
- Packaged app rules
- DLL rules

NOTE:

Before creating rules, we recommend that you first add the default rules to ensure that important system files can run.

- **Process application rules**. When selected, the **Application Security** tab controls are enabled and the agent processes rules in the current configuration set, converting them into AppLocker rules on the agent host. When not selected, the **Application Security** tab controls are disabled.

  NOTE:

  This option is not available if the Workspace Environment Management™ administration console is installed on Windows 7 SP1 or Windows Server 2008 R2 SP1 (or earlier versions).

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

- **Process DLL Rules**. When selected, the agent processes DLL rules in the current configuration set. This option is only available when you select **Process Application Security Rules**.

  IMPORTANT:

  If you use DLL rules, you must create a DLL rule with *Allow* permission for each DLL that is used by all the allowed apps.

  Caution:

  If you use DLL rules, users may experience a reduction in performance.

- The **Overwrite** and **Merge** settings let you determine how the agent processes application security rules.

  - **Overwrite**. Lets you overwrite existing rules. When selected, the rules that are processed last overwrite rules that were processed earlier. We recommend that you apply this mode only to single-session machines.
  - **Merge**. Lets you merge rules with existing rules. When conflicts occur, the rules that are processed last overwrite rules that were processed earlier. If you need to modify the rule enforcement setting during merging, use overwrite mode because merge mode keeps the old value if it differs.

Rule collections

Each collection name indicates how many rules it contains, for example (12). Click a collection name to filter the rule list to one of the following collections:

- **Executable Rules**. Rules which include files with the .exe and .com extensions that are associated with an application.
- **Windows Rules**. Rules which include installer file formats (.msi, .msp, .mst) which control the installation of files on client computers and servers.
- **Script Rules**. Rules which include files of the following formats: .ps1, .bat, .cmd, .vbs, .js.
- **Packaged Rules**. Rules which include packaged apps, also known as Universal Windows apps. In packaged apps, all files within the app package share the same identity. Therefore, one rule can control the entire app. Workspace Environment Management supports only publisher rules for packaged apps.
- **DLL Rules**. Rules which include files of the following formats: .dll, .ocx.

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

When you filter the rule list to a collection, the **Rule enforcement** option is available. The following rule enforcement values are possible:

Off (default). Rules are created and set to *off*, which means they are not applied.

On. Rules are created and set to *enforce*, which means they are active on the agent host.

Audit. Rules are created and set to *audit*, which means they are on the agent host in an inactive state.

CREATE WINDOWS INSTALLER RULE

This includes two menu items, **Basic information** and **Exceptions**. To create a Windows installer rule, complete the following steps under **Basic information** and **Exceptions**:

- Selecting *Create rule* leads you to the **Create Windows installer rule** page.
- Enter the name and an optional description.
- Choose the desired **Action**.
- Select the **Criteria type** such as **Path**, **Publisher**, or **File hash** from the drop-down list.
- Selecting **Open File info Viewer** directs you to Citrix Environment Tool Hub. Use Citrix Environment Tool Hub to quickly get the required information. For more information, see File Info Viewer.
- Optionally, you can add exceptions to include files that are normally included in the rule based on the primary criteria. To perform this task, select **Add exception**.
- Go to Citrix Environment Tool Hub to copy data from one of the specified criteria under **File Info Viewer** and then click **Paste from File Info Viewer**.
- Click **Done**.
- Select **Continue to assignment** to update the assignments as required in the **Manage assignments** page.
- Select **Assignment targets** (users and groups) to assign this item to. Use filters to contextualize the assignment. Filters you specify are effective only in the **Overwrite** mode and are supported only on agent versions 2406 or later.
- Enter an asterisk if you need a specific rule to be applied to all files.

Import AppLocker rules in WEM web console

You can directly import application security rules exported from an AppLocker xml file into the WEM web console. Doing this, you can quickly bring in multiple rules from existing AppLocker

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

configurations, streamlining setup, and improving consistency across environments. When you import a rule, its assignment is also included.

To import AppLocker rules, navigate to the **Security > Application Security** tab and select **Import AppLocker rules**.

On the **Import AppLocker rules** page, two import mode options are available:

- **Skip**: The rules with the same GUID that exist in your environment are not created or updated. The existing rules are retained instead of using the ones from the XML file.
- **Overwrite**: The existing rules with matching GUIDs are updated using the rules from the XML file.

NOTE:

- The AppLocker rule XML file must not exceed 10 MB in size.
- The file must also be a valid XML format.
- The board displays an error message if the assignee can't be found or a rule can’t be imported.
- The creation of the rule fails if the rule is invalid.

Privilege elevation

This feature defines rules to run certain programs with administrator privileges. You can elevate the privileges of non-administrative users to an administrator level necessary for some executables. As a result, the users can start those executables as if they are members of the administrators group.

Privilege elevation options

- Process privilege elevation rules: When selected, enables agents to process privilege elevation settings and other options on the Privilege Elevation tab become available.
- Apply to Windows Server OSs: Controls whether to apply privilege elevation settings to Windows Server operating systems. If selected, rules assigned to users work on Windows Server machines. By default, this option is disabled.
- Enforce RunAsInvoker: Controls whether to force all executables to run under the current Windows account. If selected, users are not prompted to run executables as administrators.

This pane also displays the complete list of rules that you have configured. Click **Executable Rules**, **Windows Installer Rules**, or **Self-elevation** to filter the rule list to a specific rule type. You

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

can use Find to filter the list. The assigned column displays a check mark icon for assigned users or user groups.

Supported rules

You can configure privilege elevation using two types of rules: executable rules and Windows installer rules.

- **Executable Rules**: Rules that include files with .exe and .com extensions associated with an application.
- **Windows Installer Rules**: Rules that include installer files with `.msi` and `.msp` extensions associated with an application. When you add Windows installer rules, consider the following scenario:
  - Privilege elevation applies only to Microsoft's msiexec.exe. Make sure that the tool you use to deploy `.msi` and `.msp` Windows installer files is msiexec.exe.
  - Suppose that a process matches a specified Windows installer rule and its parent process matches a specified executable rule. The process cannot get elevated privileges unless the **Apply to Child Processes** setting is enabled in the specified executable rule.
- **Self-elevation**: When enabled, the **Run with administrator privileges** option is available in the context menu when you right-click a file. After selecting this option, you are prompted to provide a reason for the elevation. The elevation is then either allowed or denied, based on the criteria you specify. To configure the rule, you can use the **Citrix Environment Tool Hub** > **File Info Viewer** to quickly get the information required such as, path, publisher, and hash values. You can also specify the time period, choose the day of the week, and also optionally set the criteria to determine the machines on which the rule is effective. When the **Self-elevation** toggle is enabled for the first time in a configuration set, the self-elevation rule is created and can be found in the rule list when managing assignments for an assignment target. The rule is never removed after creation.

IMPORTANT:

When configuring privilege elevation rules with folder-based path conditions, ensure that *non-administrators* do not have **Write** access to the specified paths. Allowing **Write** access can let standard users place files in those locations and potentially gain elevated privileges.

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

If you've already configured a folder-based path condition and standard users have **Write** access, either update the folder permissions to restrict **Write** access to administrators only, or change the rule to use a **hash** or **publisher** condition instead.
You can specify the time period during which the rule is effective. Also, you can optionally set the criteria to determine on which machines the rule applies. You can choose to match all or any of the following criteria:

- Machine catalog name
- Delivery group name
- Device name
- IP address
- OS platform type
- OS version
- Persistent machine status

After you select the **Executable Rules**, the **Windows Installer Rules**, or the **Self-elevation** rules, the **Actions** section displays the following actions available to you:

- **Edit**. Lets you edit an existing executable rule.
- **Delete**. Lets you delete an existing executable rule.
- **Create Rule**. Lets you create an executable rule. To create an executable rule, follow the wizard instructions.

Process hierarchy control

The process hierarchy control feature controls whether certain child processes can be started from their parent processes in parent-child scenarios. You create a rule by defining parent processes and then designating an allow list or a block list for their child processes. Review this entire section before using the feature.

NOTE:

- This feature applies only to Citrix Virtual Apps.

To understand how the rule works, keep the following in mind:

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

- A process is subject to only one rule. If you define multiple rules for the same process, only the rule with the highest priority is enforced.
- The rule you defined is not restricted only to the original parent-child hierarchy but also applies to each level of that hierarchy. Rules applicable to a parent process prevail over rules applicable to its child processes regardless of the priority of the rules. For example, you define the following two rules:
  - Rule 1: Word cannot open CMD.
  - Rule 2: Notepad can open CMD.

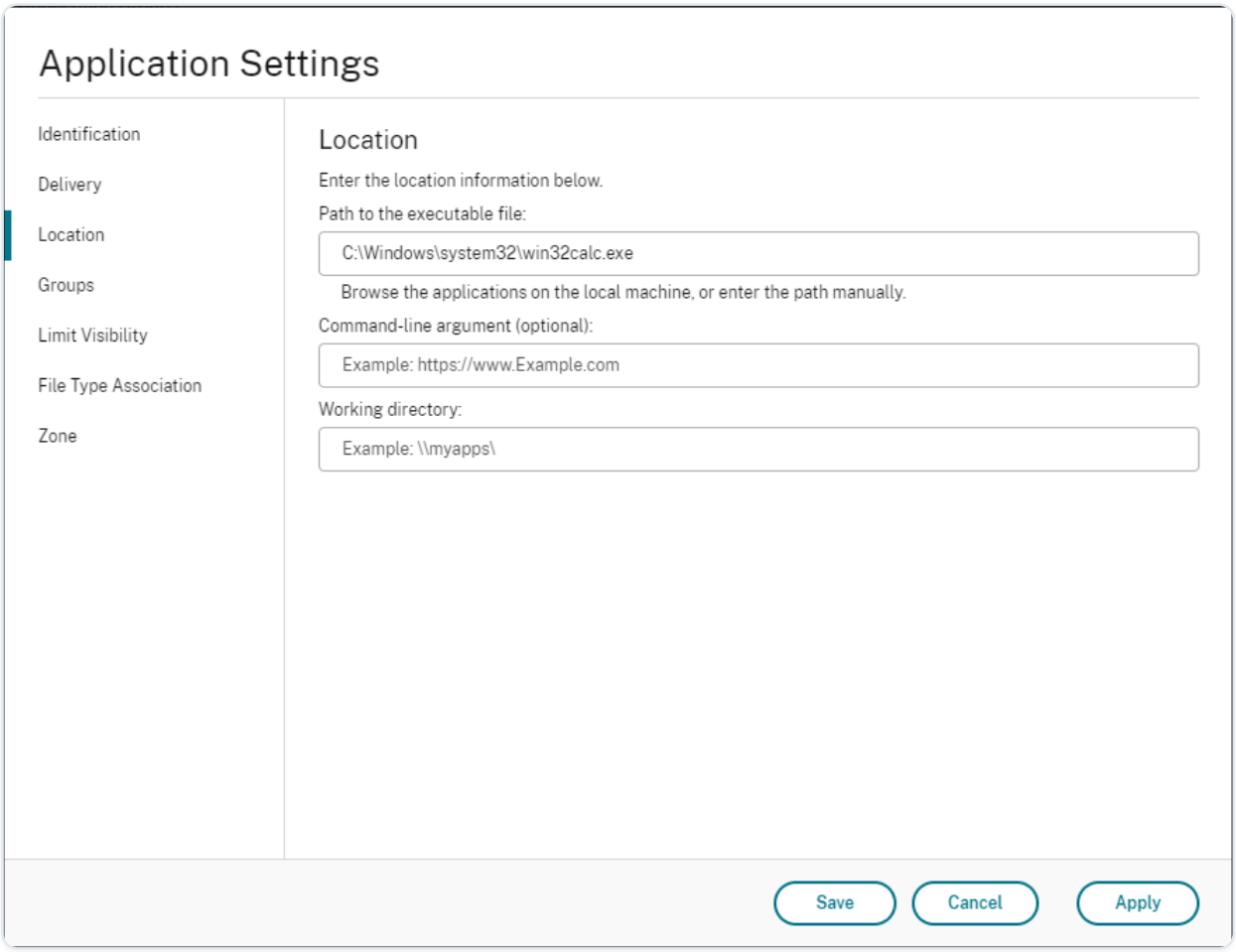
  With the two rules, you cannot open CMD from Notepad by first opening Word and then opening Notepad from Word, regardless of the priority of the rules.

This feature relies on certain process-based parent-child relationships to work. To visualize the parent-child relationships in a scenario, use the process tree feature of the Process Explorer tool. For more information about Process Explorer, see `<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>`.

To avoid any potential issues, we recommend that you add an executable file path that points to **VUEMAppCmd.exe** in the Full Configuration management interface. **VUEMAppCmd.exe** ensures that the WEM agent finishes processing settings before published applications start. Complete the following steps:

1. On the **Application** node, select the application, click **Properties** in the action bar, and then go to the **Location** page.

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



2. Type the path of the local application on the end-user operating system.

   - Under the **Path to the executable file** field, type the following:

     ```
     <%ProgramFiles%>\Citrix\Workspace Environment Management Agent\VUEMAppCmd.exe
     ```

3. Type the command-line argument to specify an application to open.

   - Under the **Command-line argument** field, type the full path to the application that you want to launch through **VUEMAppCmd.exe**. Make sure that you wrap the command line for the application in double quotes if the path contains blank spaces.
   - For example, suppose you want to launch iexplore.exe through **VUEMAppCmd.exe**. You can do so by typing the following: `%ProgramFiles(x86)%\"Internet Explorer"\iexplore.exe`.

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

Considerations

For the feature to work, you need to use the **AppInfoViewer** tool on each agent machine to enable the feature. Every time you use the tool to enable or disable the feature, a machine restart is required. With the feature enabled, be aware of the following considerations:

- You must restart the agent machine after upgrading or uninstalling the agent.
- The automatic agent upgrade feature does not work when the feature is enabled. To use the automatic agent upgrade feature, use the **AppInfoViewer** tool to first disable the process hierarchy control feature.

To verify that the process hierarchy control feature is enabled, open the **Registry Editor** on the agent machine. The feature is enabled if the following registry entry exists:

- 32-bit OS
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\WEM Hook`
- 64-bit OS
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\WEM Hook`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_Dlls\WEM Hook`

Prerequisites

To use the feature, make sure that the following prerequisites are met:

- A Citrix Virtual Apps deployment.
- The agent is running on Windows 10 or Windows Server.
- The agent host has been restarted after an in-place upgrade or fresh install.

Process hierarchy control options

When you select **Process Hierarchy Control** in **Security**, the following options appear:

Enable Process Hierarchy Control: Controls whether to enable the process hierarchy control feature. When selected, other options on the **Process Hierarchy Control** tab become available and configured settings take effect. You can use this feature only in a Citrix Virtual Apps deployment.

Hide Open With from Context Menu: Controls whether to show or hide the **Open With** option from the Windows right-click context menu. When enabled, the menu option is hidden from the

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

interface. When disabled, the option is visible and users can use it to start a process. The process hierarchy control feature does not apply to processes started through the **Open With** option. We recommend that you enable this setting to prevent applications from starting processes through system services that are unrelated to the current application hierarchy.

The **Process Hierarchy Control** tab also displays the complete list of rules that you have configured. You can use **Find** to filter the list. The assigned column displays a check mark icon for assigned users or user groups.

The **Actions** section displays the following actions:

- **Edit**. Lets you edit a rule.
- **Delete**. Lets you delete a rule.
- **Create rule**. Lets you add a rule.

CREATE RULE

1. Navigate to **Process Hierarchy Control** and click **Create rule**. The **Create rule** page appears.
2. In the **Display** section, type the following:
    - **Name**. Type the display name of the rule. The name appears in the rule list.
    - **Description**. Type additional information about the rule.
3. In the **Priority** section: set the priority for the rule. When configuring the priority, consider the following: The priority determines the order in which the rules you configured are processed. The greater the value, the higher the priority. Type an integer. If there is a conflict, the rule with the higher priority prevails.
4. In the **Criteria Type** section, select an option to add **Parent process**.
    - **Path**. The rule matches a file path.
    - **Publisher**. The rule matches a selected publisher.
    - **Hash**. The rule matches a specific hash code.
5. In the **Mode** section, select either of the following options:
    - **Allow list**. Set criteria for child processes that are allowed to open from the parent process. Everything else is denied.
    - **Deny list**. Set criteria for child processes that are not allowed to open from the parent process. Everything else is allowed.
6. Criteria for child processes.

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

7. Specify the time period during which the rule is effective.
8. Machine criteria: Set criteria to determine on which machines the rule is effective. You can optionally set the criteria to determine on which machines the rule applies. You can choose to match all or any of the following criteria:

    - Machine catalog name
    - Delivery group name
    - Device name
    - IP address
    - OS platform type
    - OS version
    - Persistent machine status

TO ASSIGN RULES TO USERS

Select one rule in the list and then click **Manage assignments** in the **Actions** section.

TO DELETE RULES

Select one or more rules in the list and then click **Delete** in the **Actions** section.

Assignments

Use assignments to make actions available to your users. This lets you replace a portion of your users' logon scripts.

Assignment targets

The **Assignment Targets** page lets you add users and groups (targets) so that you can assign actions and security rules to them. Select a target to manage its assignments.

NOTE:

Converting SIDs to target names can take some time. If the conversion is incorrect or fails, verify that the Cloud Connectors are working properly by viewing their health status. If the issue persists, contact Citrix Technical Support.

There are two built-in targets:

- **Everyone**. A built-in group that contains all users, including anonymous users and guests. Membership is controlled by the operating system.

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

- **Administrators**. A built-in group that includes all members of the administrators group. After the initial installation of the operating system, the only member of the group is the administrator account. When a computer joins a domain, the Domain Admins group is added to the administrators group. When a server becomes a domain controller, the Enterprise Admins group is added to the administrators group.

Options available to you include:

- **Filter**. Lets you filter the list.
- **Add an assignment target**. Lets you add a target.
- **Requery target names**. Updates the target names.
- **View.** Lets you view details for built-in targets.
- **Edit**. Lets you edit a target. You can change its description, priority, and enablement status. When configuring the priority, consider the following: The priority determines the order in which the actions you assign are processed. The greater the value, the higher the priority. Type an integer. If there is a conflict, the target with the higher priority prevails.
- **Enable**. Lets you enable or disable the object (target).
- **Delete**. Lets you delete a target. Note: Built-in targets will not be deleted.

TIP:

You can quickly enable or disable a target by using the toggle in the **State** column.

Add an assignment target

To add an assignment, perform the following steps:

1. On the **Assignment Targets** page, click **Add assignment target**.
2. Select the identity provider.
3. Select a domain where the targets you want to add exist.
4. Select the target type.

NOTE:

For Active Directory and Azure Active Directory, you can narrow your search to users or security groups. For Active Directory, you can also choose organizational units. Keep in mind that only Group Policy settings can be assigned to organizational units.

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

5. In the Search box, enter the name of the target you want to add. As you enter the name, matches appear in the menu.

   NOTE:

   The search returns only the top 50 results. Refine your search if necessary.

6. Click the plus icon to add the target. (Targets you already added appear with a green check mark icon.)

   TIP:

   If you want to add targets from a different identity provider, switch to a different identity type to continue.

7. After you finish, click **Add** to add the targets and to exit the wizard.

Manage assignments for a target

To manage assignments for a target, perform the following steps:

1. On the **Assignment Targets** page, select the target. If needed, use the search box to quickly find the target.
2. In the action bar, select **Manage assignments**. The **Manage assignments** window appears.
3. Manage the assignments for each action or the security rules as needed. You can also select the Privilege Elevation rules to assign the target under the Manage security rule assignments page.
4. Click **Review changes** to verify that you made the changes as intended.

Clone an assignment target

To clone an assignment target, perform the following steps:

1. On the **Assignment Targets** page, select the target. If needed, use the search box to quickly find the target.
2. In the action bar, select **Clone**. The **Clone assignment target** window appears.
3. Select the configuration set to clone the target to.
4. Click **Clone**.

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

NOTE:

- You cannot clone built-in targets.
- You can clone up to 10 targets at a time.
- If a target already exists in the destination, it is skipped.
- Descriptions of cloned targets are empty. Their assignments are not cloned, their priority is set to a default value (100), and their state defaults to enabled (check mark icon).

Filters

NOTE:

- This feature is available as a preview.
- Filters are for use with assignments and scripted tasks.

The **Filters** page lets you add filters for controlling when to assign actions to your users. A filter can comprise multiple conditions.

There is a built-in filter:

- **Always true**. If selected, the related actions are always assigned to target users. You cannot edit or delete this built-in filter.

Options available to you include:

- **Add filter**. Lets you add a filter so it is available for use when you assign actions.
- **Manage conditions**. Lets you add, delete, and edit conditions.
- **Refresh**. Updates the list of filters. Using this option also refreshes the list of conditions in **Manage conditions**.
- **Edit**. Lets you edit a filter. If you edit a filter that is bound to actions assigned to users, the change will impact those users immediately.
- **Delete**. Lets you delete a filter.
- **State**. Lets you enable or disable a filter.

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

Create filters

You can create a filter using one of two methods:

- Create manually. Create a filter from scratch by manually configuring conditions.
- Create from template. Create a filter based on a predefined template. This method simplifies setup by prepopulating conditions.

CREATE FILTERS MANUALLY

To create a filter from scratch, follow these steps:

1. On the **Filters** page, click **Create filter**, and then select **Create manually**.
2. On the **Filters** page, click **Add filter**.
3. In **Basic information**, configure the following and then click **Next**.
    - **Filter name**. Enter a name for the filter.
    - **Description**. Enter a description for the filter to help you identify it from your other filters. This field is optional.
    - **Enable this filter**. Select **Yes** to enable or **No** to disable the filter.
4. In **Conditions**, build your filter by adding conditions. Click the operator to toggle between **Match all** (**AND** operator) or **Match any** (**OR** operator). You can use both operators to combine two or more conditions into a compound condition.
    - **Add condition**. Select conditions from the list or create new ones.
    - **Add condition group**. Add a condition group to group a series of conditions using the same logical operator - **AND** or **OR**. You can add condition groups within condition groups. You can nest condition groups up to three levels.

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

NOTE:

- Conditions you create here are available for use with other filters.
- Use the **Summary** section for a deeper understanding of the criteria of compound conditions.
- Filters containing **OR** operators are evaluated only on agents whose version is 2210.2.0.1 or later.
- Certain types of conditions apply only to user settings. If you apply them to machine settings (for example, scripted tasks and GPOs), the agent skips them when evaluating the filter. For a complete list of filter conditions that do not apply to machine settings, see Conditions not applicable to machine settings.
- If the filter conditions at the same level are bound by **OR**, then meeting either of the conditions at that level is sufficient. If the filter conditions at the same level are bound by **AND**, then all the conditions at that level must be met.

5. Click **Done** when finished.

CREATE FILTERS FROM TEMPLATES

Creating a filter based on a predefined template simplifies the setup by prepopulating conditions. For example, the **Filter for Citrix virtual desktops** template helps you quickly create a filter that assigns actions only when user sessions occur on Citrix Virtual Desktops.

NOTE:

- Template-based filters currently operate only at the session level.
- Currently, three templates are available to help you quickly create filters that identify Citrix Virtual Apps™ environments, Citrix Virtual Desktops environments, and time ranges.

To create a filter from a template, follow these steps:

1. On the **Filters** page, click **Create filter**, and then select **Create from template**. The **Create filter from template** page appears.
2. Enter a name for the filter.
3. (Optional) Enter a description to help identify the filter.

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

4. Select a template for the filter. See the following table for available templates.

NAME	PURPOSE	SCOPE
Filter for Citrix virtual apps	A template for creating filters that identify Citrix Virtual Apps environments.	Session-level filtering
Filter for Citrix virtual desktops	A template for creating filters that identify Citrix Virtual Desktops environments.	Session-level filtering
Filter for time range	A template for creating filters that identify specific time ranges.	Session-level filtering
	Note: Time range filters rely on automatic refresh, which occurs by default every 30 minutes, to take effect. As a result, the filter might not apply exactly at the configured time and could be delayed until the next refresh.	

5. Click **Done**.

NOTE:

- Filters created from templates are automatically enabled.
- You can add more conditions to these filters by editing them after creation.

Create a condition

You can create conditions when you add a filter or manage conditions. In the **Create condition** wizard that appears, perform the following steps:

1. Enter a condition name.
2. Select **Yes** to enable or **No** to disable the condition.

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

3. Select a condition type from the list and then configure settings accordingly.

Different condition types might have different settings. The following condition types are available:

CONDITION TYPE	DESCRIPTION
Always true	The condition always holds true.
Active Directory attribute	True or false depending on whether the attribute name matches the specified values. Enter attribute values, separated by semicolons (;). Note: If you want the condition to hold true regardless of the attribute value, enter a question mark (?).
Active Directory group	True or false depending on whether the group name matches the specified values. Enter group names, separated by semicolons (;).
Active Directory path	True or false depending on whether the path matches the specified values. Enter paths, separated by semicolons (;). Note: You can use the asterisk (*) as a wildcard.
Active Directory site	True or false depending on whether the site name matches the specified values. Enter site names, separated by semicolons (;).
Citrix Provisioning™ image mode	True or false depending on whether the image mode is **Shared** or **Private**.

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

CONDITION TYPE	DESCRIPTION
Citrix Virtual Apps™ farm name	True or false depending on whether the farm name matches the specified value.
Citrix Virtual Apps version	True or false depending on whether the version matches the specified value.
Citrix Virtual Apps zone name	True or false depending on whether the zone name matches the specified value.
Delivery group name	True or false depending on whether the delivery group name matches the specified value. **Note:** You can use delivery groups stored in subfolders as filter conditions by specifying the full path in the name. Example: `Subfolder name\Delivery group name`
Machine catalog name	True or false depending on whether the machine catalog name matches the specified value. **Note:** You can use machine catalogs stored in subfolders as filter conditions by specifying the full path in the name. Example: `Subfolder name\Machine catalog name`

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

CONDITION TYPE	DESCRIPTION
Citrix Virtual Desktops farm name	True or false depending on whether the farm name matches the specified value.
Client IP address	True or false depending on whether the IP address matches the specified value.
Client name	True or false depending on whether the client name matches the specified values. Enter client names, separated by semicolons (;). You can use the asterisk (*) as a wildcard. You can also use dynamic tokens.
Client OS	True or false depending on whether the client OS matches the specified value.
Client remote OS	True or false depending on whether the client remote OS matches the specified value.
Computer name	True or false depending on whether the computer name matches the specified values. Enter computer names, separated by semicolons (;). You can use the asterisk (*) as a wildcard.
Connection state	True or false depending on whether the connection state is **Online** or **Offline**.
Date and time	True or false depending on whether the date and time matches the specified values. Enter dates or date ranges,

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

CONDITION TYPE	DESCRIPTION
	separated by semicolons (;). Enter dates in the format, `mm/dd/yyyy`. Enter date ranges in the format (time optional), `mm/dd/yyyy HH:mm - mm/dd/yyyy HH:mm`.
Day of week	True or false depending on whether the day matches the specified values.
Dynamic value	True or false depending on whether the dynamic value matches the specified values. Enter values the dynamic expression resolves to, separated by semicolons (;). Note: If you want the condition to hold true regardless of the value of the dynamic expression, enter a question mark (?).
Environment variable	True or false depending on whether the environment variable matches the specified values. Enter values of the environment variable, separated by semicolons (;). Note: If you want the condition to hold true regardless of the value of the environment variable, enter a question mark (?).
File version	True or false depending on whether the file version matches the specified values. Enter file versions, separated by semicolons (;).

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

CONDITION TYPE	DESCRIPTION
File/folder exists or not	True or false depending on whether the path matches the specified value. Enter a full path of the file or the folder. You can use dynamic tokens.
IP address	True or false depending on whether the IP address matches the specified value. Enter IP addresses or IP address ranges, separated by semicolons (;). Note: You can use the asterisk (*) as a wildcard.
Name is in list or not	True or false depending on whether the name is in the specified list. In the **Name** field, enter a name to look for in the list. In the **File path of XML list** field, enter a full file path of the XML list.
Name/value is in list or not	True or false depending on whether the name or value is in the specified list. In the **Name** field, enter a name or value to look for in the list. In the **File path of XML list** field, enter a full file path of the XML list.
Network connection state	True or false depending on whether the network connection state is **Available** or **Not available**.
OS platform type	True or false depending on whether the OS platform type is **x86** or **x64**.

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

CONDITION TYPE	DESCRIPTION
Published resource name	True or false depending on whether the name matches the specified values. Enter published resource names, separated by semicolons (;).
Registry value	True or false depending on whether the registry value matches the specified values. In the **Registry path and name** field, enter a full path that includes the registry value name. In the **Registry value** field, enter registry values, separated by semicolons (;). Note: If you want the condition to hold true regardless of the value of the registry entry, enter a question mark (?).
Transformer mode state	True or false depending on whether the state is **Disabled** or **Enabled**.
Regional format	True or false depending on whether the format matches the specified value. Use the **Add values not in the list** option to enter ISO language codes, separated by semicolons (;), if necessary.
User SBC resource type	True or false depending on whether the type is **Desktop** or **Published application**.
User UI language	True or false depending on whether the language matches the specified values.

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

CONDITION TYPE	DESCRIPTION
WMI query	True or false depending on whether the specified query has a result. The Windows Management Instrumentation (WMI) query operation can run queries on the agent machine. You can define this condition based on results returned from the query. For more information, see the Microsoft documentation: `<https://docs.microsoft.com/en-us/windows/win32/wmisdk/querying-with-wql>`.

When using "client" and "computer" related condition, be aware of the following two scenarios:

- If the agent is installed on a single-session or multi-session OS:
  - "Client" refers to a client device connecting to the agent host.
  - "Computer" and "Client Remote" refer to the agent host.
- If the agent is installed on a physical endpoint, conditions that contain "client" in the condition names are not applicable.

More information

Conditions not applicable to machine settings

There are two types of settings:

- **Machine settings**. Those settings apply only to machines regardless of who logs on to them. Examples: Group Policy settings and scripted tasks.
- **User settings**. Those settings apply only to users regardless of which machine they log on to. Example: User's language settings.

The following conditions do not apply to machine settings. If a filter contains any of them, the agent skips them when evaluating the filter.

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

FILTER NAME	APPLICABLE TO MACHINE SETTINGS
ClientName Match	No
Client IP Address Match	No
Registry Value Match	If you configure a registry value starting with HKCU, the **Registry Value Match** filter does not work if applied to machine settings.
User Country Match	No
User UI Language Match	No
User SBC Resource Type	No
Active Directory Path Match	No
Active Directory Attribute Match	No
No ClientName Match	No
No Client IP Address Match	No
No Registry Value Match	No
No User Country Match	No
No User UI Language Match	No
No Active Directory Path Match	No
No Active Directory Attribute Match	No
Client Remote OS Match	No
No Client Remote OS Match	No
Active Directory Group Match	No
No Active Directory Group Match	No
Published Resource Name	No

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

Triggers

Create triggers and associate tasks with them. When activated, the triggers start the associated tasks in the user environment. To view the tasks associated with a trigger, click the trigger to expand its row.

You can perform the following operations:

- Create a trigger
- Refresh the view
- Edit a trigger
- Clone a trigger
- Manage associations
- Delete a trigger

TIP:

You can quickly enable or disable a trigger by using the toggle in the **State** column.

The built-in triggers are listed as follows:

- Session triggers:
  - **Agent refresh**. Activated when users refresh the agent.
  - **Reconnect**. Activated when a user reconnects to an agent machine.
  - **Logon**. Activated when users log on to their machines.
  - **Logoff**. Activated when users log off from their machines.
  - **Disconnect**. Activated when users disconnect from their machines.
  - **Lock**. Activated when users lock their machines.
  - **Unlock**. Activated when users unlock their machines.

  NOTE:

  Session triggers let you configure session activities as triggers and are currently available only for external tasks.

- Machine triggers:

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

- **Machine shutdown**. Activated when machines shut down.
- **Machine startup**. Activated when machines start up.

NOTE:

- You cannot delete and edit built-in triggers.
- For an example of how to use startup and shutdown triggers, see Configure startup and shutdown triggers for scripted tasks.

Create a trigger

To create a trigger, perform the following steps:

1. In **Triggers**, click **Create trigger**.
2. Specify a name for the trigger.
3. Optionally, specify additional information to help you identify the trigger.
4. Choose whether to enable (**Yes**) or disable (**No**) the trigger.

   NOTE:

   If disabled, the agent does not evaluate and process the trigger.

5. Select a trigger type from the list and fill in the required information.

   - **Scheduled**
   - **Process started**
   - **Process ended**
   - **Windows event**
   - **Cloud Health Check result**
   - **Profile Management health check result**
   - **Scripted task result**

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

TIP:

- The information varies depending on the trigger type that you select. For details, see Available trigger types.
- For an example of how to use Windows events as triggers, see Use Windows events as triggers to detect VDA registration issues.

6. In **Summary**, verify that you created the trigger as intended.
7. When you have finished, click **Done** to save and exit.

Available trigger types

The following trigger types are available for selection:

- **Scheduled**. Schedules when to activate the trigger. The following options are available:
  - **Date and time**. Specify when the trigger is activated.
  - **Repeat**. Select **Yes** to specify how often the trigger is activated. For example, every one hour, every two hours, every day, every two days. If you select **Week** or **Month**, you can specify one or more specific days. Select **No** if you want the trigger to activate only once.
- User process triggers
  - **Process started**. Activates the trigger when specified processes start.
  - **Process ended**. Activates the trigger when specified processes end.

NOTE:

User process triggers let you configure user processes as triggers and are currently available only for external tasks.

- **Windows event**. Lets you define the criteria that Windows events must meet to activate the trigger. The following options are available:
  - **Add criterion**. Define the criteria that Windows events must meet to activate the trigger.
  - **Interval**. Specify an interval, in minutes, for the trigger. After being activated, the trigger will not be activated again until the specified interval elapses.

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

NOTE:

Only Windows classic event logs such as Application, System, or Security are supported.

- **Cloud Health Check result**. Activates the trigger when Cloud Health Check returns a specified health status. The following options are available:
  - **VDA health status**. Use VDA health status to activate the trigger. VDAs can be in normal or unusual state, as shown in Home > Overview.
  - **Task data**. Select data to pass to associated tasks, and specify the parameters in those tasks to receive the data. If a parameter you specify here is the same as the one configured for associated tasks, the former takes precedence. We recommend using the default parameter names. Update your script files if necessary. You can specify the following data:
    - **VDA health status (string)**. The health status that Cloud Health Check returns. Use the parameter in associated tasks to receive the status.
    - **Health report (string)**. The VDA health check report that Cloud Health Check generates. Use the parameter in associated tasks to receive the full path of the report. For more information, see Heath check results.
- **Profile Management health check result**. Activates the trigger when Profile Management health check returns a specified health status. The following options are available:
  - **Profile Management health status**. Use the following Profile Management health statuses to trigger associated tasks: Warning (suboptimal state of Profile Management) and Error (Profile Management configured incorrectly).
  - **Task data**. Select data to pass to associated tasks, and specify the parameters in those tasks to receive the data. If a parameter you specify here is the same as the one configured for associated tasks, the former takes precedence. We recommend using the default parameter names. Update your script files if necessary. You can specify the following data:
    - **Profile Management health status (string)**. The health status that the Profile Management health check returns. Use the parameter in associated tasks to receive the status. For more information, see Administration.
    - **Health report (string)**. The health check report that the Profile Management health check generates. Use the parameter in associated tasks to receive the full path of the report. For more information, see Reports.

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

- **Scripted task result**. Activates the trigger when scripted tasks return specified results. You first specify custom scripts and then define the criteria that the scripts must meet to activate the trigger. The following options are available:
  - **Add criterion**. Select one or more scripts and then define the criteria that those scripts must meet to activate the trigger.
  - **Task data**. Select data to pass to associated tasks, and specify the parameters in those tasks to receive the data. If a parameter you specify here is the same as the one configured for associated tasks, the former takes precedence. We recommend using the default parameter names. Update your script files if necessary. You can specify the following data:
    - **Script name (string)**. The name of the script that triggers the associated task. Use the parameter in associated tasks to receive the name.
    - **Task name (string)**. The name of the scripted task that triggers the associated task. Use the parameter in associated tasks to receive the name.
    - **Exit code (integer)**. The exit code value that the scripted task returns. Use the parameter in associated tasks to receive the value.
    - **Console output (string)**. The console output that the scripted task writes. Use the parameter in associated tasks to receive the full path of the output.
    - **File output (string)**. The file output that the scripted task generates. Use the parameter in associated tasks to receive the full path of the output.

Edit a trigger

To edit a trigger, perform the following steps:

1. In **Triggers**, select the trigger.
2. Click **Edit** in the action bar.
3. Make changes as needed.
4. In **Summary**, verify that you made the changes as intended.
5. When you have finished, click **Done** to save and exit.

Clone a trigger

To clone a trigger, perform the following steps:

1. In **Triggers**, select the trigger.
2. Click **Clone** in the action bar.

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

3. Specify a name for the clone.
4. Optionally, specify additional information to help you identify the trigger.
5. Select a configuration set to clone the trigger to.
6. When you have finished, click **Done** to save and exit.

Manage associations

To manage associations for a trigger, perform the following steps:

1. In **Triggers**, select the trigger.
2. Click **Manage associations** in the action bar.
3. Select scripted tasks to associate them with the trigger or unselect scripted tasks to unassociate. If needed, use the search box to quickly search for a task.
4. When you have finished, click **Done** to save and exit.

When managing associations, keep the following in mind:

- To prevent endless looping, WEM supports up to 10 triggering times in a single loop chain. The following is an example, in which Task A triggers Task B, Task B triggers Task C, …, and Task K triggers Task L. Task K fails to trigger Task L — the loop terminates because the triggering times in this single loop chain have exceeded 10.

Delete a trigger

To delete a trigger, perform the following steps:

1. In **Triggers**, select the trigger.
2. Click **Delete** in the action bar.

NOTE:

If you delete a trigger with which scripted tasks are associated, it will no longer trigger those tasks.

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

Supportability matrix for triggers

The following table lists which triggers are supported for which tasks.

	SCRIPTED TASK	EXTERNAL TASK
Agent refresh		X
Reconnect		X
Logon		X
Logoff		X
Disconnect		X
Lock		X
Unlock		X
Machine startup	X	
Machine shutdown	X	
Scheduled	X	X
Process started		X
Process ended		X
Windows event	X	X
Cloud Health Check result	X	
Profile Management health check result	X	
Scripted task result	X	

Profiles

These settings let you replace user GPOs and configure user profiles:

- Citrix Profile Management Settings

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

- Microsoft USV Settings

Citrix Profile Management Settings

NOTE:

Some options work only with specific versions of Profile Management. Consult the Profile Management documentation for details.

Workspace Environment Management™ (WEM) supports all versions of Citrix Profile Management through the current version.

In the console (**Configuration Set > Profiles > Profile Management Settings**), you can configure all settings for the current version of Citrix Profile Management.

In addition to using WEM to configure Citrix Profile Management features, you can use Active Directory GPOs, Citrix Studio policies, or .ini files on the VDA. We recommend that you use the same method consistently.

Profile Management settings

When enabled, you can configure and apply your settings. Enabling this option creates Profile Management related registries in the user environment. The option controls whether WEM deploys the Profile Management settings you configure in the console to the agent. If disabled, none of the Profile Management settings are deployed to the agent.

By default, most Profile Management settings work only at the machine level. You can enable certain Profile Management settings to work at the user level, so that you can tailor the profile experience for specific users. See User-level Profile Management settings.

You can select tags to filter the profile management settings as needed. Settings associated with the selected tags get displayed and the rest are hidden.

- File-based. Settings that support file-based solution.
- Container-based. Settings that support container-based solution.
- App access control. Settings related to app access control.

When you switch between views, the selected set of tags get saved as a part of administrator preferences for further usage.

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

Quick setup

To quickly set up Profile Management, you can restore your settings from a backup or start with a template.

RESTORE FROM BACKUP

Backups containing Profile Management settings are shown. To upload backups containing Profile Management settings, see Back up Profile Management settings.

Select one backup from the list. Click **Preview** to see the settings and make adjustments as needed. Other types of settings (if any) in the backup are ignored.

NOTE:

- To restore Profile Management settings, you can also use the back up and restore feature.
- When restoring Profile Management settings from a backup, the SMB shares selected for relevant services to use are also restored.

START WITH TEMPLATE

IMPORTANT:

If you already have Profile Management configured, keep in mind that using a template overwrites all existing settings.

There are two types of user stores based on how profiles are handled:

- **File-based**. User profiles are fetched from the remote user store to the local computer on logon and written back on logoff.
- **Container-based**. User profiles are stored in profile containers. Those containers are attached on logon and detached on logoff.

To set up Profile Management quickly for your use case, choose a template.

User-level settings

This feature lets you configure certain Profile Management settings at the user level for customization and precise control. Use this feature to apply specific Profile Management settings to individual users or user groups, tailoring the profile experience as needed.

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

There are two ways to configure Profile Management settings at the user level:

- Use the Workspace Environment Management web console
- Use the user-level policy setting available with Profile Management

The web console offers a user-friendly, UI-based interface for configuring Profile Management user-level settings.

To configure user-level settings using the web console, complete the following steps.

- On the **Profile Management Settings** page, click the user-level settings link.
- On the user-level settings page, you can do the following:
  - Add configuration.
  - Set priority order for groups.
  - Toggle between the two views: **View by configuration** and **View by user/group**.

ADD CONFIGURATION

To add a configuration, complete the following steps.

1. Name your configuration.
2. Add individual users or user groups to which you want to apply this configuration.

   NOTE:

   Active Directory (AD) and Azure Active Directory (AAD) are supported.

3. Add settings that you want to apply to those users.

   NOTE:

   - Only settings available to users are shown in the UI.
   - You can edit or delete settings as needed.

Each time you add a configuration, it appears in **Actions > Group Policy settings > Others**. For your user-level settings to take effect, you must enable GPO processing (enable the **Process GPOs** option in Group Policy Settings.

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

SET PRIORITY ORDER FOR GROUPS

When a session starts, Profile Management determines which policy settings to apply, by prioritizing user settings over user group settings, and user group settings over machine settings.

You can set the priority order for groups to handle the situation (where a user belongs to multiple groups with conflicting settings) by completing the following steps.

1. Select **Enable priority order for groups** option.
2. Click **Add** to add groups.
3. Arrange the groups in descending order of priority.

   NOTE:

   When a user belongs to multiple groups with conflicting settings, the group that appears higher in the list takes precedence.

4. On completion, click **Save** to exit.

VIEW BY CONFIGURATION OR USER/GROUP

You can toggle between the two views to view the user-level settings categorized by user/group, or by configuration.

Folder redirection

This feature lets you configure rule sets to redirect the paths of local folders to new locations. Each rule set specifies where you want to redirect the folders based on the users accessing them. A rule set mainly includes:

- **Redirection rules.** Specify which local folders you want to redirect and where to redirect them (such as a network location).
- **Assignments.** Specify the users to whom you assign the redirection rules.

To add a rule set for a configuration set, follow these steps:

1. Go to the **Profile Management Settings** page of the target configuration set.
2. Click the **Folder redirection** link above the search box.
3. On the **Folder redirection** page that appears, click **Add rule set**.
4. On the **Add rule set** page that appears, follow these steps to complete the settings:

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

a. On the **Redirection rules** page, select the folders to redirect, specify the redirection destinations, and then click **Next**.

   - You can redirect a folder to a network location, the user's home directory (only for certain folders), or the local user profile location.
   - By default, the **Move contents to new location** option is selected, identifying that after you set or modify a redirection target path, contents from the previous path are automatically moved to the new one. To prevent this behavior, clear the option.

b. On the **Assignments** page, select users, groups, or OUs to which you want to assign the redirection rules, and then click **Next**. Default groups include **Everyone** and **Administrators**. To add a group, click **Add new target**.

c. On the **Additional settings** page, specify the following settings for the rule set, and then click **Next**:

   - **Grant access to administrators:** Whether to grant the **local Administrators** group access to the redirection target paths. By default, those paths are accessible exclusively to the profile owner.
   - **Grant access to specific users and groups:** Whether to grant specific users and groups access to the redirection target paths. After selecting this option, click Add user/group to specify the users and groups as needed.
   - **Include domain name:** Whether to include the %userdomain% environment variable as part of the UNC path.
   - Set a priority for this rule set by entering a numeric value. Greater numbers indicate higher priority. When multiple rule sets apply to the same target, the one with the higher priority wins.

d. Enter a descriptive name for this rule set and review settings. To adjust, click the corresponding step in the left pane.

e. Click **Done**.

NOTE:

Currently, end users must log on twice for newly deployed rule sets to take effect.

Basic settings

Get started with Profile Management by applying basic settings. Basic settings include processed groups, excluded groups, user store, and more.

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

Enable Profile Management. Controls whether to enable the Profile Management service on the agent machine. If disabled, the Profile Management service does not work.

You might want to disable Profile Management completely so that settings already deployed to the agent will no longer be processed. To achieve the goal, do the following:

1. Clear the **Enable Profile Management** checkbox and wait for the change to apply automatically or apply the change manually for immediate effect.

   NOTE:

   The change takes some time to take effect, depending on the value you specified for **SQL settings refresh delay (min)** in Advanced Settings. For the change to take effect immediately, refresh agent host settings and then reset Profile Management settings for all related agents. See Administration.

2. After the change takes effect, disable **Profile Management Settings**.

Set processed groups. Lets you specify which groups are processed by Profile Management. Only the specified groups have their Profile Management settings processed. If left empty, all groups are processed.

Set excluded groups. Lets you specify which groups are excluded from Profile Management.

Process logons of local administrators. If enabled, local administrator logons are treated the same as non-administrator logons for Profile Management.

Set path to user store. Lets you specify the path to the user store — the central location for Citrix user profiles. Enter an absolute UNC path or a path relative to the home directory. Example path:

- `\\<IP address or FQDN>\<user store directory>\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!`

Migrate user store. Lets you specify the path to the folder where the user settings (registry changes and synchronized files) were saved. Enter the user store path that you previously used. Use this option along with the **Set path to user store** option.

Enable active write back. If enabled, profiles are written back to the user store during the user session, preventing data loss.

- **Enable active write back registry**. If enabled, registry entries are written back to the user store during the user session, preventing data loss.

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

- **Enable active write back on session lock and disconnection**. If enabled, profile files and folders are written back only when a session is locked or disconnected. With both this option and the **Enable active write back registry** option enabled, registry entries are written back only when a session is locked or disconnected.

Enable offline profile support. If enabled, profiles are cached locally for use while not connected.

Profile container

Configure profile container settings. Profile containers are VHDX disks stored on the network and attached during logon and detached during logoff.

Enable Profile Container. Lets you add the folders you want to include in the profile container. To put an entire user profile in its profile container, add an asterisk (*) instead. If enabled, Profile Management maps the listed folders to the profile disk stored on the network, thus eliminating the need to save a copy of the folders to the local profile. Specify at least one folder to include in the profile container.

- **Enable local caching for profile container**. If enabled, each local profile serves as a local cache of its profile container. This option requires you to put an entire user profile in its profile container.
- **Log off users when profile container is not available during logon.** Lets you specify whether to force log-off users when the profile container is unavailable during user logon. Enabling this option displays a notification message to users and logs them off after they click OK.

Enable folder exclusions. If enabled, Profile Management excludes the listed folders from the profile container. Specify at least one folder to exclude from the profile container.

Enable file exclusions. If enabled, Profile Management excludes the listed files from the profile container. Specify at least one file to exclude from the profile container.

Enable folder inclusions. If enabled, Profile Management keeps the listed folders in the profile container when their parent folders are excluded. Folders on this list must be subfolders of the excluded folders. This means that you must use this option with the **Enable folder exclusions** option. Specify at least one folder to include in the profile container.

Enable file inclusions. If enabled, Profile Management keeps the listed files in the profile container when their parent folders are excluded. Files on this list must be contained in the excluded folders. This means that you must use this option with the **Enable folder exclusions** option. Specify at least one file to include in the profile container.

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

TIP:

When adding files or folders, you can use wildcards. For more information, see Wildcard support.

When adding profile container content, exclusions, and inclusions, you can add them individually and in bulk. When adding them in bulk, enter paths separated by line breaks. After that, click **Run validation** to validate items you are about to add. Only valid items can be added. Invalid items are skipped.

Also, you can have a hierarchical view of the profile container content, exclusions, and inclusions. To do that, click **View hierarchy**.

Enable VHD auto-expansion for profile container. If enabled, when the profile container reaches 90% utilization, it automatically expands by 10 GB, with a maximum capacity of 80 GB. Depending on your needs, you can adjust the default auto-expansion settings using the following options:

- **Auto-expansion trigger threshold (%).** Lets you specify the utilization percentage of storage capacity at which the profile container triggers auto-expansion.
- **Auto-expansion increment (GB).** Lets you specify the amount of storage capacity (in GB) by which the profile container automatically expands when auto-expansion is triggered.
- **Auto-expansion limit (GB).** Lets you specify the maximum storage capacity (in GB) to which the profile container can automatically expand when auto-expansion is triggered.

Set users and groups to access profile container. Lets you specify which AD domain users and groups have Read & Execute permission on profile containers. By default, a profile container is accessible only to its owner.

Profile handling

Specify how Profile Management handles user profiles.

Delete locally cached profiles on logoff. If enabled, locally cached profiles are deleted when the user logs off.

- **Set delay before deleting cached profiles**. Lets you specify a delay (in seconds) before cached profiles are deleted on logoff. Supported values: 0–600.

Enable migration of existing profiles. If enabled, existing Windows profiles are migrated to Profile Management on logon. Specify the type of user profiles to migrate if the user store is empty. Types include:

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

- Local and roaming
- Local
- Roaming

Automatic migration of existing application profiles. If enabled, existing application profiles are migrated automatically. Profile Management performs the migration when a user logs on and when there are no user profiles in the user store.

Enable local profile conflict handling. Configures how WEM handles cases where Profile Management and Windows profiles conflict. Specify what to do if both a local Windows user profile and a Citrix user profile exist in the user store:

- Use local profile
- Delete local profile
- Rename local profile

Enable template profile. Lets you enter a template profile path. If enabled, Profile Management uses the specified template profile. You can configure additional settings as follows:

- **Template profile overrides local profile**. If enabled, the template profile overrides local profiles.
- **Template profile overrides roaming profile**. If enabled, the template profile overrides roaming profiles.
- **Use template profile as Citrix mandatory profile for all logons.** If enabled, the template profile overrides all other profiles.

Advanced settings

Control the advanced configuration of Profile Management.

APPLICATIONS

Enable search index roaming for Microsoft Outlook users. If enabled, the user-specific Microsoft Outlook offline folder file (*.ost) and Microsoft search database are roamed along with the user profile. This feature improves the user experience when searching mail in Microsoft Outlook.

- **Outlook search index database – backup and restore**. If enabled, Profile Management automatically saves a backup of the last known good copy of the search index database. When there is a corruption, Profile Management reverts to that copy. As a result, you no longer must manually reindex the database when the search index database becomes corrupted.

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

- **Enable concurrent session support**. Provides native Outlook search experience in concurrent sessions. If enabled, each concurrent session uses a separate Outlook OST file.
    - **Maximum number of VHDX disks for storing Outlook OST files**. Lets you specify the maximum number of VHDX disks for storing Outlook OST files. If unspecified, only two VHDX disks can be used to store Outlook OST files (one file per disk). If more sessions start, their Outlook OST files are stored in the local user profile. Supported values: 1–10.

Enable OneDrive container. If enabled, Profile Management roams OneDrive folders with users by storing the folders on a VHDX disk. The disk is attached during logons and detached during logoffs.

Enable UWP app roaming. If enabled, UWP (Universal Windows Platform) apps roam with users. As a result, users can access the same UWP apps from different devices.

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 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.

Enable use of application definition files. Lets you enter the path to the definition files. If enabled, only the settings included in the definition file are synchronized. Specify a folder where the Citrix virtual apps optimization definition files are located. For more information about creating definition files, see Create a definition file.

VHD SETTINGS

Default capacity of VHD containers (GB). Lets you specify the default storage capacity (in GB) of each VHD container.

Customize storage path for VHDX files. Lets you specify a separate path to store VHDX files. By default, VHDX files are stored in the user store. Policies that use VHDX files include the following: Profile container, Search index roaming for Outlook, and Accelerate folder mirroring. If enabled, VHDX files of different policies are stored in different folders under the storage path.

Enable multi-session write-back for profile containers. Lets you enable multi-session write-back for both FSLogix Profile Container and Citrix Profile Management profile container. If the same user launches multiple sessions on different machines, Profile Management synchronizes and saves changes made in each session to the user's profile container.

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

Enable multi-session support for machine hibernation. If enabled, VHDX disks used by a hibernated session are not reassigned to other sessions. This allows the user profile to be resumed after the machine recovers from hibernation, ensuring session continuity.

Enable VHD disk compaction. If enabled, VHD disks are automatically compacted on user logoff when certain conditions are met. This policy enables you to save the storage space consumed by the profile container, OneDrive container, and mirror folder container. Depending on your needs and the resources available, you can adjust the default VHD compaction settings and behavior using the **Disable defragmentation for VHD disk compaction**, **Set free space ratio to trigger VHD disk compaction**, and **Set number of logoffs to trigger VHD disk compaction** options in Advanced settings.

- **Set freeable space ratio to trigger VHD disk compaction**. Applicable when Enable VHD disk compaction is enabled. Lets you specify the freeable space ratio to trigger VHD disk compaction. When the freeable space ratio exceeds the specified value on user logoff, disk compaction is triggered.
    - Freeable 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.
- **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.
- **Set 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, the disk compaction is triggered again.

Enable exclusive access to profile container. If enabled, the profile container allows one access at a time.

Enable exclusive access to OneDrive container. If enabled, the OneDrive container allows one access at a time.

USER STORE

Set number of retries when accessing locked files. Configures the number of times the WEM agent retries accessing locked files. Supported values: 0–100.

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

Replicate user stores. If enabled, Profile Management replicates a user store to multiple paths on each logoff, in addition to the path that the **Set path to user store** option specifies. To synchronize to the user stores files and folders modified during a session, enable active write-back. Enabling the option can increase system I/O and might prolong logoffs.

By default, when multiple user stores are available, Profile Management selects the store with the latest profile data. If more than one store has the latest profile, Profile Management selects the one configured earliest. With the **User store selection method** option, you can now enable Profile Management to select the store with the best access performance.

When you enable the **Replicate user stores** policy for the container-based profile solution, the **Enable in-session profile container failover among user stores** policy is automatically enabled to ensure profile redundancy for the entire session. With this policy enabled, if Profile Management loses connection to the active profile container during a session, it automatically switches to another available one. If you disable this policy, profile container failover occurs only at user logon.

NOTE:

Enabling this policy requires that only the profile container is enabled in your deployment. If any other containers, such as **OneDrive**, **UWP**, **Outlook**, **folder mirroring**, or **Profile streaming for pending area**, is enabled, this policy doesn't take effect.

Limit number of user stores synced at logoff By default, profiles are synchronized to all user stores during user logoff, which can extend the logoff process and delay subsequent logons. Enabling this option lets you specify how many user stores are synced during logoff. The specified number includes the main user store, while the remaining user stores (if any) are synced after logoff is complete. Supported values: 1–8.

Enable credential-based access to user store. If disabled, Profile Management impersonates the current user to access user stores. Thus, make sure that the current user can directly access the user stores. If enabled, Profile Management accesses the user stores on behalf of the user through the connections configured for relevant services in Advanced Settings > File Shares > SMB shares. (When needed, Profile Management accesses the selected SMB shares that host the user stores.) Enabling this setting lets you put user stores in file shares (for example, Azure Files) that the current user has no permission to access. When using this option, consider the following:

- To add SMB shares hosting your user stores, go to **Advanced Settings > File Shares > SMB shares**.

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

- SMB shares you select in **File Shares** for relevant services appear here. Profile Management accesses the selected SMB shares as needed.

IMPORTANT:

Disabling this setting deletes all user store connections that the WEM agent previously established.

- When adding or editing credentials, complete the following fields:
  - **Server share**. Enter a UNC path that specifies a server share.
  - **User name**. Enter the name in the form `domain\username`.
  - **Password**. Enter the password to be used to access the server share.
  - **Show password**. Control whether to show or hide the password.

OTHER OPTIONS

Disable automatic configuration. If enabled, dynamic configuration is disabled.

Enable asynchronous processing for user Group Policy on logon. If enabled, Profile Management roams with users a registry value that Windows uses to determine the processing mode for the next user logon — synchronous or asynchronous processing mode. If the registry value does not exist, synchronous mode is applied. Enabling the option ensures that the actual processing mode is applied each time users log on. If disabled, asynchronous mode can't 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 option is enabled.

Process Internet cookie files on logoff. If enabled, stale cookies are deleted on logoff.

Alert user when profile size exceeds quota. If enabled, users receive a notification message when their profile size exceeds a quota. With this feature, you can customize the quota limit and the notification content based on the default settings. The supported quota range is 0–100,000 MB.

Set profile loading timeout. Lets you configure how long Citrix Profile Management waits for a user profile to load before switching to a temporary profile. It helps ensure a smoother, more efficient logon experience tailored to your needs. The valid timeout range is 0–1,800.

Typical use cases:

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

- **Non-persistent multi-session VDAs running Citrix Apps.** In such environments, loading user-specific data might not be necessary. You can set the timeout to 0 seconds to bypass profile loading and use a temporary profile.
- **Network disruption handling.** This policy mitigates network disruptions by automatically switching to a temporary profile if profile loading exceeds the timeout setting.

NOTE:

- This setting doesn't apply to the *profile migration* and *profile reset* processes.
- We recommend setting the timeout to greater than 10 seconds unless there is a strong need. A short timeout might cause users to unexpectedly log on to a temporary profile, even in normal conditions.

Log off user if problems occur. If enabled, users are logged off rather than switched to a temporary profile if a problem occurs.

Join the Citrix Customer Experience Improvement Program. If enabled, Profile Management uses the Customer Experience Improvement Program (CEIP) to help improve the quality and performance of Citrix products by collecting anonymous statistics and usage information. For more information on the CEIP, see About the Citrix Customer Experience Improvement Program (CEIP).

File deduplication

Specify files that you want to include in the shared store for deduplication.

Identical files can exist among various user profiles. Separating those files from the user store and storing them in a central location saves storage space by avoiding duplicates.

You can specify files that you want to include in the shared store on the server hosting the user store. Specify the file names with paths relative to the user profile.

Enable file deduplication. If enabled, Profile Management generates the shared store automatically. It then centrally stores the specified files in the shared store rather than in each user profile in the user store. Doing so reduces the load on the user store by avoiding file duplication, thus reducing your storage cost.

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

TIP:

When adding files or folders, you can use wildcards. For more information, see Wildcard support.

When adding inclusions and exclusions, you can add them individually and in bulk. When adding them in bulk, enter paths separated by commas or line breaks. After that, click **Run validation** to validate items you are about to add. Only valid items can be added. Invalid items are skipped.

By default, Profile Management deduplicates files from profile containers only when those files are larger than 256 MB. If necessary, you can increase this threshold size by providing a larger value for **Deduplicate files this size or larger (MB)**.

Enable file exclusions. If enabled, Profile Management excludes the specified files from the shared store. This option is available only after you enable the **Enable file deduplication** option. Specify at least one file to exclude from the shared store.

Streamed user profiles

Specify how Profile Management processes streamed user profiles.

Enable profile streaming. If disabled, none of the settings in this section are processed.

- **Enable profile streaming for folders**. If enabled, folders are fetched only when they are being accessed, thus eliminating the need to traverse all folders during logon. This saves bandwidth and reduces the time to synchronize files.

Always cache. If enabled, files of the specified size (in MB) or larger are always cached. Supported values: 0–20,000.

Set timeout for files in pending area when user store remains locked. Lets you specify the number of days after which user's files are written back to the user store from the pending area when the user store remains locked. Supported values: 1–30.

Set streamed user profile groups. Lets you add user groups for which streamed profiles are used.

Set excluded folders. If enabled, Profile Management does not stream folders in this list, and all the folders are fetched immediately from the user store to the local machine when users log on.

Enable profile streaming for pending area. If enabled, files in the pending area are fetched to the local profile only when they are requested. This ensures optimum logon experience in

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

concurrent session scenarios. 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 option is disabled. All files and folders in the pending area are fetched to the local profile during logon.

Log settings

Configure Profile Management logging.

Enable logging. Enables or disables logging of Profile Management operations.

Include more information in the logs. Lets you specify more information (or types of events) in the logs, including:

- Common warnings
- Common information
- File system notifications
- File system actions
- Registry actions
- Registry differences on logoff
- Active Directory actions
- Policy values on logon and logoff
- Logon
- Logoff
- Personalized user information

Set maximum size of the log file. Lets you specify a maximum allowed size for the Profile Management log file. If the log file grows beyond the maximum size, its backup (.bak) is deleted, the log file is renamed to .bak, and a new log file is created. Supported values: 1–100.

Set path to log file. Lets you specify the location where the log file is created.

Registry

Specify which registry keys are included or excluded from Profile Management processing.

NTUSER.DAT backup. If enabled, Profile Management maintains a last known good backup of the NTUSER.DAT file. If Profile Management detects corruption, it uses the last known good backup copy to recover the profile.

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

Enable default registry exclusions. Provides a default list of registry keys in the HKCU hive that are not synchronized to the user profile. If enabled, registry settings that are selected in this list are forcibly excluded from Profile Management profiles.

Enable registry exclusions. If enabled, registry settings you add are forcibly excluded from Profile Management profiles.

Enable registry inclusions. If enabled, registry settings you add are forcibly included in Profile Management profiles.

App access control

Add rules to control end user access to applications or to enforce redirections for files, folders, registry values, and keys:

1. Select the **App access control** category next to the Search box.
2. Select **Enable app access control**.
3. Click **Add rules** to add rules.
4. When adding rules, you can browse to a `.rule` file generated using Citrix Environment Tool Hub > Rule Generator for App Access Control or paste data from the clipboard. After adding rules, click **Manage** to view, edit, or update the rules. When viewing rules, you can switch between category view and raw data view.

There are two ways you can create rules:

- GUI-based tool - Citrix Environment Tool Hub > Rule Generator for App Access Control
- PowerShell tool – available with the Profile Management installation package

Example: Suppose you need to provide applications (App1, App2, App3, and App4) in desktops assigned to users from three departments: HR, Sales, and R&D.

- Only users from the HR department can access App1.
- Only users from the Sales department can access App2.
- Only users from the R&D department can access App3.
- All users can access App4.

To achieve the goal, you can deploy rules using just one image. The image contains applications App1, App2, App3, and App4. You then set up application rules as follows:

- **Create a rule for App1**. Add objects associated with App1 and users from the Sales and R&D departments.

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

- **Create a rule for App2**. Add objects associated with App2 and users from the HR and R&D departments.
- **Create a rule for App3**. Add objects associated with App3 and users from the HR and Sales departments.

Wildcard support

When adding files or folders, you can use wildcards. Wildcards in file names are applied recursively while wildcards in folder names are not. You can use the vertical bar (\|) to restrict the policy only to the current folder so that the policy does not apply to its subfolders.

Examples:

- `AppData*.tmp` excludes all files with the extension .tmp in the folder `AppData` and its subfolders.
- `AppData*.tmp|` excludes all files with the extension .tmp in the folder `AppData`.
- `Downloads*\a.txt` excludes `a.txt` in any immediate subfolder of the `Downloads` folder. Remember: wildcards in folder names are not applied recursively.
- `Downloads*` excludes all immediate subfolders of the `Downloads` folder.

Microsoft USV Settings

These settings allow you to optimize Microsoft User State Virtualization (USV).

Roaming profiles configuration

These settings allow you to configure Workspace Environment Management's integration with Microsoft roaming profiles.

Process User State Virtualization Configuration. Controls whether the agent processes USV settings. If disabled, no USV settings are processed.

Exclude Administrators. If enabled, USV settings you configure do not apply to administrators. When using this option, consider the following:

- Settings on the **Roaming Profiles Configuration** and **Roaming Profiles Advanced Configuration** tabs are machine-level and still apply regardless of whether the option is enabled.
- Settings on the **Folder Redirections** tabs are user-level. The option controls whether the settings apply to administrators.

Set Windows Roaming Profile Path. Lets you specify the path to your Windows profiles.

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

Set RDS Roaming Profiles Path. Lets you specify the path to your RDS roaming profiles.

Set RDS Home Drive Path. Lets you specify the path to your RDS home drive and the drive letter it appears with in the user environment.

Roaming profiles advanced configuration

The following are the advanced roaming profile optimization options.

Enable Folder Exclusions. If enabled, the listed folders are not included in a user's roaming profile. This allows you to exclude specific folders known to contain large amounts of data which the user does not need to have as part of their roaming profile. The list is pre-populated with default Windows 7 exclusions, and can be pre-populated with default Windows XP exclusions instead.

Delete Cached Copies of Roaming Profiles. If enabled, the agent deletes cached copies of the roaming profiles.

Add Administrators Security Group to Roaming User Profiles. If enabled, the Administrators group is added as owner to roaming user profiles.

Do Not Check for User Ownership of Roaming Profiles Folders. If enabled, the agent does not check to see if the user owns the roaming profiles folder before acting.

Do Not Detect Slow Network Connections. If enabled, connection speed detection is skipped.

Wait for Remote User Profile. If enabled, the agent waits for the remote user profile to be fully downloaded before processing its settings.

Profile Cleansing. Opens the **Profiles Cleanser** wizard, which allows you to delete existing profiles.

To delete existing profiles, click **Browse** to navigate to the folder where user profiles are stored, click **Scan Profiles Folder**, and then select the profile folder that you want to clean up on the Profiles Cleanser window. After that, click **Cleanse Profiles** to start the cleanup.

Cleanse Profiles. This button cleans the selected profiles per the Folder Exclusion settings.

Scan Profiles Folder. Scans the specified folder with the specified recursion settings to find user profiles, then displays all profiles found.

Profiles Root Folder. The root folder of your user profiles. You can also browse to this folder if you like.

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

Search Recursivity. Controls how many levels of recursion the user profile search goes through.

Folder redirection

Process Folder Redirection Configuration. This check box toggles whether the agent processes folder redirections. If it is cleared, no folder redirections are processed. Select the options to control whether and where the user's folders are redirected.

Delete Local Redirected Folders. If enabled, the agent deletes the local copies of the folders selected for redirection.

Scripted Tasks

TIP:

Scripted tasks work at a machine level. To run tasks at a user session level, use External tasks instead.

This page lets you configure and automate scripted tasks to suit your environment management needs.

Create a scripted task

Scripts are categorized into two types: **Built-in Scripts** and **Custom Scripts**. Each type provides two viewing modes: a **Script View** and a **Task View**. All scripted tasks are executed at the configuration set level.

To create a task from a script, follow these steps:

1. On the **Scripted Tasks** page, select **Script View**, locate the specific script, then click the **Create task** (+) icon.
2. In the **Create task** wizard, configure the following settings:
   - General
   - Triggers
   - Parameters
   - Output
3. Click **Done**.

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

NOTE:

After you create a scripted task, you can manage it directly from the script list. Expand the script to display its tasks, then hover over a task row to access the **View**, **Edit**, and **Delete** action icons.

General

Configure the following settings on the **General** page:

- **Enable this task**. Choose whether to enable (**Yes**) or disable (**No**) the task for the current configuration set. If disabled, the agent does not process the task.
- **Verify signature**. Choose whether to verify the signature before running the task. Signature verification is mandatory when the scripted task is granted full access.
- **Task timeout**. Choose whether to set a timeout (in minutes) for the task. When the timeout occurs, the task is forced to end. Supported values: 1–60. We recommend setting a timeout for the task. Otherwise, the task might be left running, preventing other tasks from running.
- **Filter**. Choose whether to contextualize the task by selecting a filter. With a filter selected, this task runs only when all conditions in the filter are met. When selecting a filter, consider the following:
    - If the filter contains conditions that do not apply to scripted tasks, the agent skips those conditions when evaluating the filter before running the task. For a complete list of conditions that do not apply to scripted tasks, see Conditions not applicable to machine settings.

Triggers

Configure the following settings on the **Triggers** page:

- Configure triggers for the task. You can do the following:
    - Select triggers that you want to associate with the task. When activated, those triggers start the task in the user environment.
    - Choose whether to show only triggers that apply to this task.
    - Create a new trigger. See Create a trigger.

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

> **NOTE:**
>
> To edit existing triggers, go to Triggers.

Parameters

Configure the following settings on the **Parameters** page:

- **Pass parameters to the scripted task**. Choose whether to pass parameters to the scripted task. When enabled, lets you provide inputs as parameter variables in the scripted task at runtime. The benefit is that you can control how the scripted task behaves without changing the underlying code. The following parameter types are available:
  - **Integer**. Example: `123`.
  - **String**. Example: `hello world`.
  - **Boolean**. Ture or False.
  - **Character**. Example: `c`.
  - **Switch**. Ture or False.
  - **Double**. Example: `1.023`.
  - **Date and time**. Example: `YYYY-MM-DD HH:mm:ss`.
  - **File path**. Enter a path that you want to pass to the `System.IO.FileInfo` class. Environment variables are supported. The path must not include the following characters: `* ? < >`.

> **NOTE:**
>
> - You can configure up to 20 parameters.
> - The name field is optional except for parameters of the "switch" type.
> - PowerShell supports partial parameter names. When using a partial parameter name, make sure that the name is unique — disambiguate it from existing parameter names. Example: The following parameter names are the same for PowerShell: `-t`, `-ti`, and `-title`. In this case, supply enough letters of the parameter name to distinguish it from the other parameters.

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

Output

Configure the following settings on the **Output** page:

- **Output files.** Choose whether you want to collect files that the task outputs. If selected, includes output file content in reports generated for the task. You can then view the output file content in the reports without the need to access the output files in the user environment.
- **Output highlights**. Choose whether you want to highlight certain content in the output file content and the console output.
    - **Highlight keywords.** Specify keywords that you want the report to highlight. You can type multiple keywords, separated by commas. After typing a keyword, press **Enter** to continue. If specified, report contents that match your keywords will be highlighted in the **Output file content** and **Console output** sections in the generated reports.
    - **Highlight regular expression matches**. Enter a regular expression that describes the content you want to highlight. The regular expression must conform to the .NET regular expression library syntax, which is PCRE compatible. For more information, see the Microsoft documentation: `<https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference>`.
        - **Regular expression.** Enter a regular expression that describes the content you want to highlight.
        - **Ignore case**. Choose whether content must exactly match the case.
        - **Use multiline matching**. Choose whether to use multiline matching, where \^ and \$ match the beginning and end of each line, instead of the beginning and end of the entire output content.
        - **Capture only named groups**. Choose whether to capture only named groups. Captured groups are defined by using parentheses in the regular expression pattern. Named groups are explicitly assigned a name or a number by the `(?<name> subexpression)` syntax.
        - **Number of lines to include as context clues**. Specify the number of lines before and after the match you want to include in the highlight as context clues. Supported values: 1–10.
        - **Include only regular expression matches in reports**. Controls whether to include the entire output content in reports or only content that matches the regular expression. Enabling this option reduces the amount of data transmitted to Citrix Cloud. With the option enabled, the Highlight keywords feature has no content to show regardless of the specified keywords.

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

- **Advanced options**.
  - **Collect output even if runtime errors occur**. Controls whether to collect output file content and console output even if errors occur while running the task.

View reports for a scripted task

1. On the **Scripted Tasks** page, click the tasks dropdown menu in the script row to expand its task list.
2. Hover over a task to display the action icons.
3. Click the **View reports** icon.

As a result, you are taken to the **Monitoring > Reports** page, where you see the reports (if any) related to the task. Click the ellipsis to view more detailed information. For details, see Reports.

NOTE:

To run a scripted task that's set to **Run as logged-on user**, select a recently connected agent in **Monitoring > Administration > Agents**, and then select **More > Run scripted task**.

App package delivery

This feature provides app delivery capabilities by allowing you to configure app installation/uninstallation tasks for agent machines that support WEM agent installers and custom `.exe` installers. You can add app packages with installers stored in their SMB shares, specify the command, execution criteria, and relevant settings for the package. You can then configure delivery tasks to deploy applications to the user environment, with schedules and rules to handle the execution. App packages are shared across all configuration sets. You can configure delivery tasks with app packages in each configuration set. Only machine-wide installers are supported.

For the cloud environment, only one built-in WEM agent package is available. You can create a delivery task, edit a package, and also delete a package using the ellipses associated with the WEM agent package. All packages in use cannot be deleted. You can also sort the app packages and delivery tasks in alphabetical order or based on the date of creation.

Configure storage location

To configure the current configuration set's storage location, complete the following steps:

1. In the **Storage location** section, click the **Edit** icon.
2. On the **Storage location** page that appears, click **Add New**.

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

3. On the **Add SMB share** page that appears, enter the UNC path for an SMB share and the credentials of an administrator with permission to access that share, and then click **Done**.

   NOTE:

   Do not use administrator credentials. We recommend setting up a dedicated SMB username and password with read-only access.

4. Repeat step 3 to add more SMB shares if needed.
5. In **SMB share** drop-down list, select the one that stores your installers.
6. Click **Save**.

NOTE:

The storage location specified applies to only the current configuration set. Ensure to store your installers in the following path in your SMB share `(Storage location)\Citrix\WEM\AppPackages` and click **Save**.

Add app package

To add an app package, complete the following steps.

1. Click **Add app package > EXE** to access the **Add app package** page. This page lists **Basic information**, **Execution criteria**, and **Settings** in the tree structure.

   - **Execution criteria**. You must specify the criteria that determine when the app package must run. The execution criteria is classified into **File or folder existence**, **File creation date**, **File modification date**, **File version**, **File size**, **Registry key existence**, **Registry value existence**, and **Registry value**. Ensure to configure the Criteria to prevent errors caused by the repeated execution of packages.

     - On a 64-bit version of Windows, when a file or folder path is configured within the `Program Files` directory, the WEM agent will automatically check both the 32-bit `Program Files (x86)` and the 64-bit `Program Files` folders, if you choose the **Criterion type** as **File or folder existence**. For instance, if the configured path is `C:\Program Files\Test`, the WEM agent verifies the existence of the following two paths: `C:\Program Files (x86)\Test` and `C:\Program Files\Test`. Similarly, if the configured path is `C:\Program Files (x86)\Test`, the WEM agent checks both

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

`C:\Program Files (x86)\Test` and `C:\Program Files\Test`. This ensures compatibility and accessibility across both 32-bit and 64-bit applications.

- If you choose the **Criterion type** as **File size**, the WEM agent calculates the file size in kilobytes (KB) by considering the whole number part and ignoring decimal values. For instance, if a file is 46,913,080 bytes in size, the WEM agent calculates its size in KB as 45,813 KB (46,913,080 divided by 1024 is equal to 45,813.554, and the decimal portion, **.554**,' is disregarded).
- If you choose the **Criterion type** as **Registry key existence**: In 64-bit versions of Windows, the registry is divided into 32-bit and 64-bit keys. When you configure a registry key as the 64-bit version, the WEM agent attempts to confirm the existence of the registry key-in both the 32-bit and 64-bit versions. However, if you configure a registry key as the 32-bit version, the WEM agent only verifies its presence in the 32-bit version. For instance, if your configured registry key is `HKEY_LOCAL_MACHINE\Software\test`, the criteria is met if either of the following registry keys exists: `HKEY_LOCAL_MACHINE\Software\test` or `HKEY_LOCAL_MACHINE\Software\WOW6432Node\test`. If your configured registry key is `HKEY_LOCAL_MACHINE\Software\WOW6432Node\test`, the criterion is met if `HKEY_LOCAL_MACHINE\Software\WOW6432Node\test` exists.

2. Update the fields listed under each option.
3. After installing or uninstalling some packages, you can select the **Reboot machine after execution** checkbox under **Settings**, if necessary.

   - If the application package triggers a machine reboot during installation, the status is recorded as an **Unexpected Reboot** as you cannot retrieve the precise result. Ensure to incorporate a parameter in the installation command to prevent a reboot, and also select the **Reboot machine after execution** check box to address this issue.
   - If the application package requires ongoing operation after a reboot, the result of the package may not be entirely accurate. This is because WEM cannot retrieve the result of a package that was not initiated by WEM.

4. Ensure to specify return codes to indicate the success status. You can define the return code for your packages under **Settings**.

Create a WEM agent upgrade task

To create a WEM agent upgrade task, complete the following steps.

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

1. Choose the **Create delivery task > WEM agent upgrade** task type to access the **Create delivery task** page. This page lists **Basic information** and **Schedule and rules** in the tree structure.
2. Update the fields listed under each option.
3. By default, the **Latest version** is selected under **Upgrade to**.
4. For agents running in UI mode, enabling the **Allow users to upgrade agent manually** makes the **Upgrade** option available in the agent user interface. You can use this option to upgrade the agents to the version specified in the drop-down menu (last three versions). This setting is a sub-set of the WEM agent upgrade delivery task. This means that manual upgrade task upgrades to the version specified by the WEM agent upgrade delivery task subject to the set Rules.
5. Ensure to set the **Schedule** by specifying the time window and the day you need the delivery task to run as the delivery task does not run manually without any set schedule. The start and end times must be set at least two hours apart and on the same day.
6. You can also set **Rules** to determine which agent must run the task. You can select **Match all** or **Match any** from **Machine catalog name**, **Delivery group name**, **Device name**, **IP address**, **OS platform type**, **OS version**, and **Persistent machine** rules.

NOTE:

The following WEM agent upgrade settings may result in compatibility issues while performing an agent upgrade, with versions older than 2310.

- **Day of week** is configured in schedule settings.
- Rules are configured with a rule other than **Persistent machine**.
- **Match any** is selected in Rules.
- Rules are configured without a Schedule.

Limitation

- When you upgrade a WEM agent, the WEM agent versions earlier than 2310 can only use the first created task among all the currently available agent upgrade tasks.

Create a custom task

To create a custom task, complete the following steps.

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

1. Choose the **Create delivery task > Custom** task type to access the **Create delivery task** page. This page lists **Basic information** and **Schedule and rules** in the tree structure.
2. Update the fields listed under each option.
3. You can choose the required app packages and arrange them in the order that you want them to run.
4. To avoid blocking the other scheduled tasks, ensure to choose **Continue if failed** under **Task content** to continue with the seamless processing of other app packages even if one of the selected package functions (install/uninstall) fails.
5. If you select the **Wait until the end to reboot** checkbox, the reboot settings for individual app packages are ignored and the machine will reboot when the entire list of tasks finish running.
6. Selecting the **Run once** checkbox enables you to run the scheduled task only once.
7. Ensure to set the schedule by specifying the time window and the day you need the delivery task to run as the delivery task does not run manually without any schedule set.
8. The maximum execution time for each package is 60 minutes. Otherwise, the package times out and gets terminated.

For more information, see Reports, Agents, and Advanced Settings.

Advanced Settings

Use these settings to control how and when the Workspace Environment Management™ (WEM) agent processes actions.

Agent settings

This page lets you configure the WEM agent behavior.

Agent options

Configure settings for the agent.

Agent launch behavior:

- **Launch agent on logon**. Controls whether the agent runs on logon.
- **Launch agent on reconnection**. Controls whether the agent runs when a user reconnects to a machine where the agent is running.
- **Launch agent for administrators**. Controls whether the agent runs when a user is an administrator.

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

- **Enable desktop compatibility mode**. Ensures that the agent is compatible with desktops on which it is running. This setting is necessary for the agent to launch when the user logs on to a session.
- **Run only CMD agent in published applications**. If enabled, the agent launches in CMD mode rather than in UI mode in published applications. CMD mode displays a command prompt instead of an agent splash screen. For more information about CMD and UI mode, see Agent in CMD and UI mode.

Agent launch exclusions:

- **Do not launch agent for specified groups**. If enabled, the Citrix WEM Agent Host is not launched for any user belonging to the specified user groups.
- **Launch agent only for specified groups**. If enabled, the Citrix WEM Agent Host is launched only for users belonging to the specified user groups.

Agent logs:

- **Enable agent logging**. If enabled, the agent outputs the agent log file.
- **Debug mode**. Controls whether to enable verbose logging for the agent.

Refresh:

- **Refresh environment settings**. If enabled, the agent triggers a refresh of user environment settings when an agent refresh occurs. For information about environment settings, see Environment Settings.
- **Refresh system settings**. If enabled, the agent triggers a refresh of Windows system settings (for example, Windows Explorer and Control Panel) when an agent refresh occurs.
- **Refresh when environment settings change**. If enabled, the agent triggers a Windows refresh on endpoints when any environment setting changes.
- **Refresh desktop**. If enabled, the agent triggers a refresh of desktop settings when an agent refresh occurs. For information about desktop settings, see Desktop.
- **Refresh appearance**. If enabled, the agent triggers a refresh of Windows theme and desktop wallpaper when an agent refresh occurs.

Automatic refresh (UI agent only):

- **Enable automatic refresh**. If enabled, the Citrix WEM Agent Host refreshes automatically. By default, the refresh delay is 30 minutes.

Offline mode:

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

- **Enable offline mode**. If disabled, the agent does not fall back on its cache when it fails to connect to the WEM service.
- **Use cache even when online**. If enabled, the agent always reads its settings and actions from its cache (which is built whenever the agent service cycles).
- **Use cache to accelerate actions processing**. If enabled, the agent processes actions by retrieving relevant settings from the agent local cache instead of from the infrastructure services. Doing so speeds up the processing of actions. By default, this option is enabled. Disable this option if you want to revert to the previous behavior.

  IMPORTANT:

  - The agent local cache is synchronized with the WEM service on a periodic basis. Therefore, changes to action settings take some time to take effect, depending on the value that you specified for the **Agent cache refresh delay** option (in the **Advanced Settings > Agent Settings > Agent service options** tile).
  - To reduce delays, specify a lower value. For the changes to take effect immediately, navigate to **Monitoring > Administration > Agents > Statistics** , select the target agent, and then select **Agent > Refresh cache** in **More**.
  - We recommend that you do not disable this setting. Otherwise, users might have a degraded user experience in scenarios with poor network connectivity. If disabled, actions you configured through the administration console might fail to be applied on the agent hosts in scenarios where there is a high volume of traffic to the WEM service.

Agent service options

Configure settings for the agent host service.

Agent cache refresh delay (min). This setting controls how long the Citrix WEM Agent Host Service waits to refresh its cache. The refresh keeps the cache in sync with the WEM service database. The default is 30 minutes. When using this option, keep the following in mind:

- The minimum interval at which the cache synchronizes with the WEM service database is 15 minutes. Type an integer that is equal to or greater than 15 minutes.
- The actual sync interval might vary. Based on the specified value, the WEM agent calculates an interval in which a random value is selected as the actual sync interval each time the agent

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

cache refresh delay times out. For example, you set the value to 30 minutes. The agent selects a random value from this interval: .

SQL settings refresh delay (min). This setting controls how long the Citrix WEM Agent Host Service waits to refresh its SQL connection settings. The default is 15 minutes. Type an integer that is equal to or greater than 15 minutes.

Agent extra launch delay (ms). This setting controls how long the Citrix WEM Agent Host Service waits to launch the agent host executable. The default is 0.

TIP:

In scenarios where you want the agent host to complete the necessary work first, you can specify how long the agent application launcher (VUEMAppCmd.exe) waits. VUEMAppCmd.exe ensures that the agent host finishes processing an environment before Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) and Citrix Virtual Apps and Desktops published applications are started. To specify the wait time, configure the VUEMAppCmd extra sync delay setting, available in the Agent Host Configuration group policy. For more information, see Install and configure the agent.

Enable debug mode. Controls whether to enable verbose logging for all agents connecting to the configuration set.

Bypass ie4uinit check. By default, the Citrix WEM Agent Host Service awaits ie4uinit to run before launching the agent host executable. This setting forces the Citrix WEM Agent Host service to not wait for ie4uinit.

Agent upgrade

Schedules automatic upgrades for all agents bound to this configuration set.

Upgrading an agent is now done within the new **App Package Delivery** feature. To configure and schedule agent upgrades, go to **App Package Delivery > Delivery tasks** and create a **WEM agent upgrade** delivery task. Settings configured previously are turned into delivery tasks automatically.

Miscellaneous

Configure settings such as notifications, initial environment cleanup, and Wake on LAN.

Notifications:

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

- **Enable notifications for connection state change**. If enabled, the agent displays notification messages on the agent host when the connection to the infrastructure service is lost or restored. Citrix recommends that you do not enable this option on poor-quality network connections. Otherwise, connection state change notifications might appear frequently on the endpoint (agent host).

Extra features:

- **Initial environment cleanup**. If enabled, the agent cleans up the user environment during the first logon. Specifically, it deletes the following items:
  - User network printers.
    - With **Preserve Auto-created Printers** on the **Cleanup Actions** tab enabled, the agent does not delete auto-created printers.
    - With **Preserve Specific Printers** on the **Cleanup Actions** tab enabled, the agent does not delete any of the printers specified in the list.
  - All network drives except the network drive that is the home drive.
  - All non-system desktop, Start menu, Quick Launch, and Start-button-context-menu shortcuts.
  - All taskbar and Start menu pinned shortcuts.
- **Initial desktop UI cleanup**. If enabled, the agent cleans up the session desktop during the first logon. Specifically, it deletes the following items:
  - All non-system desktop, Start menu, Quick Launch, and Start-button-context-menu shortcuts.
  - All taskbar and Start menu pinned shortcuts.
- **Enable cross-domain search for user groups**. If enabled, the agent queries user groups in all Active Directory domains. Cross-domain search can be time-intensive. Select this option only if necessary.
- **Enable agent to use cached domain search results**. If enabled, the agent uses the cache for domain query results to improve performance and resiliency. The domain query results is cached up to seven days.
- **Check application existence**. If enabled, the agent does not create a shortcut unless it confirms that the application exists on the machine the user signs in to.

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

- **Expand environment variables for applications**. Controls whether to expand environment variables in the application target path and working folder before processing them.
- **WEM service timeout (ms)**. The timeout value after which the agent switches to its own cache, when it fails to connect to the infrastructure service. The default value is 15000 milliseconds.
- **Agent max degree of parallelism**. The maximum number of threads that the agent can use. The default value is 0 (as many threads as physically allowed by the processor). 1 is single-threaded, 2 is dual-threaded, and so on. Usually, this value does not need changing.
- **Directory services timeout (ms)**. The timeout value for directory services on the Agent Host machine, after which the agent uses its own internal cache of user group associations. The default value is 15000 milliseconds.
- **Network resources timeout (ms)**. The timeout value for resolving network resources (network drives or file/folder resources located on the network), after which the agent considers that the action has failed. The default value is 500 milliseconds.

Wake on LAN:

Use this tab to remotely turn on agent hosts. WEM automatically selects agents that reside on the same subnet as the target agents and uses those agents as Wake on LAN messengers. This feature requires hardware compatible with Wake on LAN. To use this feature, verify that the target machines satisfy the hardware requirements and relevant BIOS settings are configured.

Enable Wake on LAN for agents. Controls whether to configure settings on Windows operating systems to enable Wake on LAN for the agent hosts. If selected, the agents configure the following system settings:

- Disable **Energy Efficient Ethernet** for the network adapter
- Enable **Wake on Magic Packet** for the network adapter
- Enable **Allow this device to wake the computer** for the network adapter
- Enable **Only allow a magic packet to wake the computer** for the network adapter
- Disable **Turn on fast startup**

After enabling this option, navigate to **Monitoring > Administration > Agents > Statistics**, select one or more agents from the list, and then select **Power Management > Wake** in **More** to wake up the selected agents.

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

Action settings

This page lets you configure settings related to action processing and cleanup.

Action processing

Control how and when the agent processes actions, and whether unassigned actions get deleted from desktops.

Action processing on logon and refresh. The following settings control what actions the agent processes when users log on and when the agent refreshes.

- **Process applications on logon and refresh**
- **Process printers on logon and refresh**
- **Process virtual drives on logon and refresh**
- **Process registries on logon and refresh**
- **Process environment variables on logon and refresh**
- **Process ports on logon and refresh**
- **Process INI files on logon and refresh**
- **Process external tasks on logon and refresh**
- **Process file system operations on logon and refresh**
- **Process user DSNs on logon and refresh**
- **Process FTAs on logon and refresh**

Other Settings:

- **Await policy and JSON file processing on logon**. Use this option if you want users to complete logon until all settings (GPOs and JSON objects) are processed.

Action processing on reconnection. The following settings control what actions the agent processes when users reconnect to the agent machine.

- **Process applications on reconnection**
- **Process printers on reconnection**
- **Process network drives on reconnection**
- **Process virtual drives on reconnection**
- **Process registries on reconnection**
- **Process environment variables on reconnection**

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

- **Process ports on reconnection**
- **Process INI files on reconnection**
- **Process external tasks on reconnection**
- **Process file system operations on reconnection**
- **Process user DSNs on reconnection**
- **Process FTAs on reconnection**

Delete actions when unassigned. If these settings are enabled, the agent deletes any unassigned actions when it next refreshes.

- **Delete applications from desktops when unassigned**
- **Delete printers from desktops when unassigned**
- **Delete network drives from desktops when unassigned**
- **Delete virtual drives from desktops when unassigned**
- **Delete registries from desktops when unassigned**
- **Delete environment variables from desktops when unassigned**
- **Delete ports from desktops when unassigned**
- **Delete file system operations from desktops when unassigned**
- **Delete user DSNs from desktops when unassigned**
- **Delete FTAs from desktops when unassigned**

Enforce action processing. If these settings are enabled, the agent always refreshes those actions, even if no changes have been made.

- **Enforce processing of applications**
- **Enforce processing of printers**
- **Enforce processing of network drives**
- **Enforce processing of virtual drives**
- **Enforce processing of environment variables**
- **Enforce processing of ports**

Enforce filter processing. If enabled, these options force the agent to reprocess filters on every refresh.

- **Enforce processing of filters for applications**

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

- **Enforce processing of filters for printers**
- **Enforce processing of filters for network drives**
- **Enforce processing of filters for virtual drives**
- **Enforce processing of filters for registries**
- **Enforce processing of filters for environment variables**
- **Enforce processing of filters for ports**
- **Enforce processing of filters for file system operations**
- **Enforce processing of filters for user DSNs**
- **Enforce processing of filters for FTAs**

Asynchronous processing:

- **Process printers asynchronously**. If enabled, the agent processes printers asynchronously, without awaiting the completion of the processing of other actions.
- **Process network drives asynchronously**. If enabled, the agent processes network drives asynchronously, without awaiting the completion of the processing of other actions.

Action cleanup

Options present on this tile control whether the agent deletes the shortcuts or other items (network drives and printers) on startup. When you assign actions to a user or user group, you might find that you can also control the creation of the shortcuts or items. For example, you can specify where to create the application shortcut when managing assignments for an application. Workspace Environment Management processes these options according to a specific priority:

1. The options configured for the assigned actions in **Manage assignments**.
2. The options present on the **Action cleanup** tile.

For example, suppose you have enabled the **Create desktop shortcut** option for the assigned application in **Manage assignment**, and the application shortcut is already created on the desktop. The shortcut is still on the desktop when the agent starts, even though you enabled the **Delete desktop shortcuts on startup** option on the **Action cleanup** tile.

Application shortcut. The following settings control what shortcuts to delete on startup.

- Delete desktop shortcuts on startup.
- Delete shortcuts pinned to the taskbar on startup.
- Delete Quick Launch shortcuts on startup.

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

- Delete the Start menu shortcuts on startup.
- Delete shortcuts pinned to the Start menu on startup.

Network printer:

- **Delete network printers on startup**. If enabled, the agent deletes all network printers on startup.

Network drive:

- Delete network drives on startup. If enabled, the agent deletes all network drives on startup.

UI Agent Personalization

This page lets you personalize the appearance of the agent (in UI mode) in the user environment and customize how users interact with it.

Appearance and interaction

Customize UI agent appearance and interactions.

Splash screen and theme:

- **Custom logo**. By default, when the agent launches or refreshes, users see a splash screen with the Citrix Workspace™ Environment Management logo. You can specify an image accessible from the user environment to replace the logo.
- **Loading circle color**. Modifies the color of the loading circle to fit your custom logo.
- **Text label color**. Modifies the color of the loading text to fit your custom logo.
- **UI agent theme**. Select an appearance theme for dialogs that open from the UI agent.
- **Hide agent splash screen**. If enabled, hides the splash screen when the agent is loading or refreshing. This setting does not take effect the first time the agent refreshes.
- **Hide agent splash screen on reconnection**. If enabled, hides the splash screen when users reconnect to the agent machine.
- **Hide agent splash screen for published applications**. If enabled, hides the agent splash screen for published applications where the agent is running.
- **Hide agent icon for published applications**. If enabled, published applications do not display the agent icon.

User interaction:

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

- **Only administrators can close agent**. If enabled, only administrators can exit the agent. As a result, the Exit option in the agent menu is disabled on endpoints for non-administrators.
- **Prohibit administrators from closing agent**. If enabled, administrators cannot exit the agent.
- **Disable administrative refresh feedback**. If selected, no notification appears in the user environment when an administrator refreshes the agent using the administration console.
- **Allow users to reset actions**. Controls whether to display the **Reset Actions** option in the agent menu. By default, the option is disabled. The **Reset Actions** option lets current users specify what actions to reset in their environment. After a user selects **Reset Actions**, the **Reset actions** dialog appears. In the dialog, the user can have granular control over what to reset. The user can select the applicable actions and then click **Reset**. Doing so purges the corresponding action-related registry entries.

  NOTE:

  The following two options are always available in the agent menu: **Refresh** and **About**. The **Refresh** option triggers an immediate update of the WEM agent settings. As a result, settings configured in the administration console take effect immediately. The **About** option opens a dialog displaying version details about the agent in use.

- **Allow users to manage applications**. If enabled, the **Manage Applications** option in the agent menu is available to users on endpoints. Users can click the option to open the **Manage applications** dialog and configure the following options. By default, the option is enabled.
- **Allow users to manage printers**. If enabled, the **Manage Printers** option in the agent menu is available to users on endpoints. Users can click the option to open the **Manage printers** dialog to configure a default printer and to modify print preferences. By default, the option is enabled.
- **Show My Applications in agent menu**. If enabled, show the **My Applications** option in the agent menu. If shown, users can view applications assigned to them.
- **Show Agent Insights in agent menu**. Shows the **Agent Insights** option in the agent menu. When visible, users can enable or disable **Agent Insights** from the menu.

Help desk options

Specify help and support links and configure screen capture options.

HELP AND SUPPORT

- **Help link**. Enter a web link where users can ask for help. If specified, users see the Help option in the agent menu. Clicking it opens the website.

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

- **Support link**. Enter a web link where users can access support-related information. If specified, users see the Support option in the agent menu. Clicking it opens the website.

SCREEN CAPTURE

Enable screen capture. Controls whether to display the **Capture** option in the agent menu. Users can use the option to open a screen capture tool. The tool provides the following options:

- **New capture**. Takes a screenshot of errors in the user environment.
- **Save**. Saves the screenshot.
- **Send to support**. Sends the screenshot to support staff.

Show Send to support option. Controls whether to display the **Send to support** option in the screen capture tool. If enabled, users can use the option to send screenshots and log files directly to the specified support email address, in the specified format. This setting requires a working, configured email client.

Support email address. Enter an email address.

Email template. Specify an email content template that the screen capture tool uses to send support emails. This field cannot be empty.

NOTE:

For a list of hash-tags that you can use in the email template, see Dynamic tokens. Users are only presented with the option to enter a comment if the `##UserScreenCaptureComment## hash-tag` is included in the email template.

Custom subject. Specify an email subject template that the screen capture tool uses to send support emails.

Use SMTP to send Email. If enabled, sends a support email using SMTP instead of MAPI.

Power saving

Specify when to shut down or suspend the agent machine.

- **Shut down at specified time**. If enabled, the agent automatically shuts down the machine where it is running at the specified time. The time is based on the agent time zone.
- **Shut down when idle**. If enabled, the agent automatically shuts down the machine where it is running after the machine remains idle (no user input) for the specified length of time.

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

- **Suspend rather than shutting down**. If enabled, the agent instead suspends the machine where it is running at the specified time or after the machine remains idle for the specified length of time.

Monitoring preferences

This page contains the following settings:

- **Action processing results**. Lets you collect results of action processing and view a report. Select the actions you want to collect results for.

  > **NOTE:**
  >
  > Results are uploaded every four hours. To immediately upload results from the agents, use the **Retrieve statistics from agent** option in Monitoring > Administration > Agents.

- **Group Policy settings**
- **JSON files**
  - **Group Policy settings**
  - **External tasks**
  - **JSON files**
- **Additional settings.** Configure how agent reports are handled:
  - **Save reports locally to display in Agent Insights**. Enables the agent to save reports locally so they appear in **Agent Insights**. When this setting is enabled, the following **Reports to save** options are selected automatically:
    - **Reports to save**. Specifies the types of reports to save locally:
      - **Logon analysis**: Saves the logon analysis report.
      - **Profile insights**: Saves the profile container insights report.
  - **Set alternative location for locally saved agent reports.** Specifies an alternative location for saving the reports.
- **Optimization and usage insights**. Lets you gain insights into application behavior. Use the following option to control whether the agent collects and uploads data for insights.
  - **Enable data collection and upload for optimization and usage insights**

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

After you enable the option, data updates might take a few hours to complete.

- **Profile insights**. Lets you gain insights into profile containers for Profile Management and FSLogix. Use the following option to control whether the agent scans large files on profile containers.

  - **Enable large file scanning**

    If enabled, run a scan of large files on profile containers when container usage exceeds the specified threshold value. Scanning is limited to once every 24 hours. You can specify what files are treated as large files based on their size.

- **Profile Management health check**. Lets you specify the scope of settings to cover in Profile Management health check reports. Health checks run every 24 hours or on demand. Select the Profile Management settings that you want to cover in the reports.

  NOTE:

  - To run health checks on demand, use the **Run Profile Management health check** option in Monitoring > Administration > Agents.
  - Changes you make are reflected only in new reports and do not affect existing reports. Only the latest report is maintained for each agent.

- **Security logs**. Lets you collect logs on security rule executions and generates a report. Select the security aspects that you want to include in the report.

  - The **Privilege elevation** security aspect controls log collection for the events, **EXE privilege elevation**, **MSI privilege elevation**, and **Self-elevation**.
  - When you select the **Process hierarchy control** security aspect, **Blocked activities** option is selected by default, but the **Allowed activities** option can be edited.
  - When you select the **Application security log** security aspect, **Blocked activities** option is checked by default, whereas the **Audited activities**, and **Allowed activities** option can be edited.

  For more details, see Reports.

- **Application delivery results**. Lets you collect the results of application delivery and generates a report. If you select the **Application delivery task results** check box, the agent will collect the report and upload the report to the WEM server. For more details, see Reports.

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

NOTE:

- Results are uploaded every four hours. To immediately upload results from the agents, use the **Retrieve statistics from agent** option in Monitoring > Administration > Agents

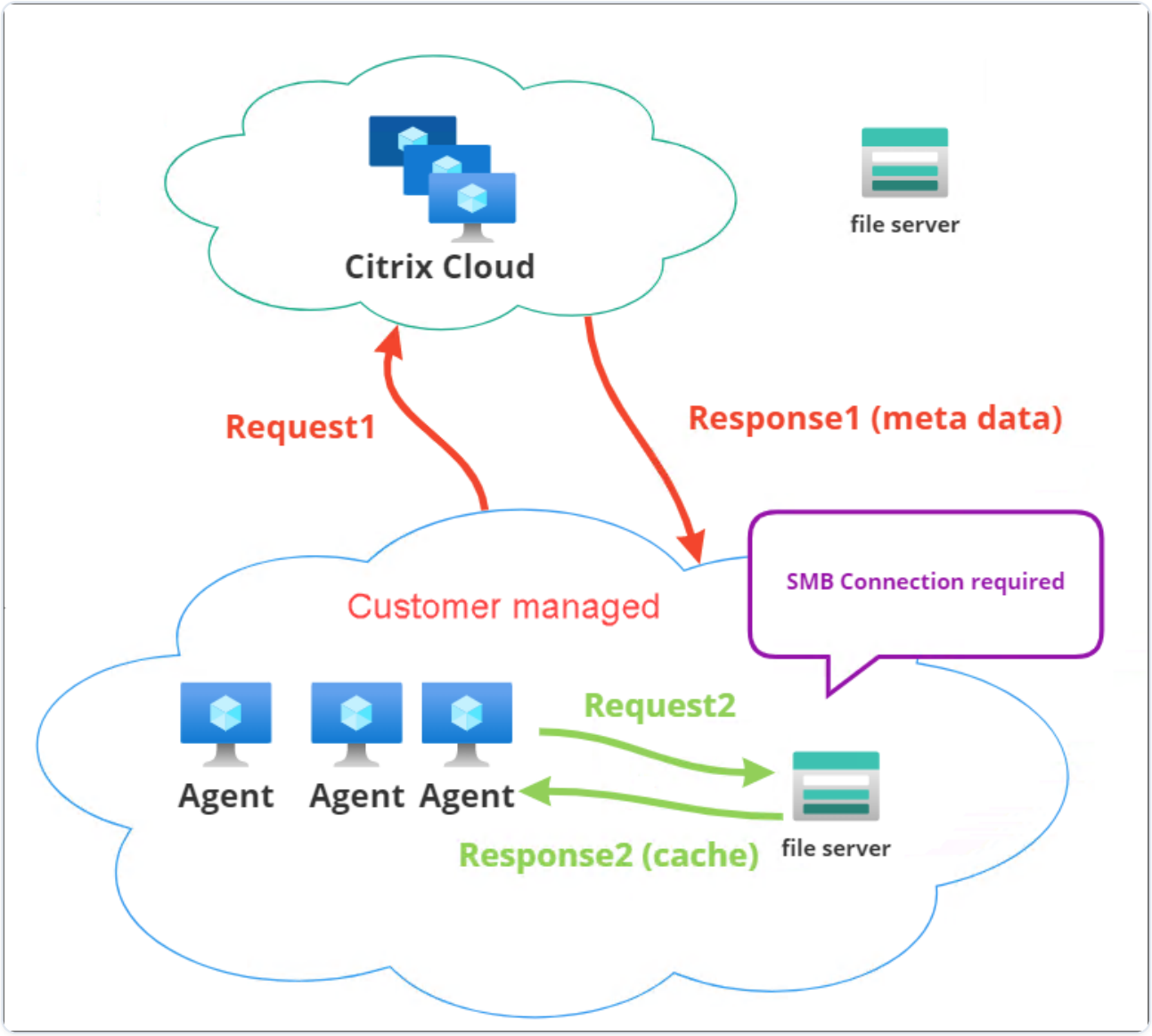
- **VHD management**. Collects results and generates reports on operations related to VHD management. If you select VHD disk compaction, the agent collects the related report and uploads it to the WEM service. For more information, see Reports.

File shares

This page lets you add SMB shares to which WEM can connect. You can then configure shares for desired features so that those features can use the shares as needed. Using SMB shares reduces traffic on networks and reduces the time to download files to agent machines.

The following graphic provides an overview of how file shares work.

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



A file download begins with a specific agent machine. This initial download occurs through Citrix Cloud. After the download completes, the agent uploads the file to the file share for other agents to use. So, later downloads occur directly through the file share rather than through Citrix Cloud.

With a file share configured, when a file download is needed, the agent first verifies whether the file is available on the file share. If available, the download occurs through the file share. If unavailable, the agent connects to Citrix Cloud for the initial download and then uploads the downloaded file to the file share.

Add SMB share

Enter an SMB share and credentials of an administrator with permission to access that share. Complete the following steps:

1. On the **File Shares** page, click **Add SMB share**.
2. In the Add SMB share wizard, fill in the following information:

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

- **SMB share**. Enter the path in the form `\\ServerName\ShareName` where `ServerName` is the FQDN or IP address of the server hosting the SMB share and `ShareName` is the name of the SMB share.
- **User name**. Enter the name in the form `domain\username`.
- **Password**. Enter the password to be used to access the SMB share.

3. Click **Done** to save and exit.

Select SMB shares for features to use

Select an SMB share from the list. The setting defaults to **None**. When selecting shares for features, consider the following:

- The credentials must have full read/write permission on the shares.
- To connect to the shares, the agent must run under the local system account.
- When configured, the features use the shares as needed — the connections to the shares are non-persistent and established only when necessary.
- If the shares are not accessible, agents fall back to downloading files through Citrix Cloud.

You can also change or remove the SMB shares for the **App package delivery** feature.

Select SMB shares for relevant services to use

Select one or more SMB shares from the list. When selected, services (for example, Citrix Profile Management service) running under the local system account in your deployment can use the shares as needed — the connections to the shares are persistent. This feature enables those services to access the shares through the connections.

SMB configuration example

For examples of how to configure SMB shares:

- See Configure SMB shares for Citrix Profile Management service to use.

System Optimization

Workspace Environment Management™ (WEM) system optimization consists of the following settings:

- CPU Management
- Memory Management
- I/O Management

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

- Fast Logoff
- Citrix Optimizer
- Multi-session Optimization

These settings are designed to lower resource usage on the agent machine. They help to make sure that freed-up resources are available for other applications. Doing so increases user density by supporting more users per server.

System optimization settings are machine-based and apply to all user sessions, but process optimization is user centric. This means that when a process triggers CPU spike protection in user A's session, the event is recorded only for user A. When user B starts the same process, process optimization behavior is determined only by process triggers in user B's session.

CPU management

These settings let you optimize CPU usage.

Processes can run across all cores and can use up as much CPU as they want. In WEM, the CPU management feature lets you limit how much CPU capacity individual processes can use. CPU spike protection is not designed to reduce overall CPU usage. It is designed to reduce the impact on user experience by processes that consume an excessive percentage of CPU usage.

When CPU spike protection is enabled, if a process reaches a specified threshold, WEM automatically lowers the priority of the process for a certain time. Then, when a new application is launched, it has a higher priority than the lower-priority process and the system will continue to run smoothly.

CPU spike protection examines each process in a quick "snapshot." If the average load of a process exceeds the specified usage limit for a specified sample time, its priority reduces immediately. After a specified time, the process' CPU priority returns to its previous value. The process is not "throttled." Unlike in **CPU Clamping**, only its priority is reduced.

CPU spike protection is not triggered until at least one instance of an individual process exceeds the threshold. In other words, even if total CPU consumption exceeds the specified threshold, CPU spike protection is not triggered unless at least one process instance exceeds the threshold. But when that process instance triggers CPU spike protection, new instances of the same process are (CPU) optimized when the option **Enable intelligent CPU optimization** is enabled.

Whenever a specific process triggers CPU spike protection, the event is recorded in the agent's local database. The agent records trigger events for each user separately. This means that CPU

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

optimization for a specific process for user1 does not affect the behavior of the same process for user2.

For example, if Internet Explorer is sometimes consuming 50–60% of CPU, you can use CPU spike protection to target only those iexplore.exe instances that are threatening VDA performance. (By contrast, CPU clamping applies to all processes.)

We recommend that you experiment with the sample time to decide the optimal value for your environment that does not affect other users logged on to the same VDA.

CPU spike protection

NOTE:

- "CPU usage" in the following settings is based on "logical processors" in the physical or virtual machine. Each core in a CPU is considered as a logical processor, in the same way that Windows does. For example, a physical machine with one 6-core CPU is considered to have 12 logical processors (Hyper-Threading Technology means that cores are doubled). A physical machine with 8 x CPUs, each with 12 cores has 96 logical processors. A VM configured with two 4-core CPUs has 8 logical processors.
- The same applies to virtual machines. For example, suppose you have a physical machine with 8 x CPUs, each with 12 cores (96 logical processors), supporting four multi-session OS VDA VMs. Each VM is configured with two 4-cores CPUs (8 logical processors). To restrict processes that trigger CPU spike protection on a VM, to use half of its cores, set **CPU core usage limit** to 4 (half of the VM's logical processors), not to 48 (half of the physical machine's logical processors).

When enabled, lowers the CPU priority of processes for a period of time (specified in the **Idle priority time** field) if they exceed the specified percentage of CPU usage for a period of time (specified in the **Sample time limit** field).

Automatically prevent CPU spikes. This option automatically reduce the CPU priority of processes that overload your CPU. This option automatically calculates the threshold value at which to trigger CPU spike protection based on the number of logical processors (CPU cores). For example, suppose that there are 4 cores. With this option enabled, if the overall CPU usage exceeds 23%, the CPU priority of processes that consume more than 15% of the overall CPU resources reduces automatically. Similarly, in the case of 8 cores, if the overall CPU usage

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

exceeds 11%, the CPU priority of processes that consume more than 8% of the CPU resources reduces automatically.

Customize CPU spike protection. Lets you customize settings for CPU spike protection.

- **CPU usage limit**. The percentage of CPU usage that any process instance must reach to trigger CPU spike protection. This limit is global across all logical processors in the server, and is determined on an instance-by-process basis. Multiple instances of the same process do not have their CPU usage percentages added when determining CPU spike protection triggers. If a process instance never reaches this limit, CPU spike protection is not triggered. For example, on a Server VDA, in multiple concurrent sessions, suppose that there are many iexplore.exe instances. Each instance peaks at around 35% CPU usage for periods of time, so that cumulatively, iexplore.exe is consistently consuming a high percentage of CPU usage. However, CPU spike protection is never triggered unless you set CPU Usage Limit at or below 35%.
- **Sample time limit**. The length of time for which a process must exceed the CPU usage limit before its CPU priority is lowered.
- **Idle priority time**. The length of time for which the CPU priority of the process is lowered. After that time, the priority returns to one of the following:
    - The default level (**Normal**) if the process priority is not specified in the CPU priority tile and the **Enable intelligent CPU optimization** option is not selected.
    - The specified level if the process priority is specified in the CPU priority tile, regardless of whether the **Enable intelligent CPU optimization** option is selected.
    - A random level depending on the behavior of the process. This case occurs if the process priority is not specified in the CPU priority tile and the **Enable intelligent CPU optimization** option is selected. The more frequent the process triggers CPU spike protection, the lower its CPU priority is.

Enable CPU core usage limit. Limits processes that trigger CPU spike protection to a specified number of logical processors on the machine. Type an integer in the range of 1 through X, where X is the total number of cores. If you type an integer greater than X, WEM limits the maximum consumption of isolated processes to X by default.

- **CPU core usage limit**. Specifies the number of logical processors to which processes that trigger CPU spike protection are limited. In the case of VMs, the value you type limits the processes to the number of logical processors in the VMs rather than in the underlying physical hardware.

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

Enable intelligent CPU optimization. When enabled, the agent intelligently optimizes the CPU priority of processes that trigger CPU spike protection. Processes that repeatedly trigger CPU spike protection are assigned progressively lower CPU priority at launch than processes that behave correctly. Note that WEM does not perform CPU optimization for the following system processes:

- Taskmgr
- System Idle Process
- System
- Svchost
- LSASS
- Wininit
- services
- csrss
- audiodg
- MsMpEng
- NisSrv
- mscorsvw
- vmwareresolutionset

Enable intelligent I/O optimization. When enabled, the agent intelligently optimizes the process I/O priority of processes that trigger CPU spike protection. Processes that repeatedly trigger CPU spike protection are assigned progressively lower I/O priority at launch than processes that behave correctly.

Exclude processes. By default, WEM CPU management excludes all of the most common Citrix and Windows core service processes. You can, however, use this option to **Add** or **Remove** processes from an exclusion list for CPU spike protection by executable name (for example notepad.exe). Typically, antivirus processes would be excluded.

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

TIP:

- To stop antivirus scanning taking over disk I/O in the session, you can also set a static I/O Priority of Low for antivirus processes, see I/O Management.
- When processes trigger CPU spike protection, and process CPU priority is lowered, WEM logs a warning each time it lowers the CPU priority of a process. In the Event Log, in Application and Services Logs, Norskale Agent Service, look for **Initializing process limitation thread for process**.

Prevent child processes from inheriting CPU priority. Specifies processes whose child processes you do not want to inherit the CPU priority.

CPU SPIKE PROTECTION OPTION

Choose how you want to enforce CPU spike protection:

- **Automatically prevent CPU spikes**. Use this option to let the agent perform CPU spike protection when the system CPU usage (relative to a single CPU core) exceeds 90% and the process CPU usage (relative to a single CPU core) exceeds 80%.
- **Customize CPU spike protection**. Lets you customize settings for CPU spike protection.
    - **CPU usage limit**. The percentage of CPU usage that any process instance must reach to trigger CPU spike protection. This limit is global across all logical processors on the server, and is determined on an instance-by-process basis. To configure the limit based on a single CPU core as a reference, use the **Set limit relative to single CPU core** option.

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

NOTE:

- Both integer and non-integer values are supported. By entering a non-integer value, for example 37.5%, you restrict processes that use more than three cores on an eight-core platform.
- **Set limit relative to single CPU core**. Lets you set a limit on CPU usage based on a single CPU core as a reference. The value can be greater than 100%, for example, 200% or 250%. Example: When the value is set to 200%, the agent optimizes processes that use two or more CPU cores. Both integer and non-integer values are supported. **Note:**
- With **Customize CPU spike protection** configured, CPU spike protection is triggered when either the global CPU usage limit or the CPU usage limit relative to a single CPU core is reached, whichever occurs first.

For processes that trigger CPU spike protection, the agent can do the following:

- If the **Enable CPU core usage limit** option is not selected: The agent lowers the CPU priority of those processes.
- If the **Enable CPU core usage limit** option is selected: The agent lowers the CPU priority of those processes and limits them to the specified number of logical processors on the machine.

When configuring CPU spike protection, keep the following in mind:

- Multiple instances of the same process do not have their CPU usage percentages added when determining CPU spike protection triggers. If a process instance never reaches this limit, CPU spike protection is not triggered. For example, in the case of a multi-session VDA with multiple concurrent sessions, there are multiple chrome.exe processes. Their CPU usage is not summed together when calculating the CPU usage.

SAMPLING TIME FOR CPU SPIKE PROTECTION

Sample time limit. The length of time for which a process must exceed the CPU usage limit before CPU spike protection is enforced.

PRIORITY LOWERING TIME FOR CPU SPIKE PROTECTION

Idle priority time. The length of time for which the CPU priority of the process is lowered. After that time, the priority returns to one of the following:

The default level (**Normal**), if the process priority is not specified in the CPU priority tile and the **Enable intelligent CPU optimization** option is not selected. The specified level, if the process

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

priority is specified in the CPU priority tile, regardless of whether the **Enable intelligent CPU optimization** option is selected. The calculated random level, depending on the behavior of the process. This case occurs if the process priority is not specified in the CPU priority tile and the **Enable intelligent CPU optimization** option is selected. The more frequent the process triggers CPU spike protection, the lower its CPU priority is.

ADDITIONAL OPTIONS

Enable CPU core usage limit. Use this option to limit processes that trigger CPU spike protection to a specific number of logical processors on the machine.

CPU priority

When enabled, lets you set CPU priority for processes manually.

These settings take effect if processes are competing for a resource. They let you optimize the CPU priority level of specific processes, so that processes that are contending for CPU processor time do not cause performance bottlenecks. When processes compete with each other, processes with lower priority are served after other process with a higher priority. They are therefore less likely to consume such a large share of the overall CPU consumption.

The process priority you set here establishes the "base priority" for all of the threads in the process. The actual, or "current," priority of a thread might be higher (but is never lower than the base). When several processes are running on a computer, the processor time is shared between them based on their CPU priority level. The higher the CPU priority level of a process is, the more the processor time is assigned to it.

NOTE:

The overall CPU consumption does not necessarily decrease if you set lower CPU priority levels on specific processes. There might be other processes (with higher CPU priority) still affecting percentage CPU usage.

To add a process, click **Add process**. Specify the following information and then click **Save process**:

- **Process name**. The process executable name without the extension. For example, for Windows Explorer (explorer.exe) type "explorer".
- **Priority**. The "base" priority of all threads in the process. The higher the priority level of a process is, the more the processor time it gets. Select from **Idel**, **Below normal**, **Normal**, **Above normal**, **High**, and **Realtime**.

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

TIP:

Process CPU priorities you set here take effect when the agent receives the new settings and the process is restarted.

To delete a process, click the ellipsis next to the process and select **Delete**.

To edit a process, click the ellipsis next to the process and select **Edit**.

CPU affinity

When enabled, lets you define how many "logical processors" a process uses. For example, you can restrict every instance of Notepad launched on the VDA to the number of cores defined.

To add a process, click **Add process**. Specify the following information and then click **Save process**:

- **Process name**. The process executable name (for example, notepad.exe).
- **Affinity**. Enter a positive integer.

To delete a process, click the ellipsis next to the process and select **Delete**.

To edit a process, click the ellipsis next to the process and select **Edit**.

CPU clamping

When enabled, lets you prevent processes from using more than a specified percentage of the CPU's processing power. CPU clamping prevents processes using more than a specified percentage of the CPU's processing power. WEM "throttles" (or "clamps") that process when it reaches the specified CPU percentage you set. This lets you prevent processes from consuming large amounts of CPU.

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

NOTE:

- CPU clamping is a brute force approach that is computationally expensive. To keep the CPU usage of a troublesome process artificially low, it is better to use CPU spike protection, at the same time as assigning static CPU priorities and CPU affinities to such processes. CPU clamping is best reserved for controlling processes that are notoriously bad at resource management, but that cannot stand to be dropped in priority.
- After you apply a percentage of the CPU's processing power for a process and configure a different percentage for the same process later, select **Refresh agent host settings** for the change to take effect.

The clamping percentage you configure is applied to the total power of any individual CPU in the server, not to any individual core it contains. (In other words, 10% on a quad-core CPU is 10% of the entire CPU, not 10% of one core).

To add a process, click **Add process**. Specify the following information and then click **Save process**:

- **Process name**. The process executable name (for example, notepad.exe).
- **Percentage**. Enter a positive integer.

TIP:

- When WEM is clamping a process, it adds the process to its watchlist the WEM client initializes. You can verify that a process is clamped by viewing this.
- You can also verify that CPU clamping is working by looking at process monitor and confirming that CPU consumption never rises above the clamping percentage.

To delete a process, click the ellipsis next to the process and select **Delete**.

To edit a process, click the ellipsis next to the process and select **Edit**.

Memory management

These settings let you optimize application memory usage through WEM.

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

If these settings are enabled, WEM calculates how much memory a process is using and the minimum amount of memory a process needs without losing stability. WEM considers the difference as excess memory. When the process becomes idle, WEM releases the excess memory that the process consumes to the page file, and optimizes the process for subsequent launches. Usually, an application becomes idle when it is minimized to the task bar.

When applications are restored from the task bar, they initially run in their optimized state but can continue to consume additional memory as needed.

Similarly, WEM optimizes all applications that users are using during their desktop sessions. If there are multiple processes over multiple user sessions, all memory that is freed up is available for other processes. This behavior increases user density by supporting a greater number of users on the same server.

Optimize memory usage for idle processes

When enabled, forces processes that remain idle for a specified time to release excess memory until they are no longer idle.

Idle sample time. Lets you specify the length of time that a process is considered idle after which it is forced to release excess memory. During this time, WEM calculates how much memory a process is using, and the minimum amount of memory a process needs, without losing stability. The default value is 120 minutes.

Idle state limit. Lets you specify the percentage of CPU usage below which a process is considered idle. The default is 1%. We recommend that you do not use a value greater than 5%. Otherwise, a process being actively used can be mistaken for idle, causing its memory to be released.

Restrict optimization. Lets you specify a threshold limit below which WEM optimizes memory usage for idle applications.

Exclude processes from memory usage optimization. Lets you exclude processes from memory usage optimization. Specify the process name, for example, notepad.exe.

WEM does not optimize application memory usage for the following system processes:

- `rdpshell`
- `wfshell`
- `rdpclip`
- `wmiprvse`

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

- `dllhost`
- `audiodg`
- `msdtc`
- `mscorsvw`
- `spoolsv`
- `smss`
- `winlogon`
- `svchost`
- `taskmgr`
- `System Idle Process`
- `System`
- `LSASS`
- `wininit`
- `msiexec`
- `services`
- `csrss`
- `MsMpEng`
- `NisSrv`
- `Memory Compression`

Memory usage limit for specific processes

When enabled, lets you limit the memory usage of a process by setting an upper limit for the memory the process can consume.

WARNING:

Applying memory usage limits to certain processes might have unintended effects, including slow system responsiveness.

To add a process, click **Add process**. Specify the following information and then click **Save process**.

- **Process name**. Enter the name of the process you want to add (for example, notepad.exe.)

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

- **Memory limit**. Enter the memory usage limit.
- **Limit type**. Select a limit mode from the list.
    - **Dynamic Limit**. Lets you apply a dynamic limit to the specified process. This setting dynamically limits the amount of memory allocated to the specified process. If applied, enforces memory usage limits depending on available memory. Therefore, the memory that the specified process consumes might exceed the specified amount.
    - **Static Limit**. Lets you apply a static limit to the specified process. This setting always limits the amount of memory allocated to the specified process. If applied, restricts the process from consuming more than the specified amount of memory regardless of the amount of available memory. As a result, the memory that the specified process consumes is capped at the specified amount.

To delete a process, click the ellipsis next to the process and select **Delete**.

To edit a process, click the ellipsis next to the process and select **Edit**.

I/O management

These settings let you optimize the I/O priority of certain processes so that processes which are contending for disk and network I/O access do not cause performance bottlenecks. For example, you can use I/O Management settings to throttle back a disk-bandwidth-hungry application.

The process priority you set here establishes the "base priority" for all of the threads in the process. The actual, or "current," priority of a thread might be higher (but is never lower than the base). In general, Windows give access to threads of higher priority before threads of lower priority.

Process I/O priority

When enabled, Lets you optimize the I/O priority of specific processes, so that processes that are contending for disk and network I/O access do not cause performance bottlenecks.

To add a process, click **Add process**. Specify the following information and then click **Save process**.

- **Process name**. Enter The process executable name without the extension. For example, for Windows Explorer (explorer.exe) type "explorer".
- **I/O Priority**. Enter the "base" priority of all threads in the process. The higher the I/O priority of a process, the sooner its threads get I/O access. Choose from **High**, **Normal**, **Low**, **Very Low**.

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

TIP:

Process I/O priorities you set here take effect when the agent receives the new settings and the process is next restarted.

To delete a process, click the ellipsis next to the process and select **Delete**.

To edit a process, click the ellipsis next to the process and select **Edit**.

Fast logoff

These settings let you immediately ends the HDX™ connection to a remote session. Doing that gives users the impression that the session has immediately closed. However, the session itself continues through the session logoff phases in the background on the VDA.

NOTE:

Fast logoff supports Citrix virtual apps™ and RDS resources only.

When enabled, enables fast logoff for all users in this configuration set. Users are logged out immediately, while session logoff tasks continue in the background.

To exclude specific groups, perform the following steps:

1. Select **Exclude specified groups** and then **Add group**. The **Add group to exclude** wizard appears.
2. Select the identity type.
3. Select a domain where the group you want to add exists.
4. In the Search box, enter the name of the group you want to add. (Searches are not case-sensitive.)
5. Click the plus icon to add the group.
6. After you have finished, click **Save** to add the group and to exit the **Add group to exclude** wizard.

Citrix Optimizer

These settings let you optimize user environments for better performance. Citrix Optimizer runs a quick scan of user environments and then applies template-based optimization recommendations.

You can optimize user environments in two ways:

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

- Use built-in templates to perform optimizations. To do so, select a template applicable to the operating system.
- Alternatively, create your own customized templates with specific optimizations you want and then add the templates to Workspace Environment Management (WEM).

To get a template that you can customize, use either of the following approaches:

- Use the template builder feature that the standalone Citrix Optimizer offers. Download the standalone Citrix Optimizer at `<https://support.citrix.com/article/CTX224676>`. The template builder feature lets you build your own custom templates to be uploaded to WEM.
- On an agent host (machine where the WEM agent is installed), navigate to the `<C:\Program Files (x86)>\Citrix\Workspace Environment Management Agent\Citrix Optimizer\Templates` folder, select a default template file, and copy it to a convenient folder. Customize the template file to reflect your specifics and then upload the custom template to WEM.

When enabled, you can configure the following settings:

Run weekly. If selected, WEM runs optimizations on a weekly basis. If **Run weekly** is not selected, WEM behaves as follows:

- The first time you add a template to WEM, WEM runs the corresponding optimization. WEM runs the optimization only once unless you make changes to that template later. Changes include applying a different template to OS and enabling or disabling the template.
- Each time you make changes to a template, WEM runs the optimization once.

To add a custom template:

1. Click **Add custom template**.
2. In the **Add custom template** wizard, complete the following steps:
    a. For **Template name**, click **Browse** and then select the template you want to add.
    b. For **Applicable operating system**, select from the list one or more operating systems to which the template applies.

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

> **TIP:**
>
> You can add Windows 10 operating systems that are not available on the list but that the template applies to. Add those OSs by typing their build numbers. Be sure to separate the OSs with semicolons (;). For example, 2001;2004.

c. Select groups you want to activate as needed.

d. Click **Save**.

> **IMPORTANT:**
>
> Citrix optimizer does not support exporting custom templates. Retain a local copy of your custom template after you add it.

You can use the toggle in the **State** column to toggle the template between enabled and disabled states. If disabled, the agent does not process the template, and WEM does not run optimizations associated with the template.

To delete a template, select the ellipsis of the applicable template and then select **Delete**. Note: You cannot delete built-in templates.

To edit a template, select the ellipsis of the applicable template and then select **Edit**.

To view details of a template, select the ellipsis of the applicable template and then select **Preview**.

> **NOTE:**
>
> For a non-persistent VDI environment, WEM follows the same behavior – all changes to the environment are lost when the machine restarts. In the case of Citrix Optimizer, WEM runs optimizations each time the machine restarts.

Automatically select template to use. If you are unsure which template to use, use this option to let WEM select the best match for each OS. If you want to use custom templates as the preferred templates, enter a comma-separated list of prefixes. Custom template follows this name format:

- `prefix_<os version>_<os build>`
- `prefix_Server_<os version>_<os build>`

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

Changes to Citrix Optimizer settings take some time to take effect, depending on the value that you specified for the **SQL Settings Refresh Delay** option on the **Advanced Settings > Configuration > Service Options** tab of the legacy console.

For the changes to take effect immediately, navigate to **Monitoring > Administration > Agents**, locate the agent, and then select **Process Citrix Optimizer** from the **More** menu.

TIP:

New changes might fail to take effect immediately. We recommend that you select **Refresh agent host settings** before you select **Process Citrix Optimizer**.

Multi-session optimization

These settings let you optimize multi-session OS machines with disconnected sessions for better user experience with connected sessions.

Multi-session OS machines run multiple sessions from a single machine to deliver applications and desktops to users. A disconnected session remains active and its applications continue to run. The disconnected session can consume resources needed for connected desktops and applications that run on the same machine. These settings let you optimize multi-session OS machines with disconnected sessions for better user experience with connected sessions.

When enabled, optimizes multi-session OS machines where disconnected sessions are present. By default, multi-session optimization is disabled. The feature improves the user experience of connected sessions by limiting the number of resources disconnected sessions can consume. After a session stays disconnected for one minute, the WEM agent lowers the CPU and the I/O priorities of processes or applications associated with the session. The agent then imposes limits on the amount of memory resources the session can consume. If the user reconnects to the session, WEM restores the priorities and removes the limitations.

Exclude groups

To exclude specific groups from multi-session optimization, perform the following steps:

1. Select **Exclude specified groups** and then click **Add group**. The **Add group to exclude** wizard appears.
2. Select the identity type.
3. Select a domain where the group you want to add exist.

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

4. In the Search box, enter the name of the group you want to add. Enter the full name of the group. (Searches are not case-sensitive.)
5. Click the plus icon to add the group.
6. After you have finished, click **Save** to add the group and to exit the **Add group to exclude** wizard.

Exclude processes

To exclude specific processes from multi-session optimization, click **Add process**, browse to the process you want to add, and then click **Save process**.

To delete a process, click the ellipsis next to the process and select **Delete**.

To edit a process, click the ellipsis next to the process and select **Edit**.

Directory Objects

This page lets you add machines, groups, Organizational Units (OUs), and more, that you want Workspace Environment Management™ (WEM) to manage. You must add those objects to WEM so that the agent can manage them. After you add objects, a list of machines that have been added appears. Only the machines listed here are managed by WEM. You can use the search box to quickly search for objects you want. You can also use filters to refine your search.

When agents on those machines register with the infrastructure service, the infrastructure service sends them the necessary machine-dependent settings related to the configuration set. To improve the user experience, the infrastructure service caches data related to the configuration set for the agents. Data caching allows the infrastructure service to retrieve data from the directory less frequently. The cache refreshes on an hourly basis. Changing agents to a different configuration set can take some time to take effect.

TIP:

To check whether agents on those machines are correctly registered with the infrastructure service, go to **Monitoring > Administration > Agents**.

You can add the following objects:

- Machines and groups
- OUs

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

Click **Add object**, select the object type, and then navigate through the directory to the objects you want to add. After adding objects of one type, you can switch to a different type to continue. After you have finished, click **Add**.

Add a machine or machine group

1. On the **Directory Objects** node, click **Add object**.
2. Select **Computers and groups** from the object type list.
3. Select a domain from the list and search for the machine or machine groups that you want to add.

NOTE:

If your domain list has expired, you can force refresh your domain list by choosing one of the refresh options. **Refresh records** updates the selected record or the list of records and **Requery target names** updates the target names.

1. Click the plus sign to add. Machines you add are listed in the table under the search box.
2. Select the configuration set to which you want to add them.
3. When you are finished, click **Add**.

Add machines in an OU

1. On the **Directory Objects** node, click **Add object**.
2. Select **Organizational units** from the object type list.
3. Select a domain from the list and search for the OUs you want to add.

NOTE:

If your domain list has expired, you can force refresh your domain list by clicking the refresh button. The location configuration option restricts the OU search scope to a specific location node to find the desired target OU quickly.

1. Click the plus sign to add. Objects you add are listed in the table under the search box.
2. Select the configuration set to which you want to add them.
3. When you are finished, click **Add**.

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

Edit machine, machine group, or OU details

1. On the **Directory Objects** node, select the object you want to edit and then select **Edit** from the action bar.
2. In the **Edit object** wizard, edit any of the following details and then click **Save**.

    - **Name**. The machine, machine group, or OU name.
    - **Distinguished Name**. The distinguished name (DN) of the selected machine or machine group. This name allows you to differentiate different OUs if they have the same name. This section is not available for objects of the machine catalog type.
    - **Object type**. The object type (machines, groups, or OUs).
    - **Description**. Additional information about the machine, machine group, or OU.
    - **Configuration set**. The configuration set to which you want to add the object.
    - **Priority**. Lets you configure priority between different machines or groups. The priority determines the order in which the actions you assign are processed. The greater the value, the higher the priority. Type an integer. If there is a conflict (for example, when mapping different network drives with the same drive letter), the machine or group with the higher priority prevails.
    - Object state. Controls whether to enable (**Yes**) or disable (**No**) the object. If disabled, the machine, machine group, or OU is not available to assign actions to, and actions assigned to it no longer take effect. Alternatively, you can toggle the state on or off by using the toggle in the **State** column of the **Directory Objects** page.

    * Read-only details reported from the directory.

NOTE:

For objects of the machine catalog type, you can change only the configuration set.

Delete objects

Select the object that you want to delete and then select **Delete** from the action bar.

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

Advanced settings

Unbound agents

Control whether to apply settings to agents that are not bound to any configuration set. After you enable the following settings, go to the "Unbound Agents" configuration set and then configure the settings there so that you can control how unbound agents behave.

- **Apply settings to unbound agents**. Lets you apply the settings of the "Unbound Agents" configuration set to agents that you have not yet added in **Directory Objects**.

NOTE:

With **Apply settings to unbound agents** enabled, if you add those unbound agents to a different configuration set, it can take up to an hour for the new settings to be applied.

Active Directory connection security

By default, WEM uses *LDAP* for Active Directory queries. To enforce secure communication over *LDAPS*, select **Enable LDAPS to encrypt Active Directory connections**.

Monitoring

The **Monitoring** node provides information that you can use for monitoring and troubleshooting your Workspace Environment Management™ (WEM) deployment and lets you perform administrative tasks.

The **Monitoring** node consists of the following items:

- Administration. Lets you view user and agent statistics and administrative activities.
  - **User statistics.** Displays user statistics about your deployment.
  - **Agents.** Lets you view agent information and perform administrative tasks such as refreshing the cache, resetting settings, and retrieving agent information.
- Insights. Lets you gain insights into application behavior. To enable insights for a configuration set, go to its **Advanced Settings > Insights** page and select **Enable data collection and upload for optimization and usage insights**. To view insights, select a configuration set and a date range and then click **Apply**.
  - **Optimization Insights.** Displays the top 10 applications that triggered CPU spike protection and memory usage optimization most frequently over the specified time period.

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

    - **Usage Insights.** Displays the top 10 applications by usage time (hours) and the top 10 applications by number of users, along with the top 10 applications that consumed the most CPU and memory resources over the specified time period.
    - **Profile Container Insights.** Displays insights for Profile Management and FSLogix containers.

- Reports. Provides reports that let you analyze your deployments. Each report appears as a table record.

Administration

Lets you view user and agent statistics and administrative activities.

User statistics

Displays user statistics about your Workspace Environment Management™ (WEM) deployment. Each time users log on to their agent machine, relevant information is collected and then appears here as a table record.

This page includes the following information:

- **User summary**. Displays a count of all users who have logged on to their agent machine, for all configuration sets.
- **User history**. Displays connection information for all users associated with all configuration sets, including the last connection time (in Coordinated Universal Time, UTC), the name of the machine from which they last connected, and the session agent type (UI or CMD) and version.

TIP:

You can use **Filter** to filter the list. For example, display a count of all users for a specific configuration set and a count of users during the specified date range.

You can perform the following operations:

- **Refresh**. Updates the list of user statistics.
- **Refresh** icon. Updates the user display names. This icon appears when you hover your mouse on every record or any user display name.
- **Clear expired records**. Lets you delete expired records from the WEM service database. If a user's last logon time dates back more than 24 hours, the corresponding record expires. Unavailable when you do not have any expired records.

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

NOTE:

This option is not available for records whose **User ID** is **Local system**.

- **Delete record**. Deletes the record from the WEM service database. Available when you select only one agent and its corresponding record has expired.

  NOTE:

  This option is not available for records whose User ID is Local system, Network service, or NT Authority (Local service).

- **Export**. Lets you export the data in each record in **CSV** or **JSON** format, which opens in programs such as **Microsoft Excel**. To do that, perform the following steps:

  a. Click **Export**. The export wizard appears.

  b. Select the export format. Available options are **CSV** and **JSON**.

  c. Optionally, select **Save a copy of the export to your local machine**. The export is saved to the default download location of your browser.

  d. Click **Export** to start the export process.

  IMPORTANT:

  - You can export up to 50,000 records. When the number of records to export exceeds the limit, only the top 50,000 will be exported. We recommend that you use filters to reduce the number of records to 50,000 or fewer.
  - While an export is in progress, you cannot perform another export.
  - If an export does not complete within 30 minutes, you will no longer receive notifications about it. Go to **Files** to view the export results later.
  - When exporting user statistics, the export is saved to the cloud storage. The cloud storage has a storage limit. When you reach the limit, you cannot proceed with the export. In that case, go to **Files** and delete unnecessary files to free up space. See Files.

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

Agents

This page lets you view agent information and perform administrative tasks such as refreshing the cache, resetting settings, and retrieving agent information.

Statistics

LIST VIEW

Agents are listed in a table format with each row corresponding to the detailed information of an agent.

This tab shows statistics about the agents in your WEM deployment. You can view the following statistics about the agents in your WEM deployment.

- A count of total agents users have logged on to, for all configuration sets.

  TIP:

  If you specify a configuration set in your filter criteria, a count of total registered agents for that configuration set appears, along with the count of agents registered in the last 24 hours and in the last 30 days.

- Connection information for all agents registered with the configuration sets, including the last connection time, the name of the machine from which they last connected, and the agent version.
- The **Synchronization state** column provides information about the result of the last sync of the agent cache with the WEM service.
  - **Successful** (check mark icon). Indicates that the last sync was successful, with the sync result reported to the administration console.
  - **Unknown** (exclamation mark icon). Indicates that sync is in progress, has not started yet, or the result is not reported to the administration console.
  - **Failed** (error icon). Indicates that the last sync failed.
- The **Recently connected** column provides the following information:
  - **Online** (check mark icon). Indicates that the agent is online. The agent has uploaded statistics to the WEM service within a certain interval.
  - A blank column field indicates that the agent is offline.

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

- The **Profile Management health** column provides information about the health status of Profile Management in your environment.

  Profile Management health status performs automated status checks on your agent hosts to determine whether Profile Management is configured optimally. You can view the results of those checks to identify specific issues from the output file on each agent machine (`%systemroot%\temp\UpmConfigCheckOutput.json`). The feature performs status checks every day or each time the WEM agent host service starts. To perform the status checks manually, select the agent, and then select the **Run Profile Management health check** from the action bar. Each status check returns a status. To view the most recent status, click **Refresh**. The icon in the **Profile Management health** column provides general information about the health status of Profile Management:

  - **Good** (check mark icon). Indicates that Profile Management is in good shape.
  - **Notice** (check mark icon with blue dot in the upper right corner). Identifies an acceptable state of Profile Management.
  - **Warning** (check mark icon with orange dot in the upper right corner). Informs about a suboptimal state of Profile Management. The suboptimal state might affect the user experience with Profile Management in your deployment. This status does not necessarily require action on your part. To view the detailed report, use the **View Profile Management health check report** option in **More**.
  - **Error** (error icon). Indicates that Profile Management is configured incorrectly, causing it not to function properly.
  - **Invalid** (disabled icon). Appears when Profile Management is not found or not enabled.

  If the status checks do not reflect your experience or if they do not detect the issues you are having, contact Citrix Technical Support.

You can perform the following operations:

- **Task history**. Lists the agent tasks initiated in the last 24 hours. Clicking **Task history** on the **Agents** page directs you to the **Task history** page to check the progress and results of the initiated tasks.
- **Columns to display**. Lets you customize the table by choosing which columns you want to display.
- **Refresh**. Updates the list of agents.

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

- **Clear expired records**. Lets you delete expired records from the WEM service database. If a user's last logon time dates back more than 24 hours, the corresponding record expires. Unavailable when you do not have any expired records.
- **View details**. Lets you view detailed information about the agent.
- **Export**. Lets you export the data in each record in CSV or JSON format, which opens in programs such as Microsoft Excel. To do that, perform the following steps:

  a. Click **Export**. The export wizard appears.

  b. Select the export format. Available options: CSV and JSON.

  c. Optionally, select **Save a copy of the export to your local machine**. The export is saved to the default download location of your browser.

  d. Click **Export** to start the export process.

  IMPORTANT:

  - You can export up to 50,000 records. When the number of records to export exceeds the limit, only the top 50,000 will be exported. We recommend that you use filters to reduce the number of records to 50,000 or fewer.
  - While an export is in progress, you cannot perform another export.
  - If an export does not complete within 30 minutes, you will no longer receive notifications about it. Go to **Files** to view the export results later.
  - When exporting agent statistics, the export is saved to the cloud storage. The cloud storage has a storage limit. When you reach the limit, you cannot proceed with the export. In that case, go to **Files** and delete unnecessary files to free up space. See Files.

The following options are available in the **More** menu. When applying these options to non-domain-joined and enrolled agents, consider the following:

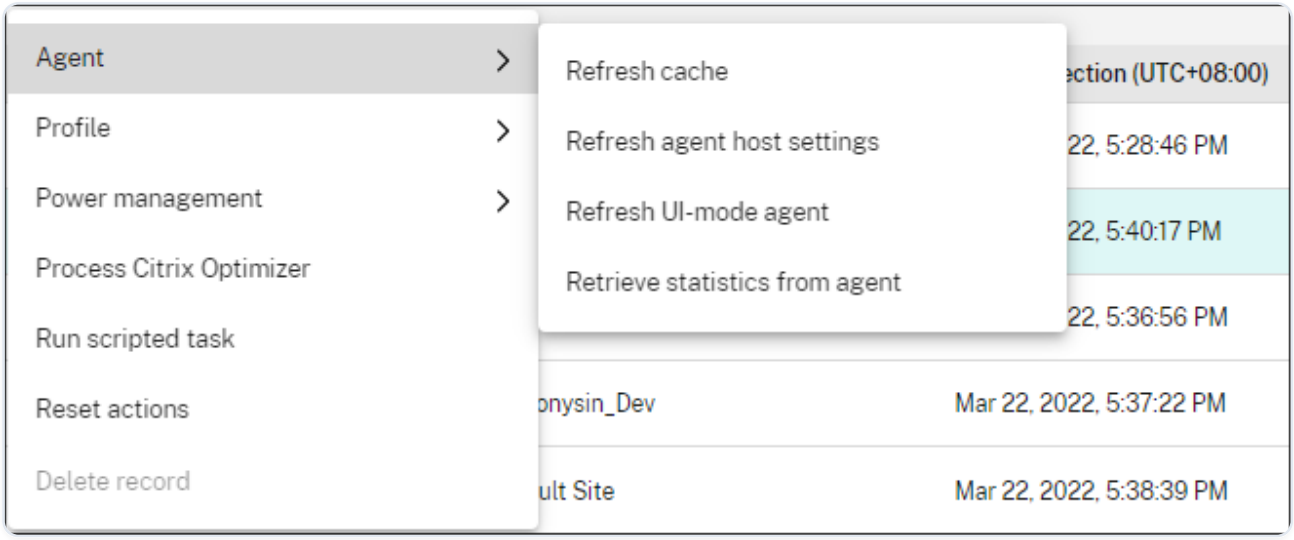
- The agent must be version 2207.1.0.1 or later.
- The target agent is not immediately notified of performing those tasks. The notifications are sent when the target agent or another agent on the same subnet connects to Citrix Cloud™ to refresh settings. So, there might be a delay until the tasks are performed on the agent side. The more agents you have on the same subnet, the shorter the delay will be.

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

- The maximum delay is 1.5 times the **SQL Settings Refresh Delay** value. By default, the **SQL Settings Refresh Delay** value is 15 minutes. See Service options. So, in that case, the maximum delay is 22.5 (1.5 x 15) minutes.

NOTE:

The **More** menu is available only when you select no more than 50 agents.



Agent:

- **Refresh cache**. Triggers a refresh of the local agent cache (an agent-side replica of the WEM configuration database). Refreshing the cache syncs the local agent cache with the infrastructure services.
- **Refresh agent host settings**. Triggers a refresh of the agent service settings in the user environment. Those settings include advanced, optimization, transformer, and non-user assigned settings.
- **Refresh UI-mode agent**. Applies the user-assigned actions to the WEM agents. Those actions include network drives, printers, applications, and more. When you refresh an agent, it communicates with the infrastructure services. The infrastructure services validate the agent host identity with the WEM database.

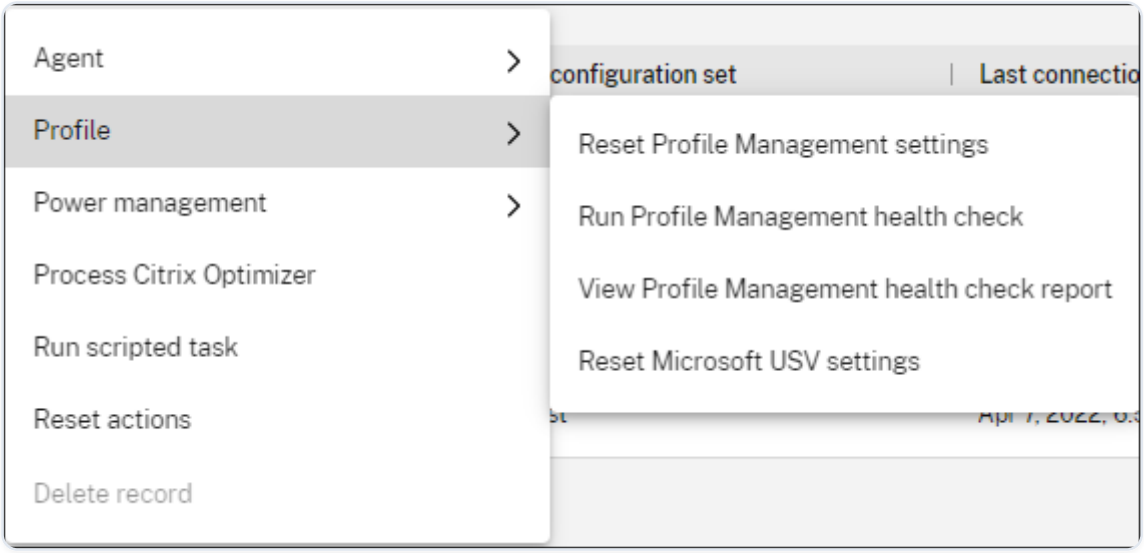
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

- The **Refresh UI-mode agent** option works only with the agents in UI mode that are automatically launched (not launched by end users or by using scripts). The option does not work with the agents in CMD mode.
- Not all settings can be refreshed. Some settings (for example, environment and group policy settings) are applied only on startup or logon.

- **Retrieve statistics from agent**. Enables the agents to upload statistics to the infrastructure services.

You can also perform the refresh operations on the agent side. However, those operations behave differently depending on actual conditions. For more information, see Agent-side refresh operations.



Profile:

- **Reset Profile Management settings**. Clears the registry cache and updates the associated configuration settings. If Profile Management settings are not applied to your agent, click **Reset Profile Management Settings**. You might need to click **Refresh** for this option to become available.

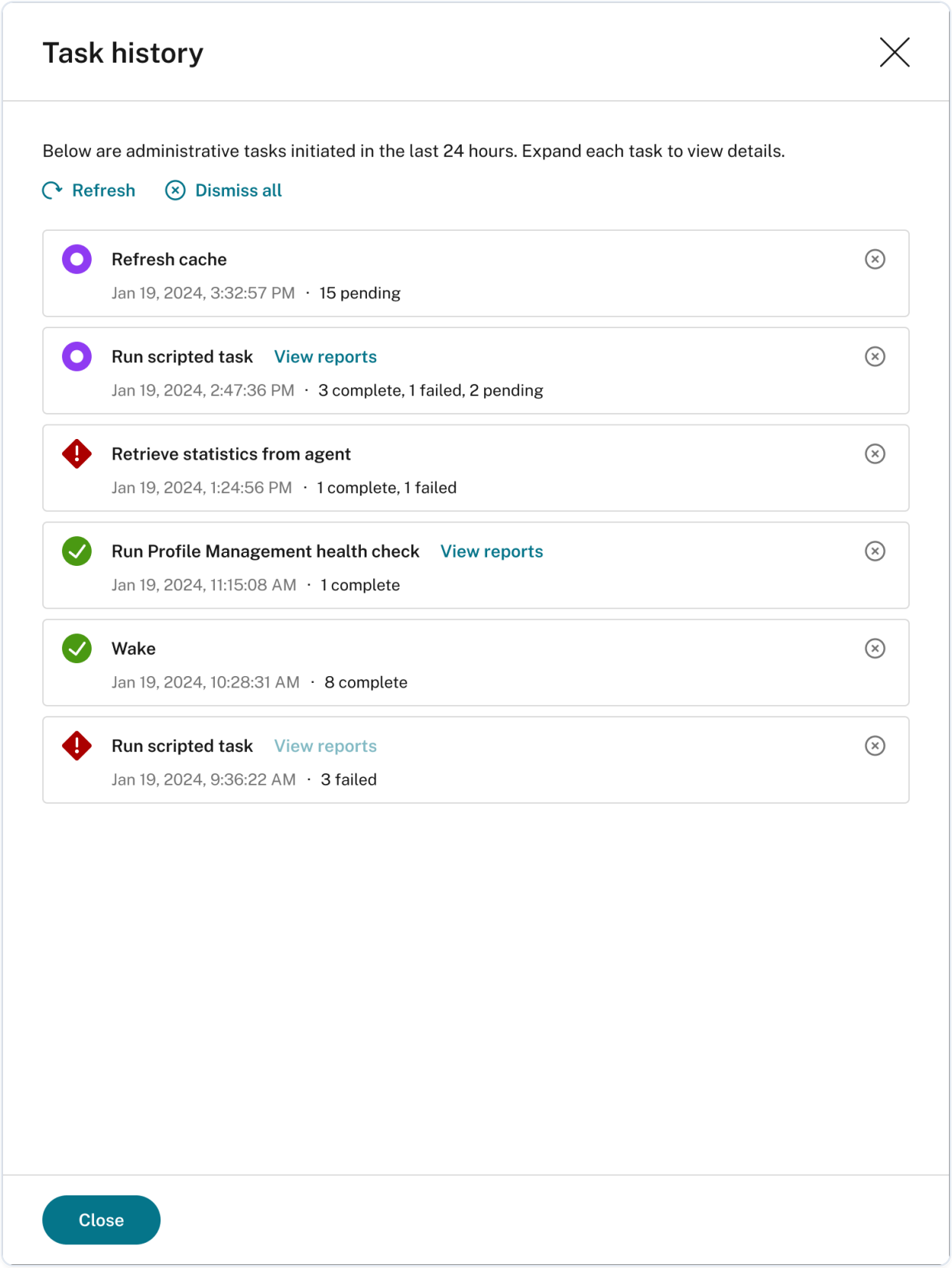
NOTE:

If the settings are not applied to the agent after configuring **Reset Profile Management Settings** from the WEM administration console, see CTX219086 for a workaround.

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

- **Run Profile Management health check**. Performs status checks on the target agent machines to determine whether Profile Management is configured optimally. After selecting this option, the **Run Profile Management health check** wizard appears. Select the Profile Management settings that you want to cover in the health check report and then click **Run**. Be aware of the following:
  - By default, the health reports cover all settings. For agents earlier than 2205.1.0.1, changes you make to the scope of settings to cover in the report do not take effect.
  - It might take some time before you can see the health reports. In Reports, refresh the view if necessary.
  - Click **View reports** to access the reports directly.

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



- **View Profile Management health check report**. Provides quick access to Profile Management health reports related to the target agent machines. For more information about Profile Management health reports, see Reports.

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

- **Reset Microsoft USV settings**. Clears the registry cache and updates the associated configuration settings. If Microsoft USV settings are not applied to your agent, click **Reset Microsoft USV settings**. You might need to click **Refresh** for this option to become available.

Power management:

- **Shut down**. Lets you shut down the selected agents.
- **Restart**. Lets you restart the selected agents.
- **Sleep**. Lets you put the selected agents into sleep mode. This option works only when the target machine supports sleep mode.
- **Hibernate**. Lets you put the selected agents into hibernate mode. This option works only when the target machine supports hibernate mode.
- **Wake**. Lets you wake up the selected agents. For the option to work, go to **Legacy Console > Advanced Settings > Configuration > Wake on LAN** and select **Enable Wake on LAN for Agents**. Also, make sure that the target machines satisfy the hardware requirements and the relevant BIOS settings are configured. For more information, see Wake on LAN.

  TIP:

  - When you shut down or restart agents, you can specify a delay (in seconds) before the shutdown or restart begins. Users receive a prompt that the machine will shut down or restart in the amount of time you specify. Shutdown prompt example: `Your administrator has initiated the shutdown of your machine from the Workspace Environment Management console. The machine shuts down in 60 seconds.`. Restart prompt example: `Your administrator has initiated the restart of your machine from the Workspace Environment Management console. The machine restarts in 60 seconds.`.
  - Consider the differences between sleep and hibernate. In sleep mode, all actions on the machine are stopped, and any open documents and applications are put in memory. The machine goes into a low-power state. In hibernate mode, open documents and running applications are saved to the hard disk. The machine is turned off entirely, using zero power.
  - To verify that the target machine supports sleep and hibernate modes, go to the machine and run the following PowerShell commands: `powercfg /a`.

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

Process Citrix Optimizer. Applies the settings to the agents so that changes to Citrix Optimizer settings take effect immediately.

Run scripted task. Lets you run scripted tasks on the target agent machines. After selecting this option, the **Run scripted task** wizard appears. Configure the following settings and then click **Run**. For more information about each setting, see Scripted Task Settings.

NOTE:

This option does not apply to non-domain-joined agents.

- **Select Script**. Select which script you want to run. This will prefill the settings using the inputs from the last time you ran this script on demand.
- **Pass parameters to the scripted task**. Choose whether to pass parameters to the scripted task. When enabled, lets you provide inputs as parameter variables in the scripted task at runtime.
- **Output files**. Choose whether you want to collect files that the task outputs. If selected, includes output file content in reports generated for the task. You can then view the output file content in the reports without the need to access the files in the user environment.
- **Highlight keywords**. Specify the keywords that you want the report to highlight. You can type multiple keywords. After typing a keyword, press **Enter** to add another. If specified, report contents that match your keywords will be highlighted in the **Output file content** and **Console output** sections in the generated reports.
- **Highlight regular expression matches**. Enter a regular expression that describes the content you want to highlight. The regular expression must conform to the .NET regular expression library syntax, which is PCRE compatible. For more information, see Scripted Task Settings.

Run delivery task. To enable this option, select agents bound to the same configuration set. To run a delivery task quickly, you can choose to run a delivery task from this page. Click **Run delivery task** and choose the delivery task from the drop-down list to run the selected delivery task on the agent. If you configure rules in the task to determine which agents must run the task, those rules get ignored when you select specific agents to run the on demand tasks.

Reset actions. Lets you reset all actions you assigned by purging all action-related registry entries on the applicable agent machine.

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

Delete record. Deletes the record from the WEM service database. If the agent is still active, this option is unavailable. Available when you select only one agent and its corresponding record has expired.

SUMMARY VIEW

The summary view on the agent statistics page displays four charts that provide statistical results of agents based on the connection state, Profile Management health status, agent version, and the last configuration set. Four charts are displayed in the **Summary** view. Clicking **Refresh** reloads all the four charts with the latest results.

Registrations

This tab shows the registration status of the agents recorded in the database.

> **IMPORTANT:**
>
> WEM agents must register with the WEM service so that settings can be applied to them. An agent can be bound only to one configuration set.

You can view the following information:

- **Device name**. Name of the machine on which the agent is running.
- **Registration status**. Registration status of the agent: **Registered** or **Unregistered**.
- **Description**. Provides more information about registration success or failure:
  - **Agent `<agent name>` bound to configuration set `<configuration set name>`**. Indicates that the WEM service is sending the necessary machine-dependent settings to the agent for the configuration set.
  - **Agent `<agent name>` not bound to any configuration set**. Indicates that the WEM service cannot resolve any configuration set for the agent. With **Apply settings to unbound agents** enabled, the settings of the "Unbound Agents" configuration set are applied to the agent. For more information about applying settings to unbound agents, see Directory Objects.
  - **Agent `<agent name>` bound multiple times to configuration set `<configuration set name>`**. Does not prevent the WEM service from applying settings to the agent.
  - **Agent `<agent name>` registered with WEM service for management with Citrix Endpoint Management™**. Appears only for Endpoint Management managed agents.

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

- **Agent `<agent name>` bound to multiple configuration sets**. Indicates that the WEM service cannot resolve a configuration set for the agent because the agent is bound to more than one configuration set.

Use **Search** to refine the results if necessary. Searches run only against device names and descriptions. By default, searches are restricted only to unregistered agents. To remove the restriction, enable **Show only unregistered agents**.

To resolve registration errors, do any of the following:

- Edit the Active Directory hierarchy (relations between computers, computer groups, and OUs) so that an agent won't be bound to the same configuration sets multiple times.
- Edit the WEM hierarchy in Directory Objects so that an agent binds only to one configuration set.
- Apply settings to unbound agents (if not yet done) so that the settings of the "Unbound Agents" configuration set are applied to unbound agents (agents that you have not yet added in **Directory Objects**).

After making these changes, use the **Refresh UI-mode agent** option to refresh the agents.

Configure Profile Management health check

WEM can check whether Citrix Profile Management is configured optimally on your agent machine. For more information, see Configure Profile Management health check.

Insights

Lets you gain insights into profile container and application behavior.

Optimization insights

This page includes two bar charts:

- **Top 20 applications by CPU optimization**. Shows the top 10 applications that triggered CPU spike protection most frequently over the specified time period.
- **Top 20 applications by memory optimization**. Shows the top 10 applications that triggered memory usage optimization most frequently over the specified time period.

To view insights, select a configuration set and a date range and then click **Apply**. Then, the charts refresh to display relevant insights.

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

IMPORTANT:

- For the charts to show data for a configuration set, you must enable insights for it. To enable insights for a configuration set, go to its **Advanced Settings > Insights** page. The charts show insights based on the data collected previously.
- Optimization insights data is not available until you enable CPU or memory management.

Excluded applications

You can exclude applications from the optimization insights (bar chart). To specify an excluded application, complete the following steps.

- Click **Add**.
- Type the name of the application as mentioned in the bar chart.
- Press **Enter** to save or **Shift + Enter** to save and start another entry.
- You can also edit and delete the added application by following the wizard instructions.

Usage insights

This page includes four bar charts:

- **Top 20 applications by usage time (hour)**
- **Top 20 applications by number of users**
- **Top 20 applications by CPU usage (%)**. Shows the top 10 applications that consumed the most CPU resources over the specified time period.
- **Top 20 applications by memory usage (MB)**. Shows the top 10 applications that consumed the most memory resources over the specified time period.

To view insights, select a configuration set and a date range and then click **Apply**. Then, the charts refresh to display relevant insights.

IMPORTANT:

For the charts to show data for a configuration set, you need to enable insights for it. To enable insights for a configuration set, go to its **Advanced Settings > Insights** page. The charts show insights based on the data collected previously.

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

Excluded applications

You can exclude applications from the usage insights (bar chart). To specify an excluded application, complete the following steps.

- Click **Add**.
- Type the name of the application as mentioned in the bar chart. When filling up the name of applications, an extension is not included.
- Press **Enter** to save or **Shift + Enter** to save and start another entry.
- You can also edit and delete the added application by following the wizard instructions.

Profile container insights

This feature monitors profile containers for Profile Management and FSLogix. It provides insights into the basic usage data of the profile containers, the status of sessions using the profile containers, the issues detected, and more.

Use this feature to stay on top of space usage for profile containers and to identify problems that prevent profile containers from working.

Summary

This page includes two doughnut charts. You can click each segment of the chart to drill down for more details.

- **Space usage**. The chart on the left side shows the space usage of profile containers over the specified time period. A numeric value represents the number of profile containers of that category.
- **Session Status**. The chart on the right side shows the results of attaching profile containers for sessions established over the specified time period. A numeric value represents the number of sessions of that category.

To view insights, select a configuration set and a date range and then click **Apply**. Then, the charts refresh to display relevant insights.

You can configure the following settings:

- **Space usage is high when used space is more than (GB)**. Lets you type a threshold value above which to treat the space usage of the profile containers as high. Type a positive integer.
- **Space usage is low when used space is less than (GB)**. Lets you type a threshold value below which to treat the space usage of the profile containers as low. Type a positive integer.

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

NOTE:

- The high threshold value must be greater than the low threshold value.
- After specifying the high and the low threshold values, click **Refresh** to trigger a refresh of the **Used Space** chart.
- After specifying the high and the low threshold values, space usage in between defaults to **Medium**.

Profile container status

This page displays a list of status records for profile containers over a specified time period. To filter records, select a configuration set and a date range and then click **Apply**. If necessary, you can use filters to refine the results further.

You can perform the following actions:

- **Columns to display**. Lets you customize the display of the table. When customizing columns, you must select at least two columns. After you complete your customization, the table refreshes to display the columns you select.
- **Refresh**. Updates the list of status records.
- **Get latest status**. Triggers the collection of data for the container the selected record pertains to. This option brings you up to date with the user's container status.

  NOTE:

  If the container is in use, the agent attempts to collect relevant data. If successful, the latest status is updated in the container's latest record. It might take a while for the update to complete. Click **Refresh** for the up-to-date record to appear.

The **Attach status** column displays information about status and error codes. For information about error codes, see the Microsoft documentation `<https://docs.microsoft.com/en-us/fslogix/fslogix-error-codes-reference>`.

The **Large file scan** column provides information on the results of the large file scan. To enable large file scanning for a configuration set, go to its **Advanced Settings > Insights** page. To view details of the large file scan results for a record, click **Results** in the relevant column field. The

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

large file scan wizard appears, presenting the results of the large file scan performed on the profile container. Files and folders smaller than 100 MB are not listed individually.

Reports

Provides reports that let you analyze your deployments.

Introduction

This page provides reports that let you analyze your deployments. Reports are generated on a per-event basis. However, not all events generate corresponding reports. Currently, events of the following types generate reports.

- **Application security logs**
  - Each time you enable the **Application security logs**, a corresponding record is generated. We consolidate those records into a single report every four hours. Within the details of each report, administrators can view the logs by subtype. The table includes information such as the filter used, **Event time**, **Event type**, **Result code**, **Result summary**, **Severity**, list of agents and users, and the **Configuration set**. The table also includes the following subtypes.
  - **EXE and DLL**
  - **MSI and script**
  - **Packaged app deployment**
  - **Packaged app execution**

    When you enable **Application security logs**, you can view all the four **EXE and DLL**, **MSI and script**, **Packaged app deployment**, and **Packaged app execution** subtype reports in the web console, but cannot view the report corresponding to each subtype separately. The table provides the logs for the fields **Time**, **Rule name**, **Event ID**, **Target**, and **Result**. The result of this selection can be **Allowed**, **Audited**, or **Blocked**.
- **Privilege elevation and process hierarchy control logs**
  - Each time you enable the **Privilege elevation** and **process hierarchy control** logs, a corresponding record is generated. We consolidate those records into a single report every four hours. Within the details of each report, administrators can view the logs by subtype. The table includes information such as the filter used, **Event time**, **Event type**, **Result code**, **Result summary**, **Severity**, list of agents and users, and the **Configuration set**. You can choose from the four security aspects to view more details.

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

- **EXE privilege elevation**. When the **EXE privilege elevation** subtype is selected, the table provides the logs for the fields **Time**, **Process**, **Command line**, **Rule name**, and **Result**. The result of the elevation can either be a success or a failure.
- **MSI privilege elevation**. When the **MSI privilege elevation** subtype is selected, the table provides the logs for the fields **Time**, **Packages**, **Command line**, **Rule name**, and **Result**. The result of the elevation can either be a success or a failure.
- **Self-elevation**. When the **Self-elevation** subtype is selected, the table provides the logs for the fields **Time**, **Process**, **Rule name**, **Reason** and **Result**. The result of the elevation can either be a success or a failure.

NOTE:

Enabling the **Show failures only** toggle displays only the records with the result **Failure** and hides the rest.

- **Process hierarchy control**. When you select the **Process hierarchy control** subtype, the table provides the logs for the fields **Time**, **Child process**, **Parent process ID**, **Rule name**, and **Result**. The result of this selection results in displaying either a blocked or allowed activity.

NOTE:

- You see the error icon on the security aspect tab when at least one failure occurs in each subtype.
- Enabling the **Show blocked only** toggle displays only the records with the result **Blocked** and hides the rest.

- **Action processing results**
  - Each time an action is assigned, a corresponding record is generated. We consolidate those records into a single report every four hours. The report includes all action processing results for the user logged on to the agent machine. You can select an action type to view details in a tabular format. The table includes information such as the name of the action, the user the action is assigned to, the filter used, and the processing result (status). There are three statuses:

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

    - **Applied (processed)**. Means that the action was applied to the target user successfully (or processed successfully).
    - **Outdated**. Means that the action processed is not the latest. This happens when an action gets updated but not yet applied.
    - **Error**. An error occurred while applying the action. To troubleshoot, enable debug mode to view the logs of the agent. See View log files.
  - Currently, you can view only Group Policy setting and JSON file processing results. To enable results collection, see Monitoring preferences.

- **Action processing events**

  This type of report is generated on demand for each action during agent processing. For example, you can configure the agent to collect output data from a script-based external task that generates console output logs. These reports provide detailed processing results, allowing you to view action outcomes directly in the WEM web console.

- **Scripted task**
  - Each time a task runs, a corresponding report is generated. The reports include information about when the task runs, the task execution results, and more.
  - Both built-in and custom tasks generate reports. In those reports, we provide predefined report data. When adding custom tasks, you can customize the data to be reported. If the predefined report data does not suit your needs, consider using the extended data for further analysis.

- **Profile container status**
  - Each time a profile container is attached, a corresponding attach record is generated. We consolidate those records into a single report on a daily basis. The report includes information about the basic usage data of the profile containers, the status of sessions using the profile containers, the issues detected, and more. With the information, you can track storage usage for profile containers and identify problems that prevent profile containers from working.

- **Optimization and usage**
  - With **Enable data collection and upload for optimization and usage insights** enabled for a configuration set on its **Advanced Settings > Insights** page, the agent collects and uploads optimization and usage data on a daily basis. A report based on the data collected is generated.

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

- **Optimization and usage insights**
  - Each time you apply insights for a configuration set, a corresponding report on optimization and usage is generated. The reports let you gain insights into application behavior. We aggregate usage and optimization insights into one report.

> **NOTE:**
>
> On the **Optimization Insights** or the **Usage Insights** page of **Monitoring > Insights**, you apply insights by selecting a configuration set and a date range. We maintain only one report for insights applied using the same configuration set and date range. Applying insights using the same configuration set and date range updates the report later.

- **Profile Management health check**
  - The agent runs Profile Management health checks every 24 hours or on demand. A corresponding report is then generated. The report contains the following elements:
    - Date and time when the report was generated
    - Detailed information such as the associated agent and configuration set
    - Issues (for example, errors and warnings) found, along with fix recommendations
  - To fix the errors/warnings and to reach the required profile management settings, click **More** > **Profile** > **View Profile Management health check report** in the **Statistics** tab of the **Agents** page, that leads you to the **Reports** page. You can then select **Profile Management Settings** under **Results** to change/update your Profile Management settings under the **Details** tab of the **Profile Management health check** page, that leads you to the Profile Management configuration page. You can cycle through all the errors/warnings in the footer that have the corresponding setting highlighted, and make the required change to the configuration.
  - To change your Profile Management settings, go to Profile Management Settings. To customize the scope of settings to cover in a report, go to Advanced Settings > Monitoring Preferences under that configuration set.
  - If you set the filter by selecting the **Application delivery task results** event type, the agent will display only the corresponding report. However, the **Application delivery task results** page provides only the **Raw data**.

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

Each report appears as a table record. Those reports provide useful diagnostic information that can inform your action. For example, you can check reports based on event severity. Based on the severity level, you can decide what action to take.

TIP:

We have pre-defined levels of severity for certain reports, for example, built-in scripted task reports.

For a scripted task, the **Result code** column can provide the following information:

- **0**: Indicates that the task has run successfully.
- **-4**: Appears when attempts to verify the checksum of the executable file you provided failed.
- **-5**: Appears when attempts to verify the signature of the executable file failed. Possible causes: no valid signature at the end of the executable file, or signature verification failure because of certificate missing.
- **-8**: Appears when the task was canceled due to a timeout.

For information about result codes (status codes) of profile container status, see the Microsoft documentation `<https://docs.microsoft.com/en-us/fslogix/fslogix-error-codes-reference>`. Remember: "-1" means that WEM might not retrieve the status code.

- **VHD disk compaction**: Each time Citrix Profile Management VHD disk compaction is completed, a corresponding report is generated. The report includes information about the container, trigger condition, size before compaction, size after compaction, and more. With the information obtained, you can effectively track changes in container storage usage. To enable the reports collection for VHD disk compaction, see Monitoring preferences.

Columns to display and filters

You can customize the display of the table. Click **Columns to display** to choose which columns you want to display. When customizing columns, you must select at least two columns. After you complete your customization, the table refreshes to display the columns you select.

You can click a column header to sort. You can apply filters to filter reports. You can also save the filters used as filter sets and directly manage these filter sets.

You can **Apply filter set** to apply a filter set and select **Delete** to delete a filter set in the **Manage filter sets** page.

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

View more details of a report

You can select a report for more detailed information. To do that, locate the report and then click the ellipsis on the right. The report wizard appears. It contains two tabs:

- **Details**. Provides a detailed result summary.
- **Raw data**. Provides raw data related to the report. The extended data is in JSON format. If needed, use the extended data for further analysis.

For a scripted task that has **Highlight regular expression matches** enabled, you can see the following option on the **Details** tab of its report:

- **View regular expression matches**. Lets you view regular expression matches in detail.

Export reports

You can export the data in each report in CSV or JSON format. To do that, perform the following steps:

1. Click **Export**. The export wizard appears.
2. Select the export format from the following options:
    - **CSV**. This option exports raw data in CSV format.
    - **CSV (formatted)**. This choice enhances the readability of extended data in CSV format.
    - **JSON**. This option exports raw data in JSON format.
    - **JSON (formatted)**. This choice improves the readability of extended data in JSON format.

In addition, the formatted options can parse the script task reports into variables if the report content follows the format `variable = value` or `variable: value`. However, if you choose the **CSV (formatted)** option, some of the excessive number of columns might be omitted in the exported data.

1. Optionally, select **Save a copy of the export to your local machine**. The export will be saved to the default download location of your browser.
2. Click **Export** to start the export process.

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

IMPORTANT:

- You can export up to 50,000 records (reports). When the number of records to export exceeds the limit, only the top 50,000 are exported. We recommend using filters to reduce the number of records to 50,000 or fewer.
- While an export is in progress, you cannot perform another export.
- If an export does not complete within 30 minutes, you will no longer receive notifications about it. Go to **Files** to view the export result later.
- When exporting reports, the export will be saved to the cloud storage. The cloud storage has a storage limit. When you reach the limit, you cannot proceed with the export. In that case, go to **Files** and delete unnecessary files to free up space. See Files.

Export to third-party platform

By exporting report data to a third-party platform, you can analyze and monitor the execution of tasks seamlessly. You can also complete some customized special requirements in the third-party platforms, such as VDA host information, CPU utilization, memory utilization, and so on.

You can export reports to third-party platforms either manually or automatically.

Manually export to third-party platform

To manually export the data in each report to a third-party platform, perform the following steps:

1. Click **Export > Export to third-party platform**.
2. In the **Export to third-party platform** pane, pick one of the third-party platform names in the **Destination** dropdown or select **Add new**.

   NOTE:

   Currently, Grafana and Splunk are the supported third-party platforms.

   If you select **Add new** in the **Add destination** pane, enter the required third-party platform details.
3. Click **Export**. After the export process is complete, you can go to the destination location (in this case, Grafana) and see the exported report data.

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

Automatically - Configure automatic report

To automatically export the data in each report to a third-party platform, perform the following steps:

1. Click **Export > Configure automatic report**.
2. In the **Configure automatic export** pane, click **Add rule**.
3. In the **Add rule** pane, enter the required third-party platform details.
4. Click **Done** to save the configuration changes of the newly added rule.

Scripts for scripted tasks

Introduction

This page lets you manage scripts that you can automate or run on your WEM agents. Scripts are organized into the following categories:

- Built-in scripts

  Ready-to-use scripts for common VDA administration and troubleshooting needs.

- Custom scripts

  Administrator-created scripts for environment-specific automation and operational requirements.

NOTE:

To configure automated tasks from a script, go to Scripted tasks in a configuration set.

Add a custom script

The **Scripted Tasks** page lists all built-in scripts and any custom scripts created by you or other administrators. You can add additional custom scripts as needed to meet your requirements.

Before you begin

Before you create a custom script in WEM web console:

- Create script content

  Write a PowerShell script based on your requirements.

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

- Validate and export the script content

  Use the **Citrix Environment Tool Hub > Scripted Task Validator** tool to run the script and review the execution results. If needed, you can export the script for later import into the WEM Web console.

  For more information, see Validate and export a scripted task.

Workflow

To add a custom script, perform the following steps:

1. On the **Scripted Tasks** page, click **Add script**.
2. In the **Add script** wizard, configure the following settings and then click **Save**.

   - **Script name**. Specify a name for the script.
   - **Tags**. Select from existing tags or enter tags separated by commas. A tag must be no more than 20 characters long. Tags are like keywords or labels. Using tags enables you to identify your scripts in new ways. Also, they act as filters, letting you rearrange your view of scripts depending on criteria that are important to you. You can use as many tags as you like.
   - **Description**. Optionally, specify additional information to help you identify the script.
   - **File type**. Select a file type for the script. Two types of files are supported:

     - **PowerShell**. Individual PowerShell script files.
     - **ZIP**. Multiple files bundled into a single zip file. Zip files larger than 10 MB are not supported. After uploading a zip file, specify an entry point, indicating which file to run at the beginning of the script. Keep in mind that the entry point file must be no more than three levels deep in the folder structure.

   - **Upload file.** Click **Browse**, navigate to the file, select it, and then click **Open**. You are returned to the **Add script** wizard.

     TIP:

     You can upload a script in two ways:

     - Select a .zip file that you've already placed on the Web Console machine.
     - After exporting a script with the Scripted Task Validator tool, the content is automatically copied to your clipboard. On the **Add Script** page, paste the content directly from the

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

clipboard (<Ctrl+V>). This method avoids the need to store a .zip file on the web console machine.

- **Grant permissions**. Specify the level of access that you want to grant to the script. Ensure that you understand the permissions associated with each option.
  - **Full access**. A script assigned Full access has extensive local access. If selected, the script is granted permissions as if it runs under the local system account.
  - **Limited access (with network access)**. A script assigned Limited access (with network access) does not have extensive local access but can access network resources. If selected, the script is granted permissions as if it runs under the network service account.
  - **Limited access (without network access)**. A script assigned Limited access (without network access) does not have extensive local access and cannot access network resources. If selected, the script is granted permissions as if it runs under the local service account.
  - **Run as logged-on user**. If selected, the script runs in the context of a logged-on user's session and is granted the same permissions, regardless of whether the user session is active or disconnected.

  For more information, see the Microsoft documentation `<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-identifiers#well-known-sids>`.
- **Working folder**. Optionally, type the absolute path of the local folder on the end-user operating system. The working folder is the current folder for the file when it starts. You can build the path with environment variables (for example, %ProgramFiles%). If unspecified, `$PSScriptRoot` is used as the default working folder. For more information about `$PSScriptRoot`, see the Microsoft documentation `<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_automatic_variables?view=powershell-7.1>`.
- **Does this task generate output files**. Choose whether the script you add generates output files.
- **Output path**. Type a path relative to the folder where the file resides. The path must contain the file name and the file name extension. Example: `output\report.txt`.

Manage scripts

You can manage scripts to meet your needs. Available actions include:

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

- Edit a script
- Delete a script
- Clone a script
- Configure tasks from a script

Edit a script

To edit a script, perform the following steps:

1. On the **Scripted Tasks** page, locate the script. Use the search box or tags to find it quickly if needed.
2. Click the ellipsis of the script and then select **Edit script**. The **Edit script** wizard appears.
3. On the **Task info** tab, configure settings as needed.
4. On the **Script file** tab, view the script content.
5. Click **Save**.

NOTE:

You cannot edit built-in scripts.

Delete a script

To delete a script, perform the following steps:

1. On the **Scripted Tasks** page, locate the script. Use the search box or tags to find it quickly if needed.
2. Click the ellipsis of the script and then select **Delete script**.

IMPORTANT:

You cannot delete built-in scripts.

Clone a script

To clone a script, perform the following steps:

1. On the **Scripted Tasks** page, locate the script. Use the search box or tags to find it quickly if needed.
2. Click the ellipsis of the script and then select **Clone script**.

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

NOTE:

When cloning a script, you are prompted to change the name to avoid duplicate names.

Configure tasks from a script

To configure and automate tasks from a script, perform the following steps:

1. On the **Scripted Tasks** page, locate the script. Use the search box or tags to find it quickly if needed.
2. Click the ellipsis of the script and then select **Configure tasks**.
3. In the **Select configuration set** wizard, choose the configuration set where you want to create the task.
4. Follow the steps in Create a scripted task to complete the configuration.

Built-in scripts

Currently, we provide the following built-in scripts for you to use:

- Cloud Health Check
- Windows Service Management
- Server Reboot
- CDF Tracing Management
- AOT Log Collection
- Check DNS Settings
- Check RDS License
- Diagnose VDA Unregistration
- Run Profile Management Health Check
- Set Profile Reset Trigger

Cloud Health Check

Lets you run checks that gauge the health of Virtual Delivery Agents (VDAs). VDA health checks identify possible causes for common VDA registration and session launch issues. Cloud Health Check runs under the local system account on the agent host.

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

Windows Service Management

Windows service management provides frequently used features regarding Windows service, such as start, stop, restart, configure one or more Windows services.

Restart Windows Service

This script checks the status of a Windows service. If the service is not currently running and the `ForceStart` parameter is specified, the script starts the service. Regardless of the current state, if the service is running and does not require forceful starting, it is restarted to ensure it's operating on the latest configuration or to recover from a stalled state.

Parameters

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`ServiceNames`	string	BrokerAgent	False	Specifies the names of the services to be managed. If not provided, defaults to `BrokerAgent`. If you need to input more than one service, separate the service names with a comma. All spaces would be trimmed. For example, ServiceA, ServiceB.
`ForceStart`	boolean	true	False	Indicates whether to start the service if it's found to be not running. It does not affect running services.

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

NAME	TYPE	DEFAULT	MANDATORY	NOTE
				Running services are always restarted for maintenance or recovery purposes.

Stop Windows Service

This script stops a list of specified Windows services. The script checks if each service is installed and attempts to force-stop the service. The script then verifies whether the service has successfully stopped and reports the status.

Parameters

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`ServiceNames`	string	BrokerAgent	False	Specifies the names of the services to be managed. If not provided, defaults to `BrokerAgent`. If you need to input more than one service, separate the service names with a comma. All spaces would be trimmed. For example, ServiceA, ServiceB.

Configure Windows Service

This script adjusts Windows service configurations, including startup type and recovery actions.

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

Parameters

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`ServiceNames`	string	null	true	Specifies the names of the services to be managed. If not provided, defaults to `BrokerAgent`. If you need to input more than one service, separate the service names with a comma. All spaces would be trimmed. For example, ServiceA, SerivceB.
`StartupType`	string	null	False	Sets the startup type of the service. Valid options are Automatic, Manual, or Disabled.
`FirstFailureAction`	string	null	False	Defines the action for the first failure. For example, restart/none.
`SecondFailureAction`	string	null	False	Defines the action for the second consecutive failure.

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

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`SubsequentFailureAction`	string	null	False	Defines the action for all subsequent failures after the second.

Server Reboot

Reboot Machine

This script restarts the local machine with an optional delay and force option.

Parameters

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`Force`	boolean	true	False	If specified, force an immediate restart, ignoring any unsaved data or active user sessions.
`Delay`	int	10	False	Specifies the delay in seconds before the computer is restarted. Must be between 3 and 30 seconds. Defaults to 10 seconds.

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

CDF Tracing Management

Start CDF Tracing

This script starts the CDF tracing process using either a single CTL file or a predefined CTL file category as input. It traces the modules defined in the selected CTL files and automatically stops `cdfcontrol.exe` after the duration specified by the `RunMinutes` parameter.

Parameters

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`traceOutputPath`	string	`C:\ProgramData\Citrix\WEM\CDFLogs`	False	Specifies the output path of CDF reports.
`category`	string	`all`	False	Specifies the predefined categories to start the trace with. Supported values are: • `all` • `always on tracing` • `desktop Server os vda`

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

NAME	TYPE	DEFAULT	MANDATORY	NOTE
				• `delivery controller` • `federated authentication service` • `provisioning service` • `universal print server` • `citrix director` • `citrix studio` • `session recording administration`

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

NAME	TYPE	DEFAULT	MANDATORY	NOTE
				• `session recording player` • `citrix workspace app for windows`
`ctlFilePath`	string	null	False	Specifies the `ctl` file to start the trace with.
`RunMinutes`	Integer	30	False	Specifies how long `cdfcontrol.exe` runs before it automatically stops and exits.

Stop CDF Tracing

This script stops the CDF tool tracing.

CDF Logs Cleanup

It is useful to clean up the CDF tracing logs to save storage consumption. It should provide a function to remove CDF files under the given directory.

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

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`FileAgeDays`	int	3	False	Specifies the age threshold in days. Files and folders older than this value are deleted. The default value is 3 days and this parameter is optional. All the files or directors are deleted if the `FileAgeDays` is less than 1 day.

AOT Log Collection

This script is a comprehensive automation tool designed for collecting and processing Citrix AOT logs. It integrates with **Citrix CDFControl** to configure trace collection, apply filtering (default: `Level=1, Class=Failure`), and convert ETL (Event Trace Log) files into a readable CSV format for analysis.

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`StartTime`	`[DateTime]`	`EndTime - 30 minutes`	False	Specifies the start time for log filtering
`EndTime`	`[DateTime]`	Current date and time	False	Specifies the end time for log filtering

Check DNS Settings

This script is a comprehensive DNS health check tool designed for Citrix VDA environments. It validates DNS configuration and performs troubleshooting to identify potential DNS-related issues that might affect Citrix services.

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

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`DomainName`	`[string]`	Not Applicable	False	Specifies the domain name to test DNS resolution (enables DNS Name Resolution test)
`FlushDNS`	`[switch]`	False	False	Specifies whether to flush the DNS cache as a standalone action

Check RDS License

This script is a comprehensive Remote Desktop Services (RDS) license validation tool designed to check RDS licensing configuration and status on local computers. It is particularly useful in Citrix VDA environments, where RDS licensing compliance is essential for proper operation. Use this script to ensure licensing compliance and maintain uninterrupted multi-session user access.

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`DomainName`	`[string]`	Not Applicable	False	Specifies the domain name to test DNS resolution (enables DNS Name Resolution test)
`FlushDNS`	`[switch]`	False	False	Specifies whether to flush the DNS cache as a standalone action

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

Diagnose VDA Unregistration

This script is a comprehensive diagnostic tool designed to troubleshoot Citrix Virtual Delivery Agent (VDA) unregistration issues. It performs multiple health checks and diagnostic procedures to identify potential causes of VDA unregistration problems in Citrix environments.

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`StartTime`	`[DateTime]`	`EndTime - 30 minutes`	False	Specifies the start time for log filtering
`EndTime`	`[DateTime]`	Current date and time	False	Specifies the end time for log filtering

Run Profile Management Health Check

This script performs a comprehensive health check of your Citrix Profile Management deployment. It scans configurations for potential issues and analyzes logs to detect critical problems, such as temporary profile errors and significant time gaps during logons.

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`CtxSessionKey`	[string]	null	False	Specifies the **Citrix session** key used to search for specific session logs. If not specified, the script analyzes sessions from the past 24 hours.
`LogonTime`	[string]	null	False	Specifies the logon time to filter event log searches. Accepts various date and time formats. If not

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

NAME	TYPE	DEFAULT	MANDATORY	NOTE
				specified, the script filters event logs from the past 24 hours.
`StructuredOutputOnly`	[switch]	True	False	Specifies whether to output structured JSON data without console logging.
`Parallel`	[switch]	True	False	Specifies whether to use parallel processing for log analysis operations to improve performance.

Set Profile Reset Trigger

This script sets a trigger to reset a user's profile. During the user's next logon, the existing profile is backed up, and a new clean profile folder is created.

NAME	TYPE	DEFAULT	MANDATORY	NOTE
`CtxSessionKey`	[string]	null	True	Specifies the Citrix session key used to trigger a profile reset for the user’s next logon.
`FoldersToRestore`	[string]	null	False	Specifies the folders to restore after a

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

NAME	TYPE	DEFAULT	MANDATORY	NOTE
				profile reset. If not specified, known folders such as **Downloads**, **Desktop**, and **Pictures** are restored by default.
`BackupNameSuffix`	[string]	null	False	Specifies the suffix for the backup folder name during a profile reset. If not specified, the suffix defaults to `upm_%CurrentTimeStamp%`.

More information

For examples of how to use scripted tasks, see:

- Analyze logon duration using scripted tasks
- Automatically apply Windows updates using scripted tasks

Files

This page lets you manage all your files on your configured data folder. If necessary, delete files to free up space.

Files of the following types take up your storage space:

- Configuration set backups
- Reports
- Scripted tasks

Currently, you can download and delete files available on the storage.

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

NOTE:

- Backup and restore files are not shown here but they take up storage space.
- You can't delete files associated with scripted tasks. To delete them, delete their tasks.

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

Manage Basic Deployment agents

You can use Workspace Environment Management™ (WEM) to manage basic deployment agents. This feature provides a lightweight method to deploy WEM. You can use this deployment method for utilizing WEM basic functionalities easily without deploying the backend components such as broker, database and consoles.

Configuring the basic deployment agent settings

When WEM agent is in basic mode, some optimization features are enabled by default. These settings are stored in the pre-defined agent cache file.

- CPU Spike Protection on VDA machines is automatically turned on. This setting lowers the priority of high CPU processes to minimize the impact on the user experience:
  - CPU spike protection
  - Automatically prevent CPU spikes
  - Enable intelligent CPU optimization
- Customize the settings for basic deployment agent. For more information, see Configure group policies. The settings available for the basic mode are listed as follows:

PROPERTY	TYPE	SETTING	DEFAULT	EXAMPLE	NOTE
enableCpuSpikeProtection	boolean	Enable CPU spike protection	true	true	CPU spike protection settings
enableCpuAutoProtection	boolean	Automatically prevent CPU spikes	true	true	
cpuUsageLimitOfSpikeProtection	float	CPU usage limit (%)	70.0	70.0	

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

PROPERTY	TYPE	SETTING	DEFAULT	EXAMPLE	NOTE
enablePerCoreCpuUsageLimit	boolean	Set limit relative to single CPU core	false	false	
perCoreCpuUsageLimitOfSpikeProtection	float	CPU usage limit relative to single CPU core (%)	80.0	80.0	
cpuUsageLimitSampleTimeOfSpikeProtection	integer	Sample time limit (sec)	30	30	
idlePriorityTimeOfSpikeProtection	integer	Idle priority time (sec)	180	180	
enableLimitCpuCoreUsage	boolean	Enable CPU core usage limit	false	false	
cpuCoreLimitOfSpikeProtection	integer	CPU core usage limit	1	1	
enableIntelligentCpuOptimization	boolean	Enable intelligent CPU optimization	true	true	
enableIntelligentIoOptimization	boolean	Enable intelligent I/O optimization	false	false	
excludeProcessesFrom	boolean	Exclude processes from CPU	false	false	

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

PROPERTY	TYPE	SETTING	DEFAULT	EXAMPLE	NOTE
CpuSpikeProtection		spike protection			
processesExcludedFromCpuSpikeProtection	array of strings	Process names	[]	["devenv", "msbuild"]	
disableProcessPriorityInheritance	boolean	Prevent child processes from inheriting CPU priority	false	false	
parentProcessesToDisablePriorityInheritance	array of strings	Process names	[]	["devenv", "msbuild"]	
enableMemoryWorkingSetOptimization	boolean	Optimize memory usage for idle processes	true	true	Memory optimization settings
idleSampleTimeOfMemoryWorkingSetOptimization	integer	Idle sample time (min)	30	30	
idleStateLimitOfMemoryWorkingSetOptimization	integer	Idle state limit (%)	1	1	
enableMemoryOptimizat	boolean	Restrict optimization	true	true	

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

PROPERTY	TYPE	SETTING	DEFAULT	EXAMPLE	NOTE
ionThreshold					
memoryOptimizationThreshold	integer	Optimize only if total available memory is less than (MB)	200	200	
excludeProcessesFromMemoryWorkingSetOptimization	boolean	Exclude processes from memory usage optimization	false	false	
processesExcludedFromMemoryWorkingSetOptimization	array of strings	Process names	[]	["devenv", "msbuild"]	
enableFastLogoff	boolean	Enable fast logoff	true	true	Fast Logoff settings
enableMultiSessionOptimization	boolean	Enable multi-session optimization	true	true	Multi-session optmizations
excludeProcessesFromMultiSessionOptimization	boolean	Exclude processes from multi-session optimization	false	false	
processesExcludedFromMultiSessi	array of strings	Process names	[]	["devenv", "msbuild"]	

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

PROPERTY	TYPE	SETTING	DEFAULT	EXAMPLE	NOTE
onOptimization					
agentServiceDebugModeEnabled	boolean	Enable agent service debug mode	false	false	Advanced settings > Agent settings > Agent service options
enableLogonDurationAnalysis	boolean	Enable logon duration analysis	true	true	Logon duration analysis
useAlternativeLocalReportLocation	boolean	Use alternative location to save local agent reports	false	false	
alternativeLocalReportLocation	string	Alternative location to save local agent reports	`%PROGRAMDATA%\Citrix\WEM\Local Agent Reports`	`D:\WEM Local Agent Reports`	
localReportMaxDays	int	Max days for local agent reports to be kept	7	7	
localReportMaxFilesPerEvent	int	Max number of local agent	30	30	

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

PROPERTY	TYPE	SETTING	DEFAULT	EXAMPLE	NOTE
		reports to be kept			
saveLogonDurationAnalysisToLocal	boolean	Save logon duration analysis reports as local agent reports	true	true	
saveUpmHealthCheckToLocal	boolean	Save UPM health check reports as local agent reports	true	true	
saveProfileContainerInsightsToLocal	boolean	Save profile container insights reports as local agent reports	true	true	
launchAgentOnLogon	boolean	Launch agent automatically when users logon	false	true	
enableAgentInsightsManagement	boolean	Enable agent insights management	false	true	Agent Insights settings
enableLargeFileScan	boolean	Enable large file scan in the profile container	false	true	

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

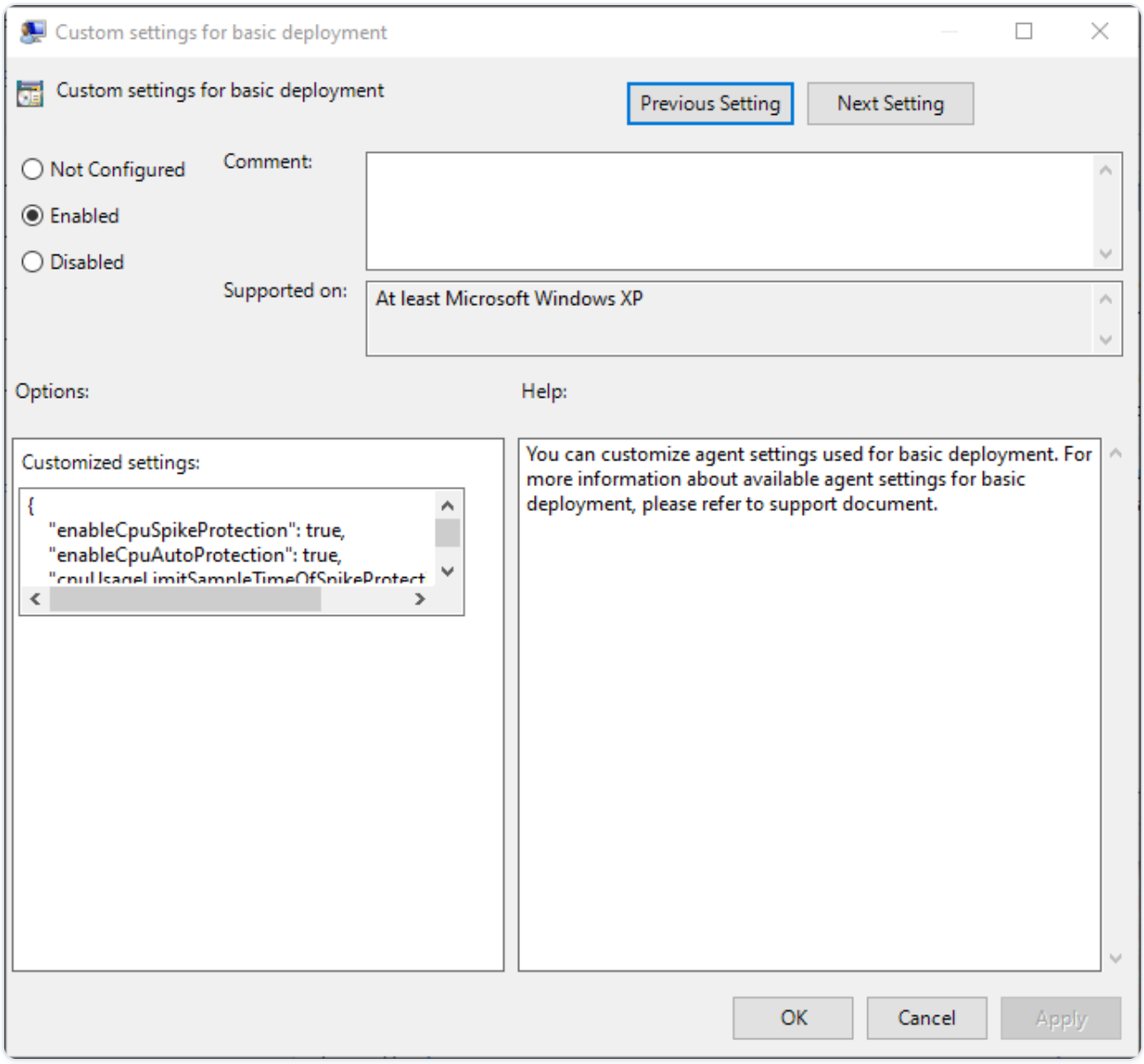
NOTE:

If the custom settings are not configured or are invalid, the WEM agent uses the default settings.

You can specify a JSON formatted string to customize settings for basic deployment agent. For example:

```
{

    "enableCpuSpikeProtection": true,

    "enableCpuAutoProtection": true,

    "enableIntelligentCpuOptimization": true,

}
```

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



Switching the agent deployment type

To switch the deployment type, choose one of the following methods.

- Utilize the agent group policies to switch the agent to another deployment type. For more information, see Configure group policies.
- Use the WEM health check tool to switch to another deployment type.

Using the WEM Logon duration feature

The benefits of using the WEM Logon duration feature are as follows:

- The WEM agent analyzes the logon duration and generates the report automatically when you log in to the agent machine.

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

- You can use the Citrix Environment Tool Hub to check the agent-generated report.

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

User experience

Start the administration console

1. From the **Start** menu select **Citrix \> Workspace Environment Management \> WEM Administration Console**. By default, the administration console launches in a disconnected state.
2. On the administration console ribbon click **Connect**.
3. In the New Infrastructure Server Connection window, type the address of your infrastructure server and click **Connect**.

Configure your installation

In the administration console:

1. Click menu items in the lower-left-hand pane to display their subsections in the pane above them.
2. Click subsection items to populate the main window area with appropriate content.
3. Change configuration as required. For more information about the settings you can use, see the user interface reference.

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

Manage (legacy console)

Use the following articles to perform specific tasks:

- Ribbon
- Actions
- Filters
- Assignments
- System Optimization
- Policies and Profiles
- Security
- Active Directory Objects
- Transformer settings
- Advanced settings
- Administration
- Monitoring
- Back up and restore

Ribbon

Home tab

The **Home tab** contains the following controls:

Connect. Connects administration console to the specified infrastructure server. In the **New Infrastructure Server Connection** dialog, specify:

- **Infrastructure server name**. Name of the infrastructure server you want to connect to.
- **Administration port**. Port on which you want to connect to the infrastructure service. Default value of 8284 is pre-populated.

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

Disconnect. Disconnects administration console from the current infrastructure service. This lets the administrator manage multiple infrastructure services from a single console, by disconnecting from one and connecting to another.

Configuration set. Switches from one Workspace Environment Management™ (WEM) site (configuration set) to another.

Create. Opens the Create configuration set window. Allows you to configure multiple WEM sites (configuration sets).

- **Name**. Site (configuration set) name as it appears in the configuration set list in the Ribbon.
- **Description**. Site (configuration set) description as it appears in the site edition window.
- **Site State**. Toggles whether the site (configuration set) is Enabled or Disabled. When Disabled, the WEM Agents cannot connect to the site (configuration set).

Edit. Opens the Edit configuration set window, with similar options to the Create configuration set window.

Delete. Deletes the site (configuration set). You cannot delete "Default site" because it is required for WEM to function. You can, however, rename it.

Refresh. Refreshes the site (configuration set) list.

NOTE:

The list does not automatically refresh when sites are created from different administration consoles.

Backup. Opens the **Backup** wizard to save a backup copy of your current configuration to the WEM administration console machine. You can back up actions, settings, security settings, and Active Directory (AD) objects.

- **Actions**. Backs up selected WEM actions. Each type of action is exported as a separate XML file.
- **Settings**. Backs up selected WEM settings. Each type of setting is exported as a separate XML file.
- **Security Settings**. Backs up all settings present on the Security tab. Each type of rule is exported as a separate XML file. You can back up the following items associated with a configuration set:

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

    - **AppLocker Rule Settings**
    - **Privilege Elevation Settings**

- **AD objects**. Backs up the users, computers, groups, and organizational units that WEM manages. The **Backup** wizard lets you specify which type of AD objects to back up. There are two types of AD objects:

    - Users. Single users and user groups
    - Machines. Single machines, machine groups, and OUs

- **Configuration set**. Backs up the WEM configuration set you selected. Each type of configuration set is exported as a separate XML file. You can back up only the current configuration set. You can back up the following items associated with a configuration set:

    - Actions
    - AppLockers
    - Assignments (related to actions and action groups)
    - Filters
    - Users
    - Settings (WEM settings)

    You cannot back up the following:

    - AD objects related to machines (single machines, machine groups, and OUs)
    - Monitoring data (statistics and reports)
    - Agents registered with the configuration set

Restore. Opens the **Restore** wizard to revert to a previously backed up version of your WEM service configuration. When prompted, select the applicable folder that contains the backup copies (.XML files).

- **Security Settings**. Restores all settings present on the Security tab. The settings in the backup files *replace* the existing settings in your current configuration set. When you switch to or refresh the **Security** tab, invalid application security rules are detected. Those rules are automatically deleted. Deleted rules are listed in a report that you can export if needed. The **Restore** wizard lets you select what to restore:

    - **AppLocker Rule Settings**
    - **Privilege Elevation Settings**

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

    - **Overwrite Existing Settings**. Controls whether to overwrite existing privilege elevation settings when there are conflicts.

  In the **Confirm Application Security Rule Assignment** dialog, select **Yes** or **No** to indicate how you want the **Restore** wizard to handle application security rule assignments:

    - If you select **Yes**, restore attempts to restore rule assignments to users and user groups in your current site. Reassignment succeeds only if the backed up users or groups are present in your current site or AD. Any mismatched rules are restored but remain unassigned, and they are listed in a report dialog which you can export in CSV format.
    - If you select **No**, all rules in the backup are restored without being assigned to users and user groups in your site.

- **AD objects**. Restores the backed up AD objects to the existing site. The **Restore** wizard gives you granular control over AD objects to be imported. On the **Select the AD objects you want to restore** page, you can specify which AD objects you want to restore and whether to overwrite (replace) existing WEM AD objects.
- **Configuration set**. Restores the backed up configuration set to WEM. You can restore only one configuration set at a time. It might take some time for the WEM administration console to reflect the configuration set you restored. To view the restored configuration set, select it from the Configuration set menu in the Ribbon. When restoring a configuration set, WEM automatically renames it to `<configuration set name>_1` if a configuration set with the same name already exists.

NOTE:

- Restored actions are *added* to existing site actions.
- Restored settings *replace* existing site settings.
- Restored AD objects are *added* to or *replace* existing site AD objects, depending on whether you selected **Overwrite mode** in the AD objects page of the Restore wizard.
- If you selected **Overwrite mode**, all existing AD objects are deleted before the restore process starts.

Migrate. Opens the **Migrate** wizard to migrate a zip backup of your Group Policy Objects (GPOs) to WEM.

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

IMPORTANT:

- The **Migrate** wizard migrates only the settings (GPOs) that WEM supports.
- We recommend that you back up your existing settings before you start the migration process.

We recommend that you perform the following steps to back up your GPOs:

1. Open the Group Policy Management Console.
2. In the **Group Policy Management** window, right-click the GPO you want to back up and then select **Back Up**.
3. In the **Back Up Group Policy Object** window, specify the location where you want to save the backup. Optionally, you can give the backup a description.
4. Click **Back Up** to start the backup and then click **OK**.
5. Navigate to the backup folder and then compress it into a zip file.

NOTE:

WEM also supports migrating zip files that contain multiple GPO backup folders.

After you back up your GPOs successfully, click **Migrate** to migrate your GPOs to WEM. On the **File to Migrate** page, click **Browse** and then navigate to the applicable file.

- **Overwrite**. Overwrites existing WEM settings (GPOs) when there are conflicts.
- **Convert**. Converts your GPOs to XML files suitable for import to WEM. Select this option if you want to have granular control over settings to be imported. After the conversion completes successfully, use the **Restore** wizard to manually import the XML files.

  NOTE:

  You can name the output folder, but you cannot specify the names for the files to be saved.

About tab

The **About tab** contains the following controls:

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

Configure License Server. Allows you to specify the address of your Citrix License Server, without which the administration console does not let you modify any settings. Alternatively, you can use the **Licensing** tab in the Infrastructure Services Configuration utility to specify these credentials. Citrix License Server information is stored in the same location in the database in both cases.

Get Help. Opens the Citrix Product Documentation website in a web browser window.

Options. Opens the **Administration Console Options** dialog. These options are specific to this local instance of the administration console.

- **Auto Admin Logon**. If enabled, the administration console automatically connects to the last infrastructure service it connected to at startup.
- **Enable Debug Mode**. Enables verbose logging for the administration console. Logs are created in the root of the current user "Users" folder.
- **Console Skin**. Allows you to select from various skins for the administration console only.
- **Port Number**. Allows you to customize the port on which the administration console connects to the infrastructure service. This port must match the port configured in the infrastructure services configuration.

About. Lists the current version of the administration console and licensing (license type, registration, and count) and legal information.

Actions

Workspace Environment Management™ streamlines the workspace configuration process by providing you with easy-to-use actions. The actions include managing applications, printers, network drives, external tasks, and more. You can use assignments to make actions available to users. Workspace Environment Management also provides you with filters to contextualize your assignments.

- Actions include managing:
  - Action Groups
  - Group Policy Settings
  - Applications
  - Printers
  - Network Drives

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

    - Virtual Drives
    - Registry Entries
    - Environment Variables
    - Ports
    - Ini Files
    - External Tasks
    - File System Operations
    - User DSN
    - File Associations
- Filters
- Assignments

Action Groups

The action groups feature lets you first define a group of actions and then assign all the defined actions in the action group to a user or user group in a single step. With this feature, you no longer have to assign each action present in the **Actions** pane one by one. As a result, you can assign multiple actions in a single step.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Action group list

Action groups

Displays a list of your existing action groups. Use **Find** to filter the list by name, display name, or description.

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

Actions

IMPORTANT:

- The action group includes only actions already present in each action category (applications, printers, and network drives, and so on). For example, unless you have added applications on the **Application List** tab, the action groups on the **Action Group List** tab do not display any applications available for you to assign under **Applications**.
- If you configure the options for actions in an assigned action group (**Action Group List > Name > Configured**), the configured options will not impact the users to which the action group is assigned.

The **Actions** section displays the actions available to you. You can perform the following operations:

- **Add**. Lets you create an action group that contains all the actions you want to assign to a user or user group.
- **Edit**. Lets you edit an existing action group.
- **Copy**. Lets you replicate an action group from an existing one.
- **Delete**. Lets you delete an existing action group.

To create an action group, follow the steps below.

1. On the **Administration Console > Actions > Action Groups > Action Group List** tab, click **Add**.
2. In the **New Action Group** window, type the required information, select the applicable option from the dropdown, and then click **OK**.

To edit an action group, select the applicable group from the list and then click **Edit**.

To clone an action group, select the group you want to clone and then click **Copy**. Note that the clone is automatically created after you click **Copy**. The clone inherits the name of the original and has a suffix “-Copy.” You can click **Edit** to change the name.

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

NOTE:

When you clone an action group, actions (if any) associated with the Network and Virtual Drives are not cloned unless the **Allow Drive Letter Reuse in assignment process** option is enabled. To enable that option, go to the **Advanced Settings > Configuration > Console Settings** tab.

To delete an action group, select the applicable group from the list and then click **Delete**.

NOTE:

If you delete or edit an action group that is already assigned, the changes you make will impact all users to which the group is assigned.

Fields and controls

Name. The display name of the action group, as it appears in the action group list.

Description. Lets you specify additional information about the action group.

Action Group State. Toggles the action group between enabled and disabled state. When disabled, the agent does not process the actions included in the action group even if you assign that action group to a user or user group.

Configuration

Lets you search for the specific action that you want to assign or you have configured. Use Find to filter the option by name, display name, or description.

Available. These are the actions available to you to add to the action group you created.

Click the plus sign to expand the actions under the specific action category. Double-click an action or click the arrow buttons to assign or unassign it.

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

NOTE:

- If you add an action to an action group that is already assigned to users, the action will be assigned to those users automatically.
- If you delete an action from an action group that is already assigned to users, the action will be unassigned from those users automatically.

Configured. These are the actions already assigned to the action group you created. You can expand individual actions to configure them. You can also configure the options for each specific action; for example, application shortcut locations, default printers, drive letter, and so on.

Assignments

IMPORTANT:

If you configure the options for actions in an assigned action group in the Assigned pane on the **Action Assignment** tab, the configured options will automatically impact the users to which the action group is assigned.

After you finish configuring the actions for the action group on the **Actions > Action Groups > Action Group List** tab, you might want to assign the configured actions to the applicable user or user group. To do so, go to the **Assignments > Action Assignment > Action Assignment** tab. On that tab, double-click a user or user group to see the Action Groups node in the **Available** pane that contains the action groups you created. You can click the plus sign next to the Action Groups node to view the action groups you created. Double-click an action group or click the arrow buttons to assign or unassign it. When you assign an action, you are prompted to select the rule you want to use to contextualize that action.

For more information about how assignments work, see Assignments.

When assigning action groups, there are several scenarios to be aware of:

- If you assign an action group, all actions included in it are assigned.
- One or more actions might overlap in different action groups. For overlapping action groups, the group that is processed last overwrites groups that were processed earlier.
- After the actions in an action group are processed, consider assigning the actions that overlap with those in another action group. In this case, the unassigned actions overwrite those that

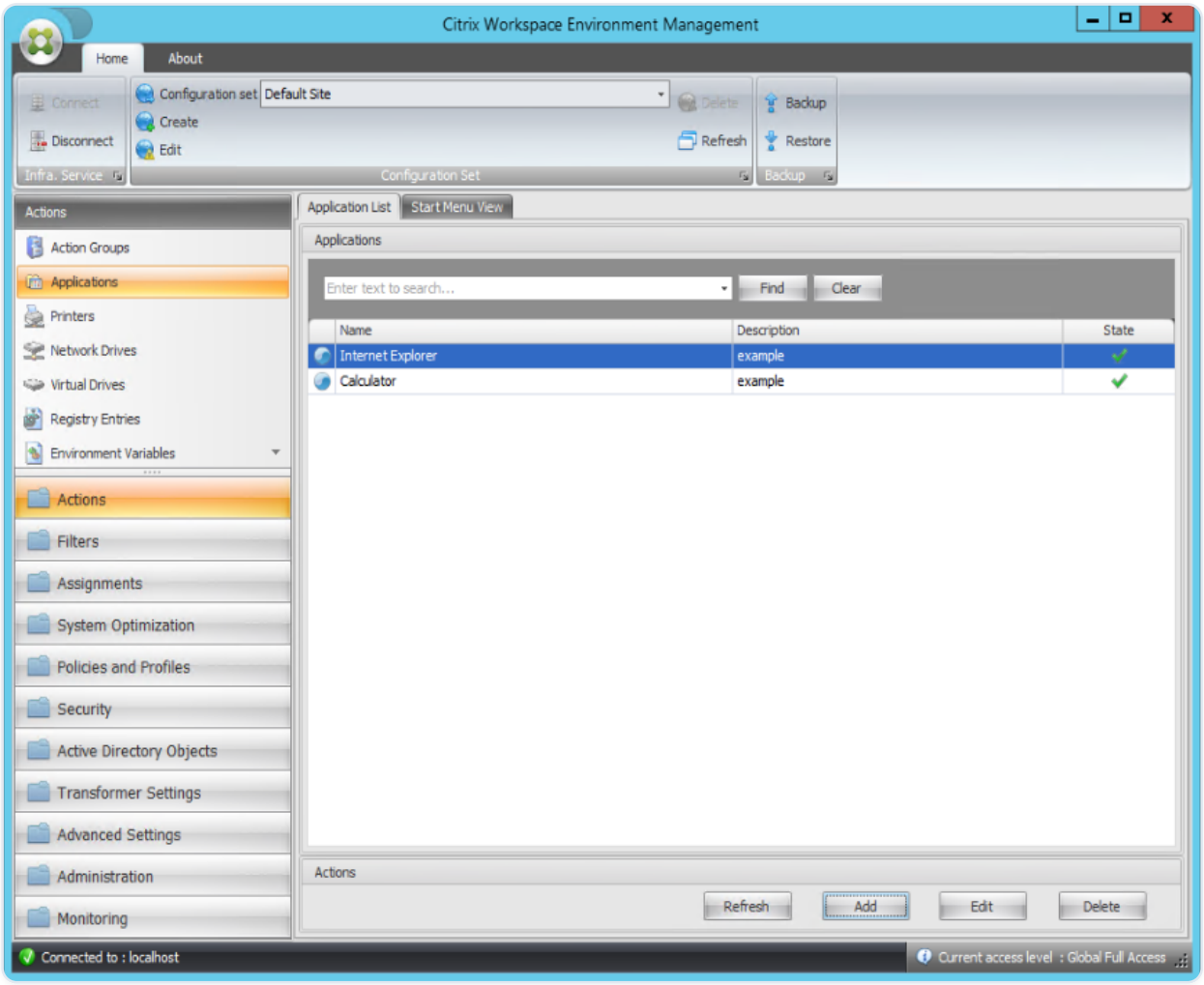
© 1997–2026 Citrix Systems, Inc. All rights reserved.

were processed earlier, resulting in the actions processed later being unassigned. The other actions remain unchanged.

Example scenario

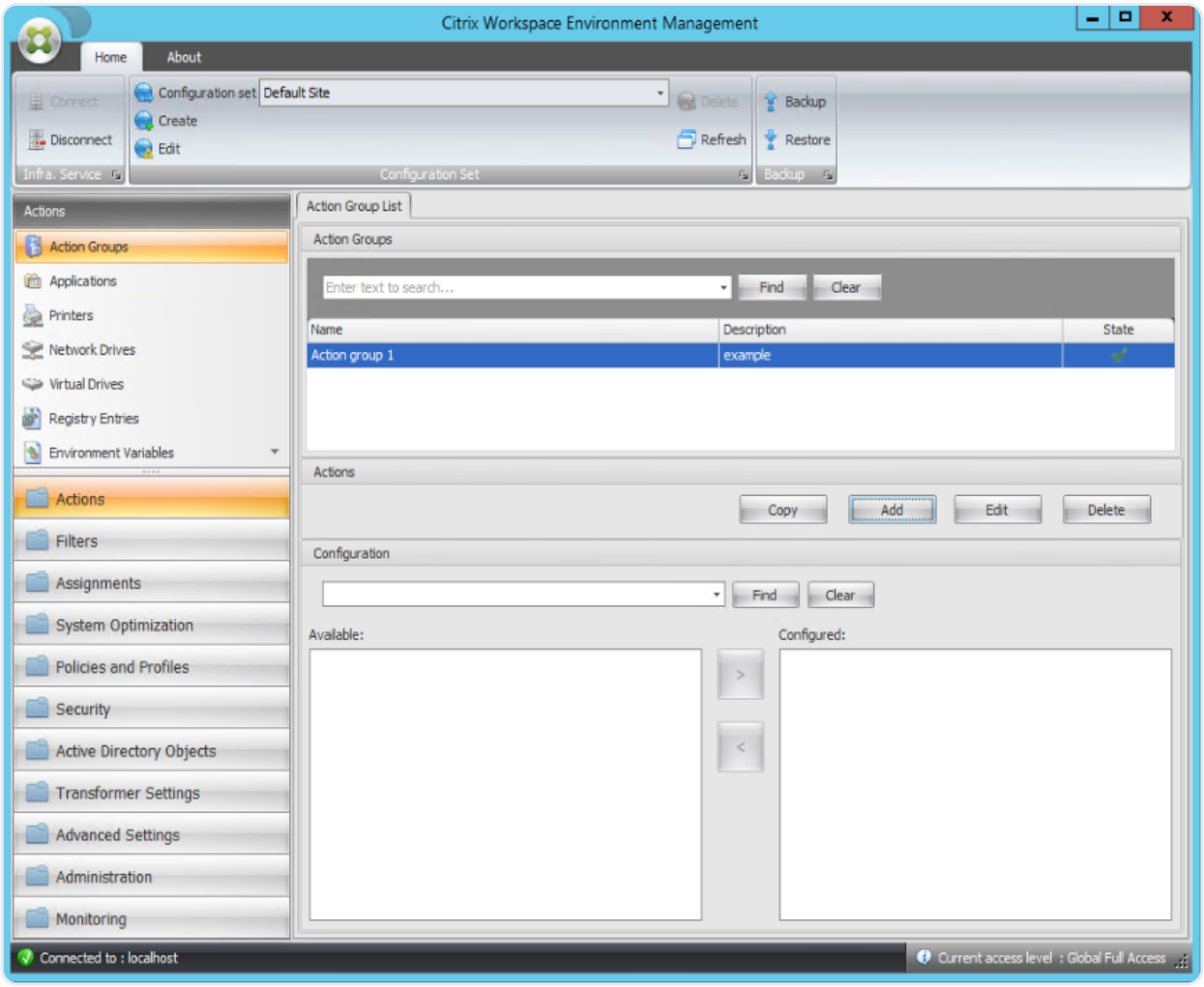
For example, to use the action groups feature to assign two applications (iexplore.exe and calc.exe) to a user at one time, follow the steps below.

1. Go to the **Administration Console > Actions > Applications > Application List** tab and then add the applications (iexplore.exe and calc.exe).



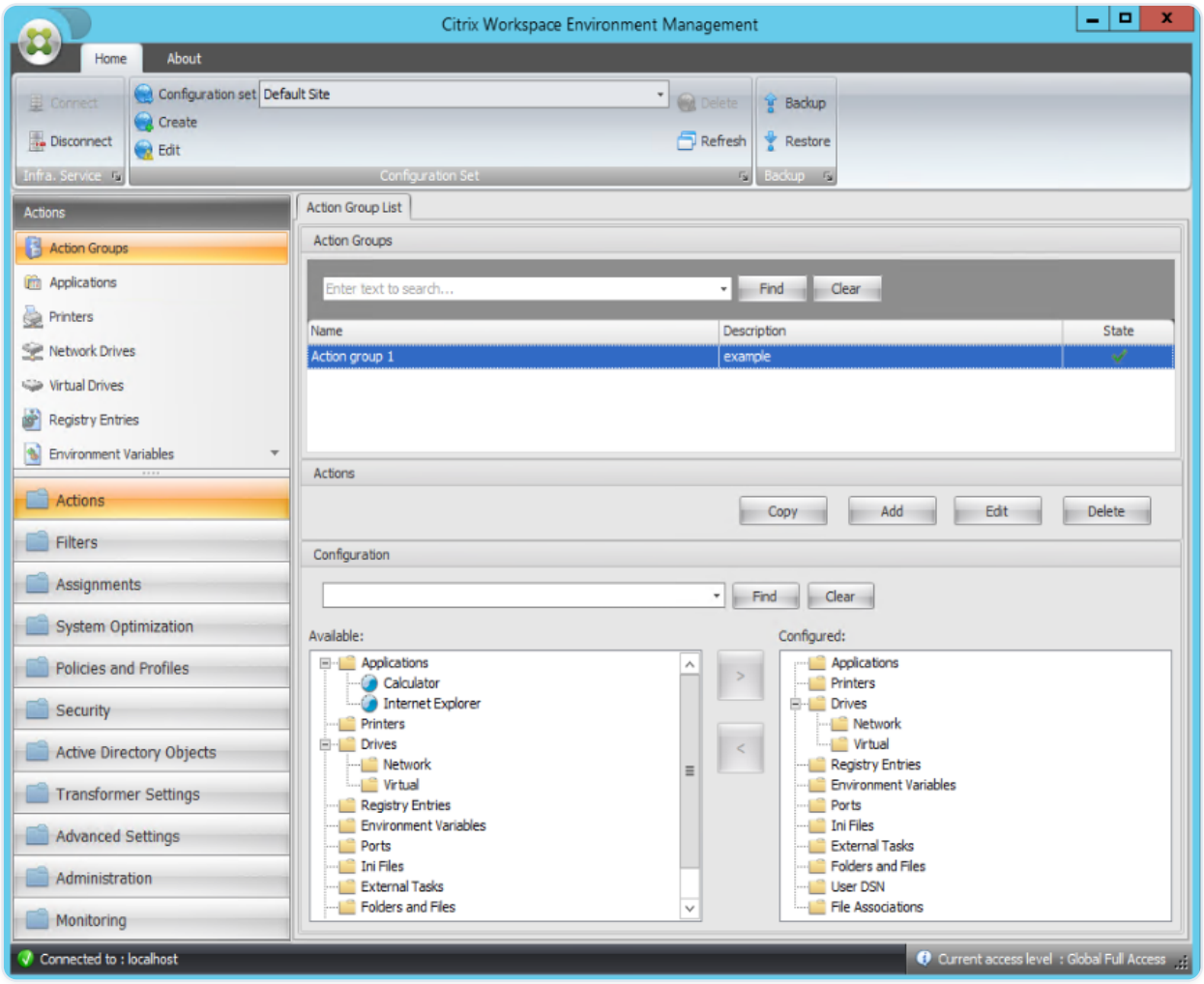
2. Go to the **Administration Console > Actions > Action Groups > Action Group List** tab and then click **Add** to create an action group.

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



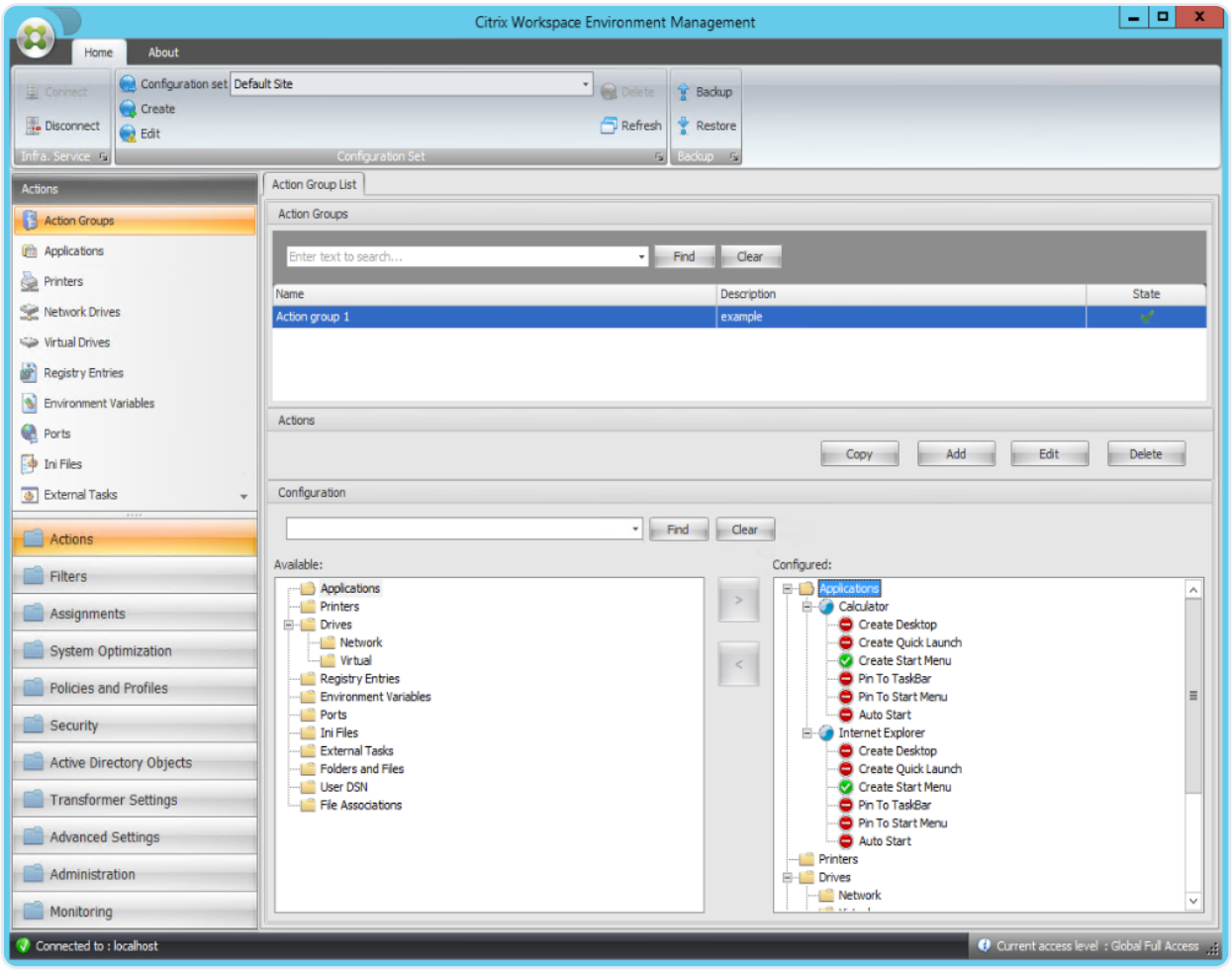
3. On the **Action Group List** tab, double-click the action group you created to display the action list in the **Available** and **Configured** panes.

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



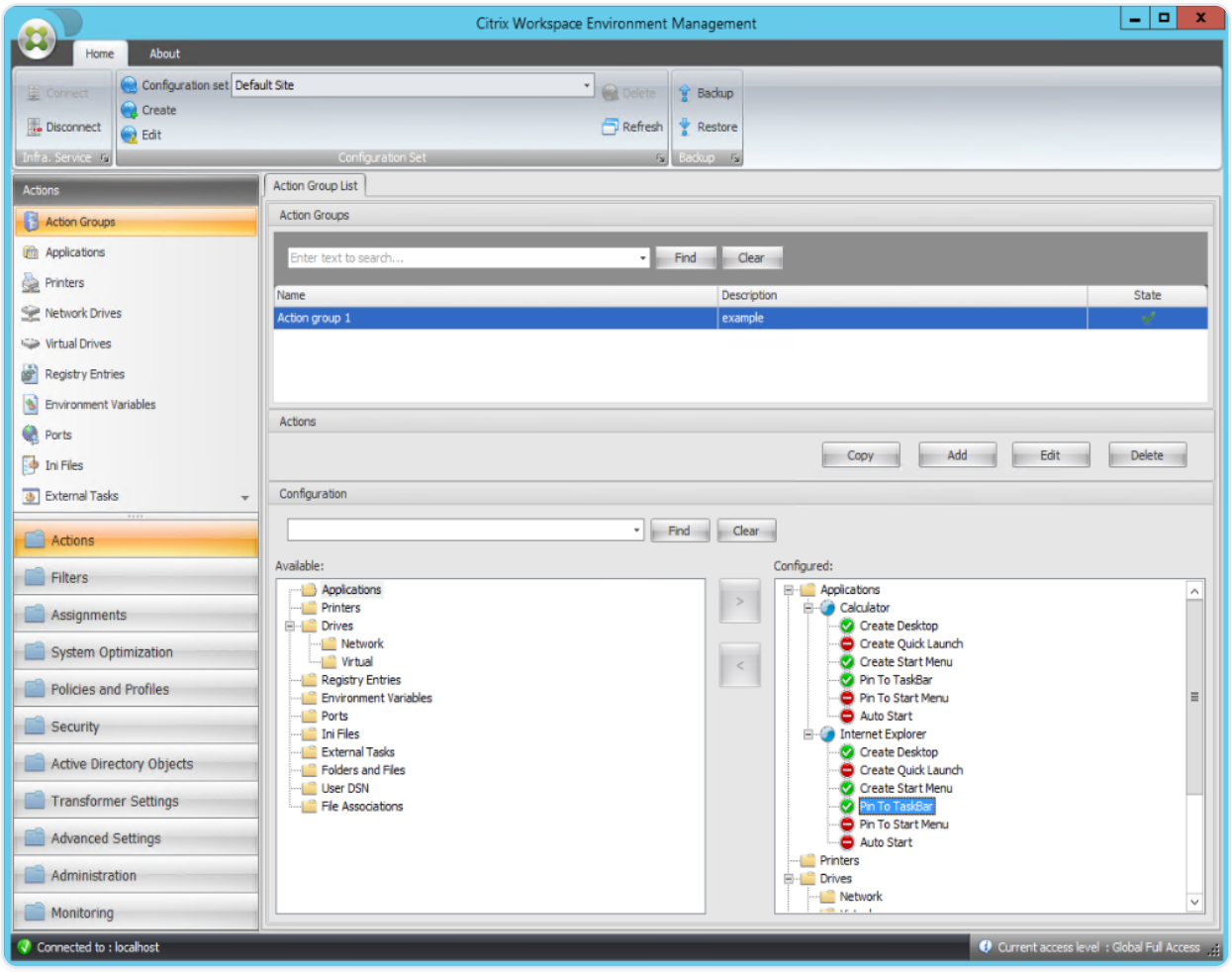
4. In the **Available** pane, double-click each application to move it to the **Configured** pane. You can also do so by selecting the application and then clicking the right arrow.

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



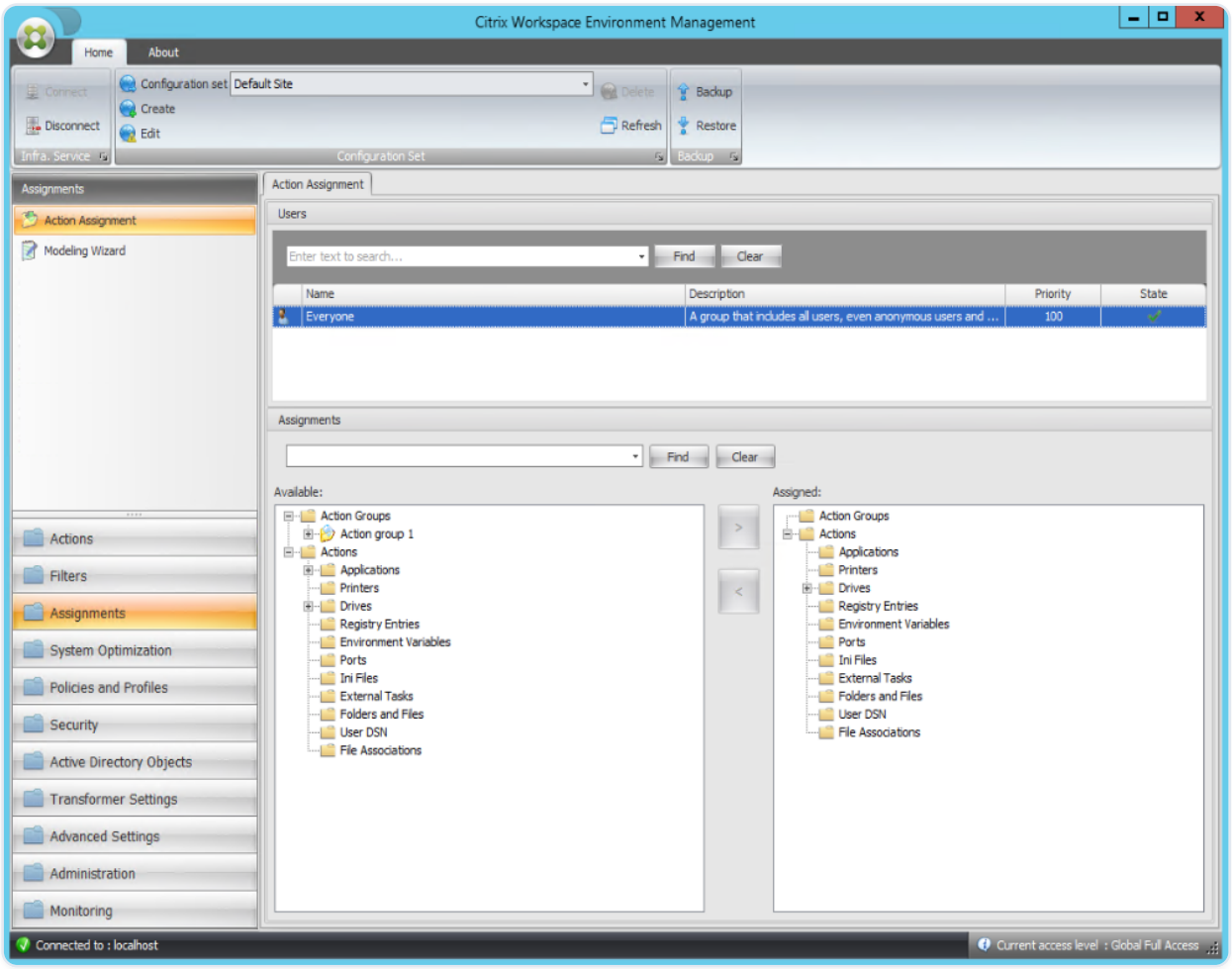
5. In the **Configured** pane, configure the options for each application. In this example, enable **Create Desktop** and **Pin To TaskBar**.

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



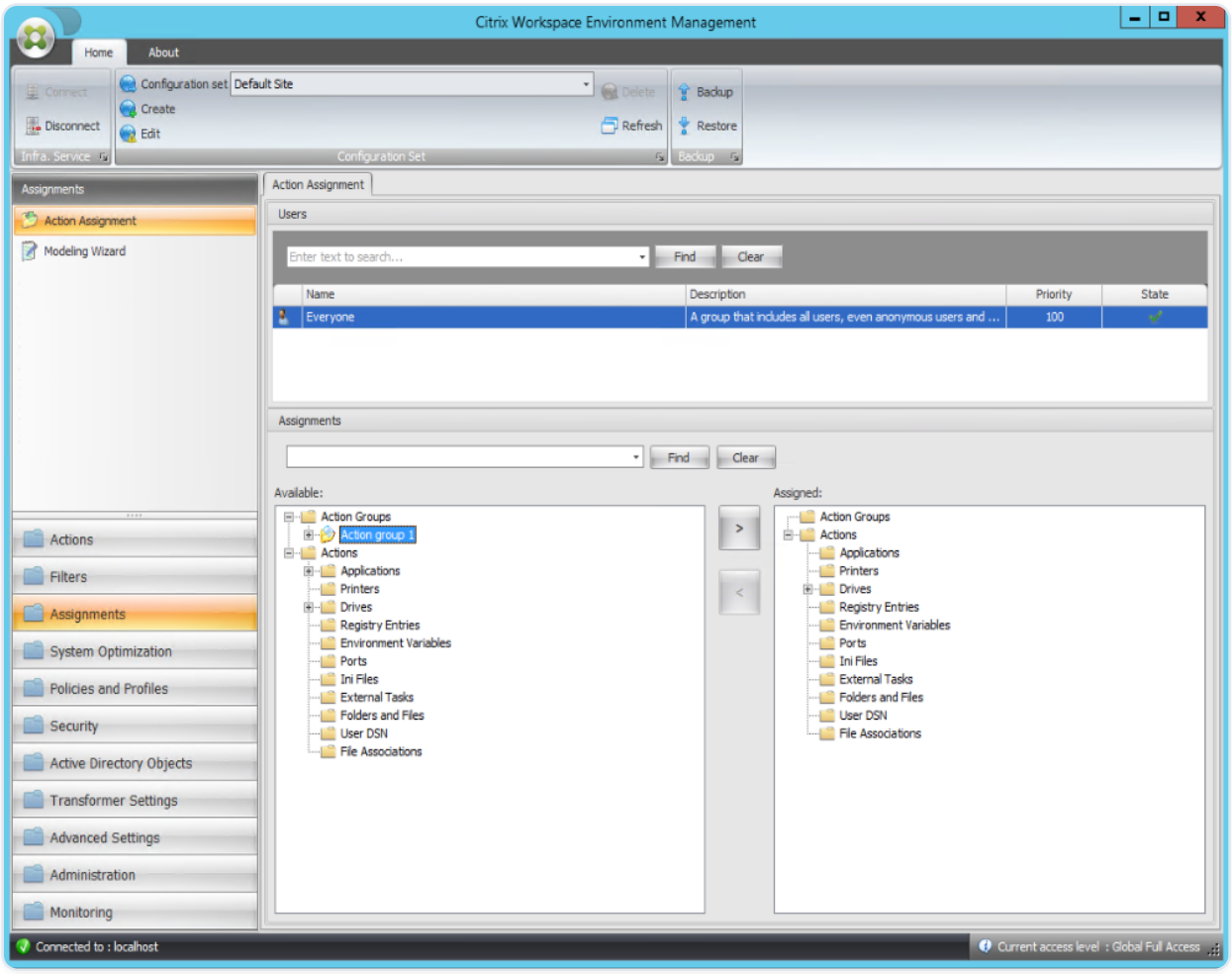
6. Go to the **Administration Console \> Assignments \> Action Assignment** tab and then double-click the applicable user to display the action group in the **Available** and **Assigned** panes.

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



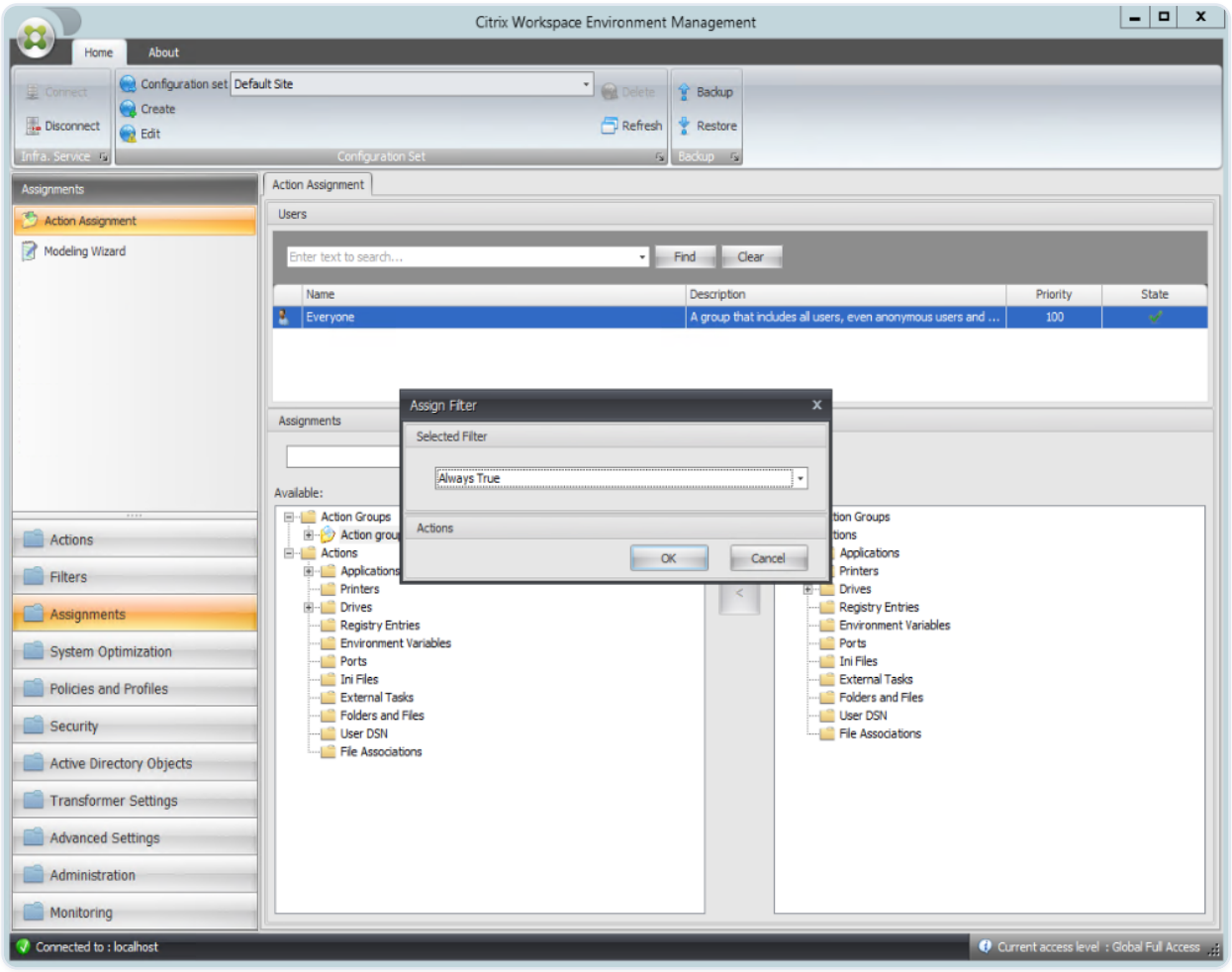
7. In the **Available** pane, double-click the action group you created (in this example, Action group 1) to move it to the **Assigned** pane. You can also do so by selecting the action group and then clicking the right arrow.

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



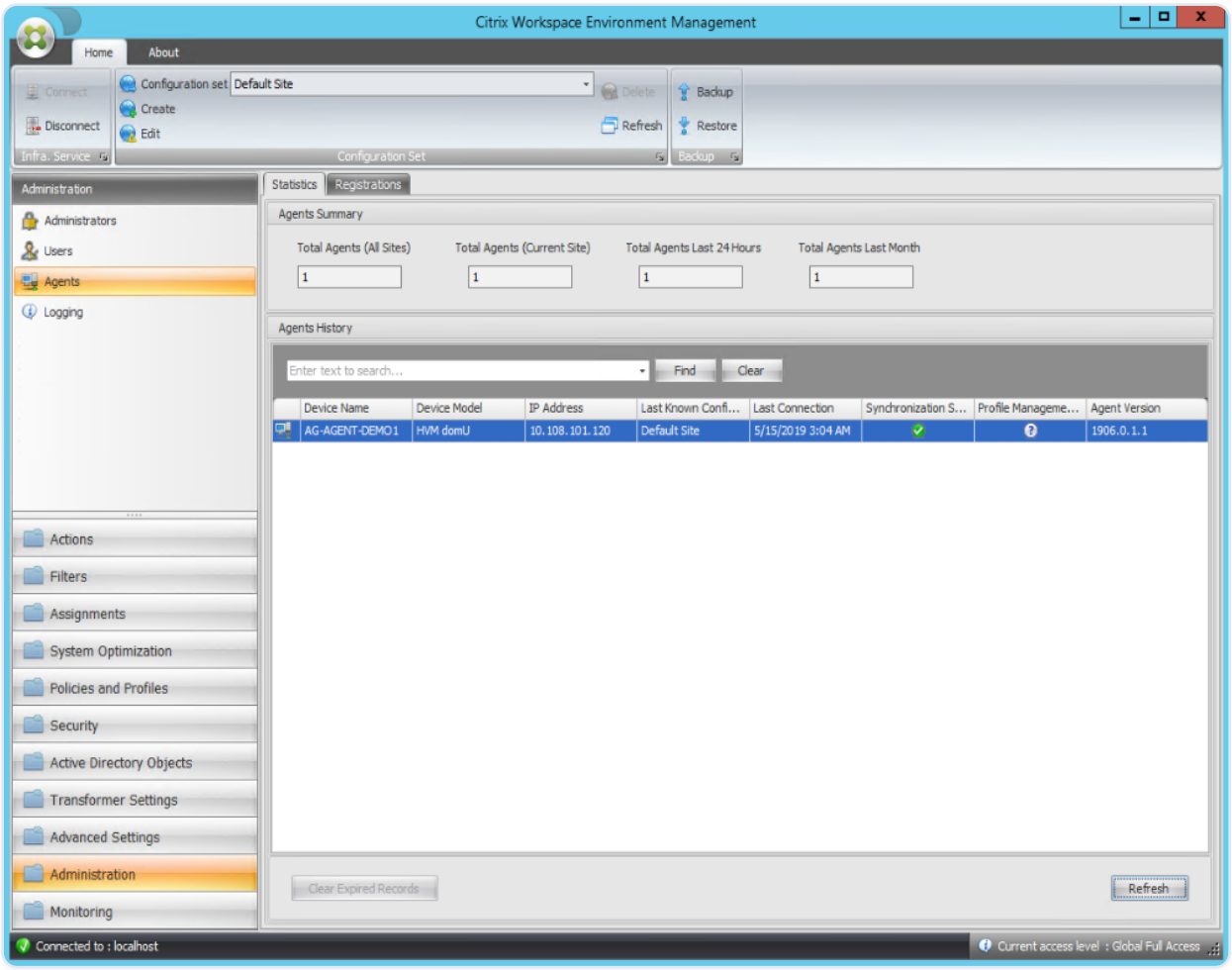
8. In the **Assign Filter** window, select **Always True** and then click **OK**.

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



9. Go to the **Administration Console > Administration > Agents > Statistics** tab and then click **Refresh**.

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



10. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.
11. On the machine where the agent is running (agent host), verify that the configured actions are taking effect.

In this example, the two applications are successfully assigned to the agent host, and their shortcuts are added to the desktop and pinned to the taskbar.

Group Policy Settings

IMPORTANT:

WEM currently supports adding and editing only Group Policy settings associated with the `HKEY_LOCAL_MACHINE` and the `HKEY_CURRENT_USER` registry hives.

In previous releases, you could migrate only Group Policy Preferences (GPP) into Workspace Environment Management (WEM). For more information, see the description of the **Migrate** wizard in Ribbon. You can now also import Group Policy settings (registry-based settings) into WEM.

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

After importing the settings, you can have an itemized view of the settings associated with each GPO before you decide which GPO to assign. You can assign the GPO to different AD groups, just like you assign other actions. If you assign GPOs to an individual user directly, the settings do not take effect. A group can contain users and machines. Machine-level settings take effect if the related machine belongs to the group. User-level settings take effect if the current user belongs to the group.

TIP:

For machine-level settings to take effect immediately, restart the Citrix WEM Agent Host Service. For user-level settings to take effect immediately, users must log off and log back on.

Group Policy settings

NOTE:

For WEM agents to process Group Policy settings properly, verify that Citrix WEM User Logon Service is enabled on them.

Enable Group Policy Settings Processing. Controls whether to enable WEM to process Group Policy settings. By default, this option is disabled. When disabled:

- You cannot configure Group Policy settings.
- WEM does not process Group Policy settings even if they are already assigned to users or user groups.

Group Policy object list

Displays a list of your existing GPOs. Use **Find** to filter the list by name or description.

- **Refresh**. Refreshes the GPO list.
- **Import**. Opens the **Import Group Policy Settings** wizard, which lets you import Group Policy settings into WEM.
- **Edit**. Lets you edit an existing GPO.
- **Delete**. Deletes the GPO you select.

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

Import Group Policy settings

Before importing Group Policy settings, back up your Group Policy settings on your domain controller:

1. Open the Group Policy Management Console.
2. In the **Group Policy Management** window, right-click the GPO you want to back up and then select **Back Up**.
3. In the **Back Up Group Policy Object** window, specify the location where you want to save the backup. Optionally, you can give the backup a description.
4. Click **Back Up** to start the backup and then click **OK**.
5. Navigate to the backup folder and then compress it into a zip file.

> **NOTE:**
>
> WEM also supports importing zip files that contain multiple GPO backup folders.

To import your Group Policy settings, complete the following steps:

1. Use **Upload**, available in the menu on the WEM service **Manage** tab, to upload the zip file of your GPOs to the default folder in Citrix Cloud.
2. Navigate to the **Administration Console > Actions > Group Policy Settings** tab, select **Enable Group Policy Settings Processing**, and then click **Import** to open the import wizard.
3. On the **File to Import** page of the import wizard, click **Browse** and then select the applicable file from the list. You can also type the name of the file and then click **Find** to locate it.
    - **Overwrites GPOs you imported previously**. Controls whether to overwrite existing GPOs.
4. Click **Start Import** to start the import process.
5. After the import completes, click **Finish**. Imported GPOs appear on the **Group Policy Settings** tab.

Import Group Policy settings from registry files

You can convert registry values that you export using the Windows Registry Editor into GPOs for management and assignment. If you are familiar with the Import registry files option available with Registry Entries, this feature:

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

- Lets you import registry values under both `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`.
- Lets you import registry values of the `REG_BINARY` and `REG_MULTI_SZ` types.
- Supports converting delete operations associated with registry keys and values that you define in .reg files. For information about deleting registry keys and values by using a .reg file, see `<https://support.microsoft.com/en-us/topic/how-to-add-modify-or-delete-registry-subkeys-and-values-by-using-a-reg-file-9c7f37cf-a5e9-e1cd-c4fa-2a26218a1a23>`.

Before you start, be aware of the following:

- When importing settings from a zip file, the file can contain one or more registry files. Make sure that the size of the unzipped file is not greater than 30 M.
- Each .reg file will be converted into a GPO. You can treat each converted GPO as a set of registry settings.
- The name of each converted GPO is generated based on the name of the corresponding .reg file. Example: If the name of the .reg file is `test1.reg`, the name of the converted GPO is `test1`.
- Descriptions of converted GPOs are empty. Their state defaults to enabled (check mark icon).

To import your Group Policy settings, complete the following steps:

1. In the administration console, go to **Actions > Group Policy Settings**, select **Enable Group Policy Settings Processing**, click the down arrow next to **Import**, and select **Import Registry File**.
2. In the wizard that appears, browse to the zip backup of your registry files.
    - **Overwrite existing GPOs**. Controls whether to overwrite existing GPOs when conflicts occur.
3. Click **Start Import**.
4. After the import completes, click **Finish**. GPOs converted from the registry files appear in **Group Policy Settings**.

Edit Group Policy settings

Double-click a GPO from the list for an itemized view of its settings and to edit the settings if needed.

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

To clone a GPO, right-click the GPO and select **Copy** from the menu. The clone is automatically created after you click **Copy**. The clone inherits the name of the original and has a suffix "-Copy." You can use **Edit** to change the name.

The **Edit Group Policy Object** window appears after you click **Edit**.

Name. The name of the GPO as it appears in the GPO list.

Description. Lets you specify additional information about the GPO, which appears in the GPO list.

Registry Operations. Displays registry operations that the GPO contains.

WARNING:

Editing, adding, and deleting registry-based settings incorrectly can prevent the settings from taking effect in the user environment.

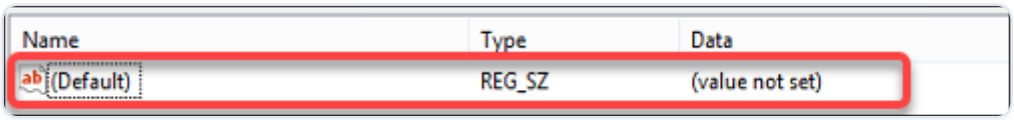
- **Add**. Lets you add a registry key.
- **Edit.** Lets you edit a registry key.
- **Delete.** Lets you delete a registry key.

To add a registry key, click **Add** on the right-hand side. The following settings become available:

- **Order**. Lets you specify the order of deployment for the registry key.
- **Action**. Lets you specify the type of action for the registry key.
  - **Set value**. Lets you set a value for the registry key.
  - **Delete value**. Lets you delete a value for the registry key.
  - **Create key**. Lets you create the key as specified by the combination of the root key and the subpath.
  - **Delete key**. Lets you delete a key under the registry key.
  - **Delete all values**. Lets you delete all values under the registry key.
- **Root Key**. Supported values: `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`.
- **Subpath**. The full path of the registry key without the root key. For example, if `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows` is the full path of the registry key, `Software\Microsoft\Windows` is the subpath.

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

- **Value**. Lets you specify a name for the registry value. The highlighted item in the following diagram as a whole is a registry value.



- **Type**. Lets you specify the data type for the value.
  - **REG_SZ**. This type is a standard string used to represent human readable text values.
  - **REG_EXPAND_SZ**. This type is an expandable data string that contains a variable to be replaced when called by an application. For example, for the following value, the string "%SystemRoot%" will be replaced by the actual location of the folder in an operating system.
  - **REG_BINARY**. Binary data in any form.
  - **REG_DWORD**. A 32-bit number. This type is commonly used for Boolean values. For example, "0" means disabled and "1" means enabled.
  - **REG_DWORD_LITTLE_ENDIAN**. A 32-bit number in little-endian format.
  - **REG_QWORD**. A 64-bit number.
  - **REG_QWORD_LITTLE_ENDIAN**. A 64-bit number in little-endian format.
  - **REG_MULTI_SZ**. This type is a multi-string used to represent values that contain lists or multiple values. Each entry is separated by a null character.
- **Data**. Lets you type data corresponding to the registry value. For different data types, you might need to type different data in different formats.

Your changes might take some time to take effect. Keep the following in mind:

- Changes associated with the `HKEY_LOCAL_MACHINE` registry hive take effect when **Citrix WEM Agent Host Service** starts or the specified **SQL Settings Refresh Delay** times out.
- Changes associated with the `HKEY_CURRENT_USER` registry hive take effect when users log on.

Contextualize Group Policy settings

You can make Group Policy settings conditional by using a filter to contextualize their assignments. A filter comprises a rule and multiple conditions. The WEM agent applies the assigned Group Policy settings only when all conditions in the rule are met in the user environment at runtime. Otherwise, the agent skips those settings when enforcing filters.

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

A general workflow to make Group Policy settings conditional is as follows:

1. In the administration console, navigate to **Filters > Conditions** and define your conditions. See Conditions.

   IMPORTANT:

   For a complete list of filter conditions available, see Filter conditions. Group Policy settings comprise user and machine settings. Some filter conditions apply only to user settings. If you apply those filter conditions to machine settings, the WEM agent ignores the filter conditions and applies the machine settings. For a complete list of filter conditions that do not apply to machine settings, see Filter conditions not applicable to machine settings.

2. Navigate to **Filters > Rules** and define your filter rule. You can include the conditions you defined in Step 1 into that rule. See Rules.
3. Navigate to **Actions > Group Policy Settings** and configure your Group Policy settings.
4. Navigate to **Administration Console > Assignments > Action Assignment** and complete the following:

   a. Double-click the user or user group to which you want to assign the settings.

   b. Select the application and click the right arrow (\>) to assign them.

   c. In the **Assign Filter** window, select the rule you defined in Step 2 and then click **OK**. The settings move from the **Available** pane to the **Assigned** pane.

   d. In the **Assigned** pane, configure priority for the settings. Type an integer to specify a priority. The greater the value, the higher the priority. Settings with higher priority are processed later, ensuring that they are in effect when there is a conflict or dependency.

Filter conditions not applicable to machine settings

FILTER NAME	APPLICABLE TO MACHINE SETTINGS
ClientName Match	No
Client IP Address Match	No
Registry Value Match	If you configure a registry value starting with HKCU, the **Registry Value Match** filter does not work if applied to machine settings.

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

FILTER NAME	APPLICABLE TO MACHINE SETTINGS
User Country Match	No
User UI Language Match	No
User SBC Resource Type	No
Active Directory Path Match	No
Active Directory Attribute Match	No
No ClientName Match	No
No Client IP Address Match	No
No Registry Value Match	No
No User Country Match	No
No User UI Language Match	No
No Active Directory Path Match	No
No Active Directory Attribute Match	No
Client Remote OS Match	No
No Client Remote OS Match	No
Active Directory Group Match	No
No Active Directory Group Match	No
Published Resource Name	No

Template-based settings

Use this tab to configure settings for Windows by using Group Policy Administrative Templates. You can configure GPOs at a machine and user level.

In **Actions > Group Policy Settings > Template-based** under a configuration set, you can perform the following operations:

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

- Create a GPO with a template.
- Manage templates.
- Import templates.
- Refresh the GPO list.
- Edit a GPO.
- Manage assignments for a GPO.
- Clone a GPO.
- Delete a GPO.

Create a GPO with a template

To create a GPO with a template, complete the following steps:

1. In the action bar, click **Create GPO**.
2. In **Basic information**:
    - Specify a name for the GPO.
    - Optionally, specify additional information to help you identify the GPO.
3. In **Computer configuration**, configure policies that you want to apply to machines (regardless of who logs on to them).
4. In **User configuration**, configure policies that you want to apply to users (regardless of which machine they log on to).
5. In **Summary**, review the changes you made.
6. After you finish, click **Done**.

In **Computer configuration** and **User configuration**, select a setting to configure it. You can show policies in tree view and list view. In list view, policies are sorted alphabetically, and you can search for desired policies.

To configure a setting, you first enable it. A setting might have multiple items that can be configured. Depending on the type of input needed, the setting can be a check box, input box (text or number as input), selection, list, or a combination.

For information about the settings, download a GPO reference sheet from Microsoft.

Manage templates

To manage templates, complete the following steps:

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

1. In the action bar, click **Manage template**.
2. In the **Manage template** wizard:

- Select **Computer configuration** to configure policies that you want to apply to machines (regardless of who logs on to them).
- Select **User configuration** to configure policies that you want to apply to users (regardless of which machine they log on to).

1. After you finish, click **Done**.

In **Computer configuration** and **User configuration**, select a setting to configure it. You can show policies in tree view and list view. In list view, policies are sorted alphabetically, and you can search for desired policies.

To configure a setting, you first enable it. A setting might have multiple items that can be configured. Depending on the type of input needed, the setting can be a check box, input box (text or number as input), selection, list, or a combination.

For information about the settings, download a GPO reference sheet from Microsoft.

Import templates

IMPORTANT:

When importing ADMX files to WEM for use as templates, ensure that all .adml files in the zip file are of the same language.

You can import ADMX files to WEM for use as templates. You then create GPOs with those templates. To import templates, complete the following steps:

1. In the action bar, click **Manage template**.
2. In the **Manage template** wizard, click **Import**.
3. Browse to the zip file that contains your ADMX files and decide what to do if the file contains a template with the same name as an existing template:

   - **Do not import**. Cancels the import.
   - **Skip the template and import the rest**.

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

- **Overwrite the existing template**. Overwriting might change associated settings originating from existing templates. Existing GPOs created with the templates are not affected. However, when you edit those GPOs, associated settings are lost.

4. Click **Start import** to start the import process.
5. After you finish, click **Done** to return to the **Manage template** wizard.
6. Manage templates there or click **Done** to exit.

For information on how to manage your imported template files, see Files. When managing them there, consider the following:

- Deleting GPO administrative template files will remove the associated settings from your current template. Existing GPOs created with the templates are not affected. However, when you edit those GPOs, associated settings are lost.

Edit a GPO

To edit a GPO, complete the following steps:

1. Select the GPO and then click **Edit** in the action bar.
2. In **Basic information**, edit the name and description.
3. In **Computer configuration**, edit machine policies.
4. In **User configuration**, edit user policies.
5. In **Summary**, review the changes you made.
6. After you finish, click **Save**.

NOTE:

If a GPO is already assigned to users, editing it will impact those users.

Manage assignments for a GPO

You can manage assignments for GPOs created using templates, just like you do for registry-based GPOs. For more information, see Manage assignments for a GPO.

Clone a GPO

To clone a GPO, complete the following steps:

1. Select the GPO and then click **Clone** in the action bar.
2. Decide whether to clone the GPO as a registry-based GPO or a template-based GPO.

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

NOTE:

When cloned as registry-based, the GPO is converted to registry values and appears on the **Registry-based** tab. You can treat each converted GPO as a set of registry settings.

3. Edit the name and description.
4. Select the configuration set you want to clone the GPO to.
5. Click **Clone** to start the clone process.

Delete a GPO

To delete a GPO, select it and then click **Delete** in the action bar.

NOTE:

If a GPO is already assigned to users, deleting it will impact those users.

Scripted Task Settings

Lists all scripted tasks available on the **Scripted Tasks** page. Scripted tasks run at a configuration set level. Here, you configure which scripted tasks to enable for the current configuration set. To edit your scripted tasks, go to Scripted Tasks.

Configure a scripted task

1. On the **Scripted Task Settings** page, locate the scripted task, select the ellipsis, and then select **Configure**.
2. In the **Configure scripted task** wizard, configure the following settings and then click **Save**.

In **General**:

- **Enable this task**. Choose whether to enable (**Yes**) or disable (**No**) the task for the current configuration set. If disabled, the agent does not process the task.
- **Verify signature**. Choose whether to verify the signature before running the task. Signature verification is mandatory when the scripted task is granted full access.
- **Task timeout**. Choose whether to set a timeout (in minutes) for the task. When the timeout occurs, the task is forced to end. Supported values: 1–60. We recommend setting a timeout for the task. Otherwise, the task might be left running, preventing other tasks from running.

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

- **Filter**. Choose whether to contextualize the task by selecting a filter. With a filter selected, this task runs only when all conditions in the filter are met. When selecting a filter, consider the following:
  - If the filter contains conditions that do not apply to scripted tasks, the agent skips those conditions when evaluating the filter before running the task. For a complete list of conditions that do not apply to scripted tasks, see Conditions not applicable to machine settings.

In **Triggers**:

- Configure triggers for the task. You can do the following:
  - Select triggers that you want to associate with the task. When activated, those triggers start the task in the user environment.
  - Choose whether to show only triggers that apply to this task.
  - Create a new trigger. See Create a trigger.

> **NOTE:**
>
> To edit existing triggers, go to Triggers.

In **Parameters**:

- **Pass parameters to the scripted task**. Choose whether to pass parameters to the scripted task. When enabled, lets you provide inputs as parameter variables in the scripted task at runtime. The benefit is that you can control how the scripted task behaves without changing the underlying code. The following parameter types are available:
  - **Integer**. Example: `123`.
  - **String**. Example: `hello world`.
  - **Boolean**. True or False.
  - **Character**. Example: `c`.
  - **Switch**. True or False.
  - **Double**. Example: `1.023`.
  - **Date and time**. Example: `YYYY-MM-DD HH:mm:ss`.

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

- **File path**. Enter a path that you want to pass to the `System.IO.FileInfo` class. Environment variables are supported. The path must not include the following characters: `* ? < >`.

> **NOTE:**
>
> - You can configure up to 20 parameters.
> - The name field is optional except for parameters of the "switch" type.
> - PowerShell supports partial parameter names. When using a partial parameter name, make sure that the name is unique — disambiguate it from existing parameter names. Example: The following parameter names are the same for PowerShell: `-t`, `-ti`, and `-title`. In this case, supply enough letters of the parameter name to distinguish it from the other parameters.

In **Output**:

- **Output files.** Choose whether you want to collect files that the task outputs. If selected, includes output file content in reports generated for the task. You can then view the output file content in the reports without the need to access the output files in the user environment.
- **Output highlights**. Choose whether you want to highlight certain content in the output file content and the console output.
  - **Highlight keywords.** Specify keywords that you want the report to highlight. You can type multiple keywords, separated by commas. After typing a keyword, press **Enter** to continue. If specified, report contents that match your keywords will be highlighted in the **Output file content** and **Console output** sections in the generated reports.
  - **Highlight regular expression matches**. Enter a regular expression that describes the content you want to highlight. The regular expression must conform to the .NET regular expression library syntax, which is PCRE compatible. For more information, see the Microsoft documentation: `<https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference>`.
    - **Regular expression.** Enter a regular expression that describes the content you want to highlight.
    - **Ignore case**. Choose whether content must exactly match the case.

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

    - **Use multiline matching**. Choose whether to use multiline matching, where \^ and \$ match the beginning and end of each line, instead of the beginning and end of the entire output content.
    - **Capture only named groups**. Choose whether to capture only named groups. Captured groups are defined by using parentheses in the regular expression pattern. Named groups are explicitly assigned a name or a number by the `(?<name> subexpression)` syntax.
    - **Number of lines to include as context clues**. Specify the number of lines before and after the match you want to include in the highlight as context clues. Supported values: 1–10.
    - **Include only regular expression matches in reports**. Controls whether to include the entire output content in reports or only content that matches the regular expression. Enabling this option reduces the amount of data transmitted to Citrix Cloud. With the option enabled, the Highlight keywords feature has no content to show regardless of the specified keywords.

- **Advanced options**.

    - **Collect output even if runtime errors occur**. Controls whether to collect output file content and console output even if errors occur while running the task.

View reports for a scripted task

On the **Scripted Task Settings** page, locate the scripted task, select the ellipsis, and then select **View reports**. As a result, you are taken to the **Monitoring > Reports** page, where you see the reports (if any) related to the task. Click the ellipsis to view more detailed information. For details, see Reports.

Applications

Controls the creation of application shortcuts.

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

TIP:

- You can use Citrix Studio to edit the application settings and then add an executable file path that points to **VUEMAppCmd.exe**. **VUEMAppCmd.exe** ensures that the Workspace Environment Management agent finishes processing an environment before Citrix Virtual Apps and Desktops published applications are started. For more information, see Editing application settings using Citrix Studio.
- You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Application list

A list of your existing application resources. You can use **Find** to filter the list by name or ID against a text string.

To add an application

1. Use the context menu **Add** command.
2. Enter details in the **New Application** dialog tabs, then click **OK**.

Fields and controls

General

- **Name**. The display name of the application shortcut, as it appears in the application list.
- **Description**. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.
- **Application Type**. The type of application the shortcut starts, which can be one of **Installed application**, **File/Folder**, **URL**, or **StoreFront store**. The following values are required depending on the selection:
  - **Command Line**. The path to the application executable as the client machine sees it. The **Browse** button allows you to browse to a locally installed executable.
  - **Working Directory**. The shortcut working directory. Automatically filled out if you browse to the executable.
  - **Parameters**. Any launch parameters for the application.
  - **Target**. (File/Folder) The name of the target file or folder the application opens.
  - **Shortcut URL**. (URL) The URL of the application shortcut you are adding.

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

  - **Store URL**. (StoreFront™ store) The URL of the StoreFront store containing the resource you want to start from the shortcut.
  - **Store Resource**. (StoreFront store) The resource on the StoreFront store that you want to start from the shortcut. The **Browse** button allows you to browse and select the resource.

    TIP:

    To add an application that is based on a StoreFront store, you must provide valid credentials. A dialog appears the first time you click **Browse** to view store resources. The dialog prompts you to type credentials that you use to log on to Citrix Workspace™ app for Windows. After that, the Store Resources window appears, displaying a list of published applications retrieved by Citrix Workspace app for Windows running on the WEM administration console machine.

- **Start Menu Integration**. Select where the application shortcut is created in the Start menu. By default, a new shortcut is created in Programs.

Options

- **Select Icon**. Allows you to browse to an icon file and select an icon for your application. By default, this setting uses the application executable's icon but you can select any valid icon. Icons are stored in the database as text.
  - **High Resolution Icons Only**. Displays only HD icons in the selection box.
- **Application State**. Controls whether the application shortcut is enabled. When disabled, the agent does not process it even if it is assigned to a user.
- **Maintenance Mode**. When active, this setting prevents the user from running the application shortcut. The shortcut icon is modified to include a warning sign to denote that the icon is not available, and the user receives a short message informing them the application is unavailable if they try to launch it. This allows you to proactively manage scenarios where published applications are in maintenance without having to disable or delete application shortcut resources.
- **Display Name**. The name of the shortcut as it appears in the user's environment.
- **Hotkey**. Allows you to specify a hotkey for the user to launch the application with. Hotkeys are case sensitive and are entered in the following format (for example): Ctrl + Alt + S.
- **Action Type**. Describes what type of action this resource is.

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

Advanced Settings

- **Enable Automatic Self-Healing**. When selected, the agent automatically recreates application shortcuts on refresh if the user has moved or deleted them.
- **Enforce Icon Location**. Allows you to specify the exact location of the application shortcut on the user's desktop. Values are in pixels.
- **Windows Style**. Controls whether the application opens in a minimized, normal, or maximized window on endpoints.
- **Do Not Show in Self Services**. Hides the application from the self-service interface accessible from a status bar icon available to end-users when the session agent is running in UI mode. This includes hiding it in the context menu "My Applications" icon list, and in the Manage Applications form.
- **Create Shortcut in User Favorites Folder**. Creates an application shortcut in the end-user Favorites folder.

To add an Application entry that is based on a StoreFront store, you must provide valid credentials, so that a list of published applications can be retrieved by Citrix Workspace app for Windows installed on the WEM administration console machine.

Start menu view

Displays a tree view of your application shortcut resource locations in the Start Menu.

Refresh. Refreshes the application list.

Move. Opens up a wizard which allows you to select a location to move the application shortcut to.

Edit. Opens up the application edition wizard.

Delete. Deletes the selected application shortcut resource.

Editing application settings using Citrix Studio

Workspace Environment Management (WEM) provides you with client-side tools to troubleshoot issues you experience. The VUEMAppCMD tool (**VUEMAppCmd.exe**) ensures that the WEM agent finishes processing an environment before Citrix Virtual Apps and Desktops published applications are started. It is located in the agent installation folder: `%ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMAppCmd.exe`.

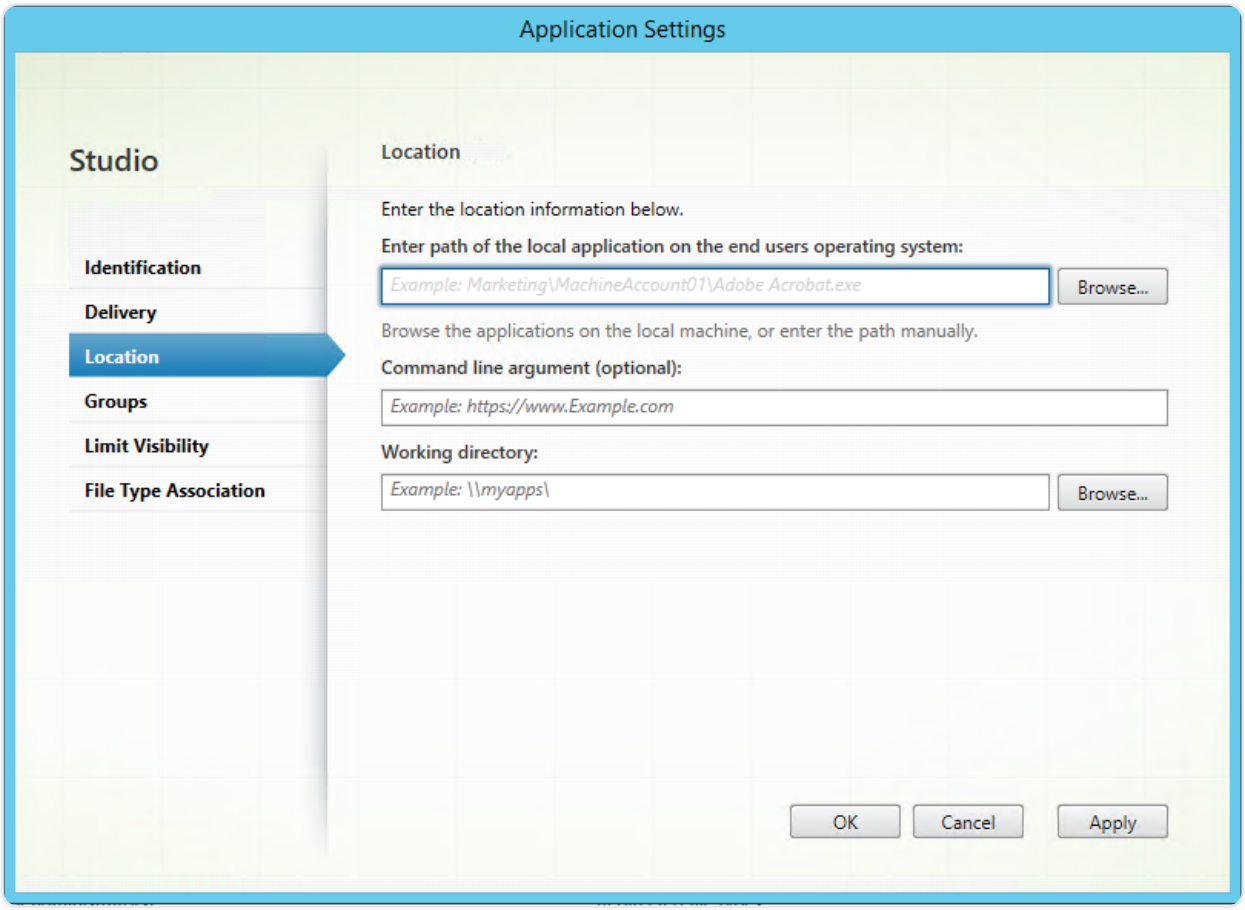
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

For the 64-bit OS, use `%ProgramFiles(x86)%` instead.

You can use Citrix Studio to edit the application settings and then add an executable file path that points to **VUEMAppCmd.exe**. To do so, complete the following steps:

1. Navigate to the **Application Settings > Location** page of Citrix Studio.



2. Type the path of the local application on the end-user operating system.
   - Type the following: `%ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMAppCmd.exe`.
3. Type the command-line argument to specify an application to open.
   - Type the full path to the application that you want to launch through **VUEMAppCmd.exe**. Make sure that you wrap the command line for the application in double quotes if the path contains blank spaces.

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

- For example, suppose you want to launch **iexplore.exe** through **VUEMAppCmd.exe**. You can do so by typing the following: `"%ProgramFiles%\Internet Explorer\iexplore.exe"`.

Printers

This tab controls the mapping of printers.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Network printer list

A list of your of your existing printer resources, with unique IDs. You can use **Find** to filter your printers list by name or ID against a text string. You can import printers using Import Network Print Server on the ribbon.

To add a printer

1. On the **Network Printer List** tab, click **Add** or right-click the blank area and then select **Add** in the context menu.
2. In the **New Network Printer** window, type the required information and then click **OK**.

Fields and controls

Name. The display name of the printer, as it appears in the printer list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

Target Path. The path to the printer as it resolves in the user's environment.

Printer State. Toggles whether the printer is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

External Credentials. Allows you to state specific credentials with which to connect to the printer.

Self-Healing. Toggles whether the printer is automatically recreated for users when the agent refreshes.

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

Action Type. Describes what type of action this resource is. For **Use Device Mapping Printers File**, specify Target Path as the absolute path to an XML printer list file (see XML printer list configuration). When the agent refreshes it parses this XML file for printers to add to the action queue.

To import a printer

1. In the ribbon click **Import Network Print Server**.
2. Enter details in the **Import from Network Print Server** dialog, then click **OK**:

Fields and controls

Print Server Name. The name of the print server you wish to import printers from.

Use Alternate Credentials. By default, the import uses the credentials of the Windows account under whose identity the administration console is currently running. Select this option to specify different credentials for the connection to the print server.

Network Drives

Controls the mapping of network drives.

> **TIP:**
>
> You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Network drive list

A list of your existing network drives. You can use **Find** to filter the list by name or ID against a text string.

To add a network drive

1. Use the context menu **Add** command.
2. Enter details in the **New Network Drive** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the drive, as it appears in the network drive list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

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

Target Path. The path to the network drive as it resolves in the user's environment.

Network Drive State. Toggles whether the network drive is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

External Credentials. Allows you to state specific credentials with which to connect to the network drive.

Enable Automatic Self-Healing. Toggles whether the network drive is automatically recreated for your users when the agent refreshes.

Set as Home Drive.

Action Type. Describes what type of action this resource is. Defaults to Map Network Drive.

Virtual Drives

Controls the mapping of virtual drives. Virtual drives are Windows virtual drives or MS-DOS device names that map local file paths to drive letters.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Virtual drive list

Displays a list of your existing virtual drives. You can use **Find** to filter the list by name or ID.

A general workflow to add and assign a virtual disk is as follows:

1. Go to the **Administration Console > Actions > Virtual Drives > Virtual Drives List** tab, click **Add**. Alternatively, right-click the blank area and then select **Add** in the context menu. The **New Virtual Drive** window appears.
    a. On the **General** tab, type the required information and select whether to set the virtual drive as a home drive.
    b. Click **OK** to save changes and to exit the **New Virtual Drive** window.
2. Go to the **Administration Console > Assignments > Action Assignment** tab.
    a. Double-click the user or user group to which you want to assign the virtual drive.
    b. Select the virtual drive and click the right arrow (>) to assign it.

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

c. In the **Assign Filter & Driver Letter** window, select **Always True**, select a driver letter, and then click **OK**. The virtual drive moves from the **Available** pane to the **Assigned** pane.

The assignment might take some time to take effect, depending on the value you specified for **SQL Settings Refresh Delay** on the **Advanced Settings > Configuration > Service Options** tab. Perform the following steps for the assignment to take effect immediately if needed.

1. Go to the **Administration Console > Administration > Agents > Statistics** tab and then click **Refresh**.
2. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.

Fields and controls

THE GENERAL TAB

Name. The display name of the drive, as it appears in the virtual drive list.

Description. Lets you specify additional information about the virtual drive. The information appears only in the edition or creation wizard.

Target Path. Type the path to the virtual drive as it resolves in the user's environment.

Virtual Drive State. Toggles whether the virtual drive is enabled or disabled. When disabled, the agent does not process it even if it is assigned to a user.

Set as Home Drive. Lets you choose whether to set it as a home drive.

THE OPTIONS TAB

Action Type. Describes what type of action this resource is.

Registry Entries

Controls the creation of registry entries.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Registry value list

A list of your existing registry entries. You can use **Find** to filter the list by name or ID against a text string.

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

To add a registry entry

1. Use the context menu **Add** command.
2. Enter details in the **New Registry Value** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the registry entry, as it appears in the registry entry list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

Registry Value State. Toggles whether the registry entry is enabled or disabled. When disabled, it will not be processed by the agent even if assigned to a user.

Target Path. The registry location in which the registry entry will be created. Workspace Environment Management can only create Current User registry entries, so you do not need to preface your value with %ComputerName%\HKEY_CURRENT_USER – this is done automatically.

Target Name. The name of your registry value. It will appear in the registry (for example, NoNtSecurity).

Target Type. The type of registry entry that will be created.

Target Value. The value of the registry entry once created (for example, 0 or C:\Program Files)

Run Once. By default, Workspace Environment Management™ creates registry entries every time the agent refreshes. Select this check box to make Workspace Environment Management create the registry entry only once - on the first refresh - rather than on every refresh. This speeds up the agent refresh process, especially if you have many registry entries assigned to your users.

Action Type. Describes what type of action this resource is.

Import registry files

You can convert your registry file into registry entries for assignment. This feature has the following limitations:

- It supports only registry values under `HKEY_CURRENT_USER`. With the registry entries feature, you can assign only registry settings under `HKEY_CURRENT_USER`.
- It does not support registry values of the `REG_BINARY` and `REG_MULTI_SZ` types.

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

To avoid the limitations, we recommend that you import your registry files to WEM by using the **Import Registry File** option in **Group Policy Settings**. For more information, see Import Group Policy settings from registry files.

To import a registry file, do the following:

1. In the administration console, go to **Actions > Registry Entries**.
2. In the ribbon, click **Import Registry File**.
3. In the **Import from Registry File** window, browse to the registry file.
4. Click **Scan** to start scanning the registry file. After the scan completes successfully, a list of registry settings appears.
5. Select the registry settings that you want to import and then click **Import Selected** to start the import process.
6. Click **OK** to exit.

Fields and controls

Registry File Name. Populates automatically after you navigate to a **.reg** file and click **Open**. The **.reg** file contains registry settings you want to import into WEM. The **.reg** file must be generated from a clean environment to which only the registry settings you want to import are applied.

Scan. Scans the **.reg** file and then displays a list of registry settings that the file contains.

Registry Values List. Lists all registry values that the **.reg** file you want to import contains.

Enable Imported Items. If disabled, newly imported registry keys are disabled by default.

Prefix Imported Item Names. If selected, adds a prefix to the name of all registry items imported through this wizard (for example, “XP ONLY” or “finance”). Doing so makes it easier to identify and organize your registry entries.

NOTE:

The wizard cannot import registry entries with the same names. If your **.reg** file contains more than one registry entry that has the same name (as displayed in the Registry Values List), select one of these entries for import. If you want to import the others, rename them.

Environment Variables

Controls the creation of environment variables.

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

TIP

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Environment variable list

A list of your existing environment variables. You can use **Find** to filter the list by name or ID against a text string.

To add an environment variable

1. Use the context menu **Add** command.
2. Enter details in the **New Environment Variable** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the variable, as it appears in the environment variable list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

Environment Variable State. Toggles whether the environment variable is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Variable Name. The functional name of the environment variable.

Variable Value. The environment variable value.

Action Type. Describes what type of action this resource is.

Execution order.

Ports

The Ports feature allows client COM and LPT port mapping. You can also use Citrix Studio policies to enable automatic connection of COM ports and LPT ports. For more information, see Port redirection policy settings.

If you use the Ports feature to manually control the mapping of each port, remember to enable the Client COM port redirection or the Client LPT port redirection policies in Citrix Studio. By default, COM port redirection and LPT port redirection are prohibited.

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

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Ports list

A list of your existing ports. You can use **Find** to filter the list by name or ID.

To add a port

1. Select **Add** from the context menu.
2. Enter details on the **New Port** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the port, as it appears in the port list.

Description. Appears only in the edition/creation wizard and allows you to specify additional information about the resource.

Port State. Toggles whether the port is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Port Name. The functional name of the port.

Port Target. The target port.

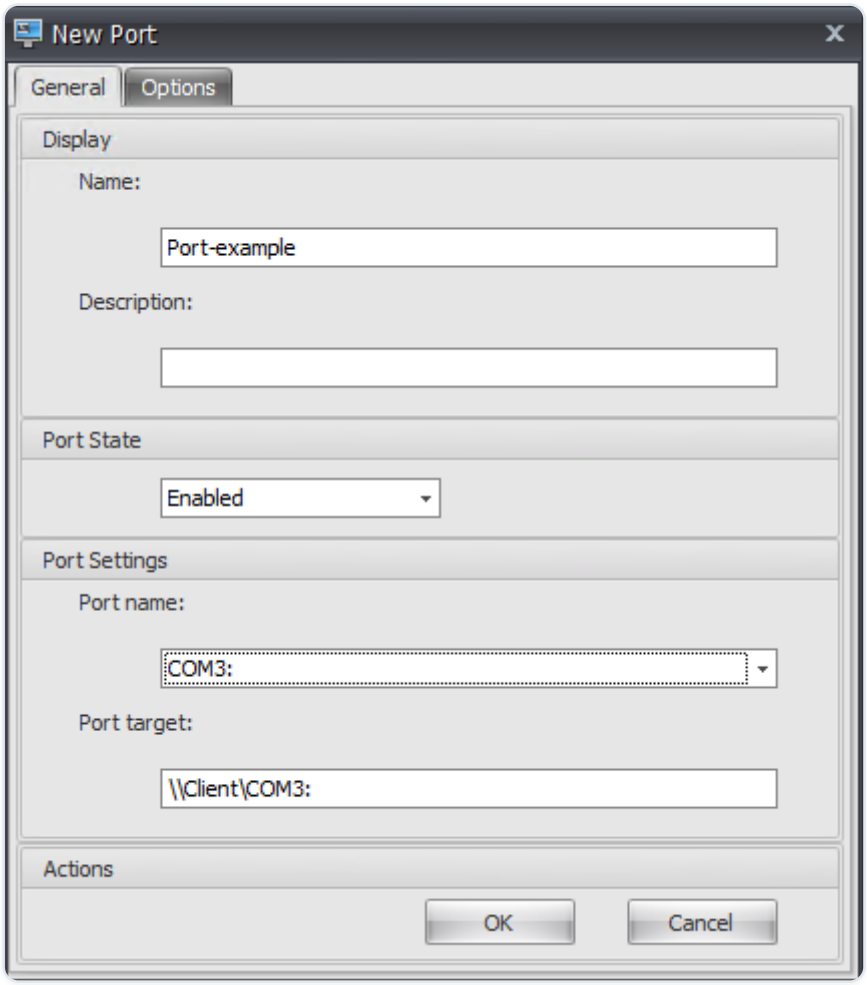
OPTIONS TAB

Action Type. Describes what type of action this resource is.

For example, you can configure the port settings as follows:

- **Port name**: Select “COM3:”
- **Port target**: Enter `\\Client\COM3:`

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



Ini Files

Controls the creation of **.ini** file operations, allowing you to modify **.ini** files.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Ini files operation list

A list of your existing ini file operations. You can use **Find** to filter the list by name or ID against a text string.

To add an .ini files operation

1. Use the context menu **Add** command.
2. Enter details in the **New Ini Files Operation** dialog tabs, then click **OK**.

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

Fields and controls

Name. The display name of the .ini file operation, as it appears in the **Ini File Operations** list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

.ini File Operation State. Toggles whether the .ini file operation is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Target Path. This specifies the location of the .ini file that will be modified as it resolves in the user's environment.

Target Section. This specifies which section of the .ini file is targeted by this operation. If you specify a non-existent section, it will be created.

Target Value Name. This specifies the name of the value that will be added.

Target Value. This specifies the value itself.

Run Once. By default, Workspace Environment Management™ performs an .ini file operation every time the agent refreshes. Tick this box to make Workspace Environment Management only perform the operation once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many .ini file operations assigned to your users.

Action Type. Describes what type of action this resource is.

External Tasks

Controls the execution of external tasks. External tasks include running scripts and applications as long as the agent host has the corresponding programs to run them. Commonly used scripts include: **.vbs** and **.cmd** scripts.

With the external tasks feature, you can specify when to run an external task. Doing so lets you more effectively manage user environments.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

External task list

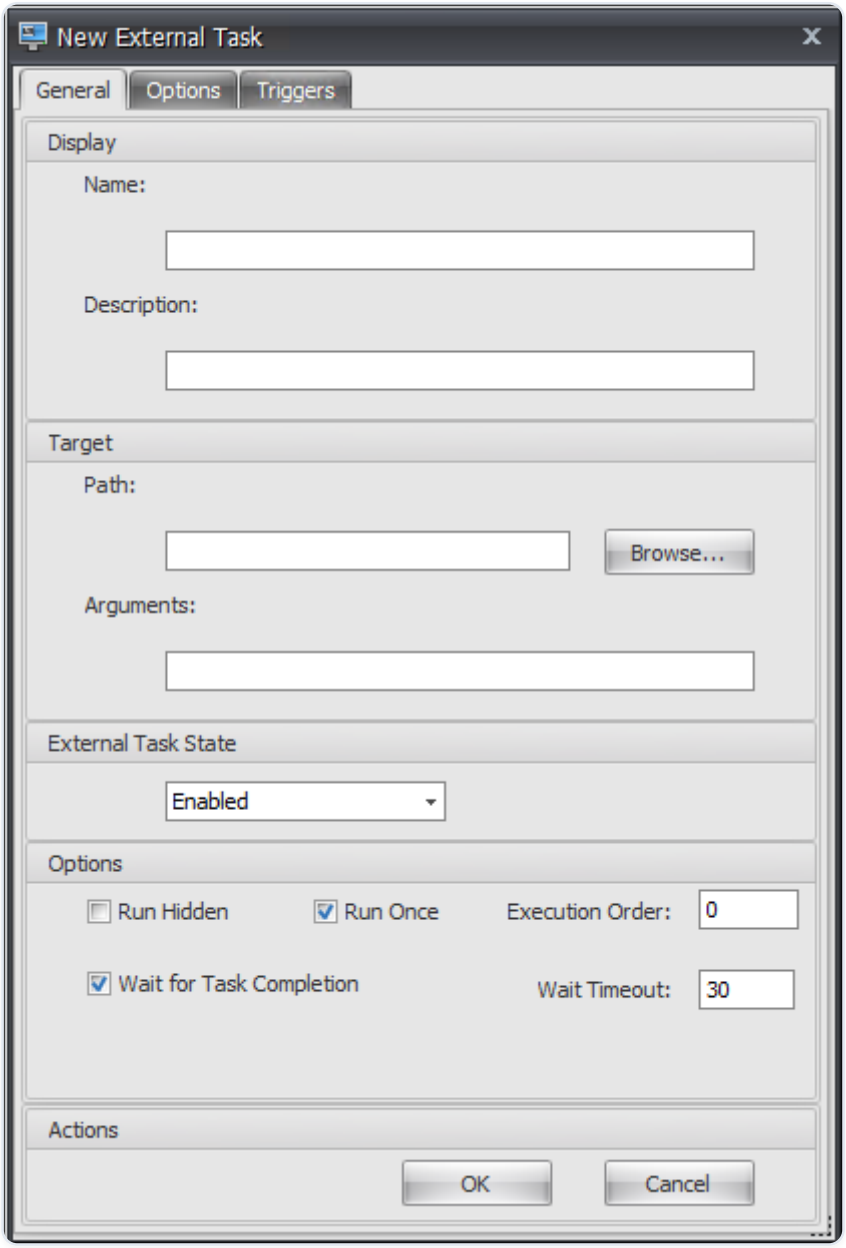
A list of your existing external tasks. You can use **Find** to filter the list.

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

To add an external task

1. Use the context menu **Add** command.
2. Enter details in the **New External Task** dialog tabs and then click **OK**.

Fields and controls



Name. Lets you specify the display name of the external task, which appears in the external task list.

Description. Lets you specify additional information about the external task.

Path. Lets you specify the path to the external task. The path resolves in the user environment. Make sure that:

- The path you specified here is consistent with the agent host.

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

- The agent host has the corresponding program to run the task.

Arguments. Lets you specify launch parameters or arguments. You can type a string. The string contains arguments to pass to the target script or application. For examples to use the **Path** and **Arguments** fields, see External task examples.

External Task State. Controls whether the external task is enabled or disabled. When disabled, the agent does not process the task even if the task is assigned to users.

Run Hidden. If selected, the task runs in the background and is not displayed to users.

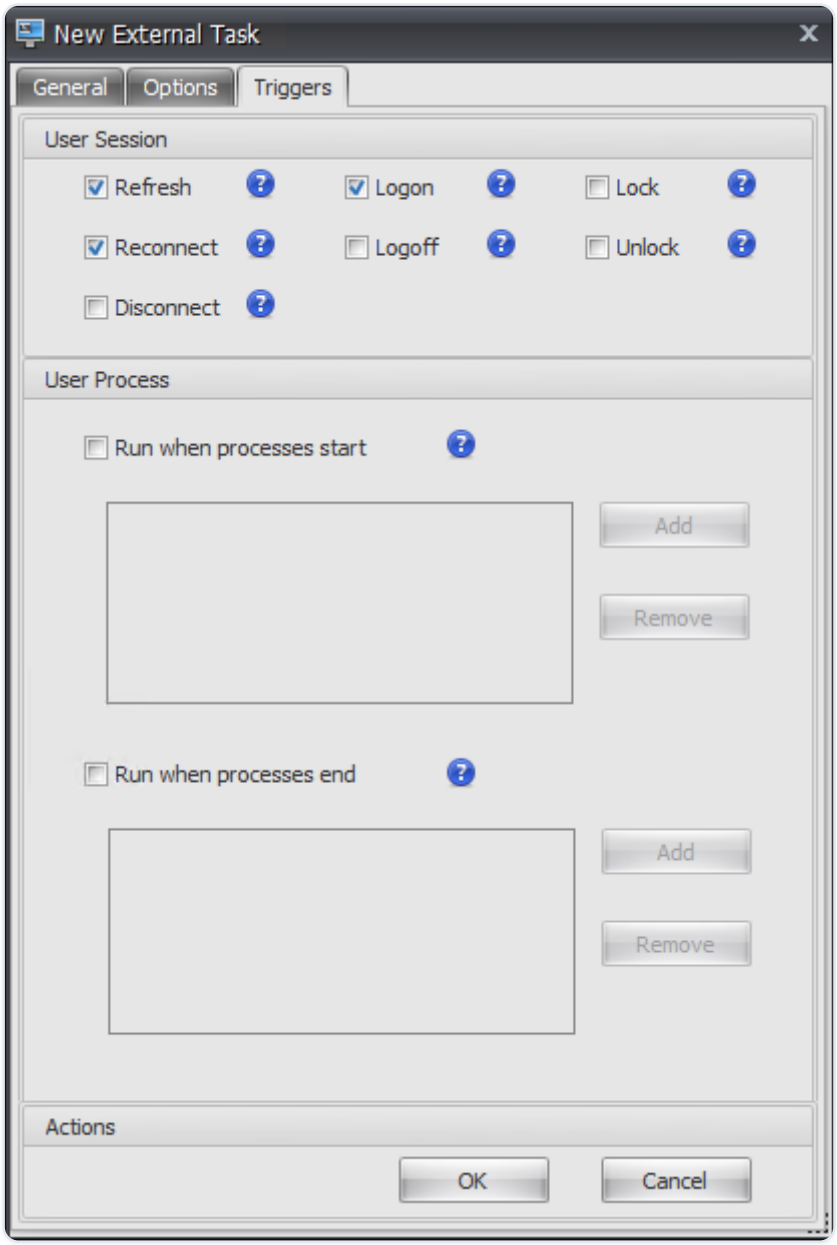
Run Once. If selected, WEM runs the task only once regardless of which options you select on the **Triggers** tab and regardless of whether agents restart. By default, this option is selected.

Execution Order. Lets you specify the running order of each task. The option can be useful when you have multiple tasks assigned to users and some of those tasks rely on others to run successfully. By default, the value is 0. Tasks with an execution order value of 0 (zero) run first, then those with a value of 1, then those with a value of 2, and so on.

Wait for Task Completion. Lets you specify how long the agent waits for the task to complete. By default, the **Wait Timeout** value is 30 seconds.

Action Type. Describes what type of action the external task is.

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



User session triggers. This feature lets you configure the following session activities as triggers for external tasks:

- **Refresh**. Controls whether to run the external task when users refresh the agent. By default, the option is selected.
- **Reconnect**. Controls whether to run the external task when a user reconnects to a machine on which the agent is running. By default, the option is selected. If the WEM agent is installed on a physical Windows device, this option is not applicable.
- **Logon**. Controls whether to run the external task when users log on. By default, the option is selected.
- **Logoff**. Controls whether to run the external task when users log off. This option does not work unless Citrix User Logon Service is running. By default, the option is not selected.

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

- **Disconnect**. Controls whether to run the external task when a user disconnects from a machine where the agent is running. By default, the option is not selected.
- **Lock**. Controls whether to run the external task when a user locks a machine where the agent is running. By default, the option is not selected.
- **Unlock**. Controls whether to run the external task when a user unlocks a machine where the agent is running. By default, the option is not selected.

When using disconnect, lock, and unlock options, consider the following constraints:

- The implementation of these options is based on Windows events. In some environments, these options might not work as expected. For example, in desktops running on Windows 10 or Windows 11 single-session VDAs, the disconnect option does not work. Instead, use the lock option. (In this scenario, the action we receive is “lock.”)
- We recommend that you use these options with the UI agent. Two reasons:
    - When you use the options with the CMD agent, the agent starts in the user environment each time the corresponding event occurs, to check whether the external task runs.
    - The CMD agent might not work optimally in concurrent task scenarios.

User process triggers. This feature lets you configure user processes as triggers for external tasks. Using this feature, you can define external tasks to supply resources only when certain processes are running and to revoke those resources when the processes end. Using processes as triggers for external tasks lets you manage your user environments more precisely compared with processing external tasks on logon or logoff.

- Before you use this feature, verify that the following prerequisites are met:
    - The WEM agent launches and runs in UI mode.
    - The specified processes run in the same user session as the logged-on user.
    - To keep the configured external tasks up to date, be sure to select **Enable Automatic Refresh** on the **Advanced Settings > Configuration > Advanced Options** tab.
- **Run when processes start**. Controls whether to run the external task when specified processes start.
- **Run when processes end**. Controls whether to run the external task when specified processes end.

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

Troubleshooting

After you enable the feature, the WEM agent creates a log file named `Citrix WEM Agent Logoff.log` the first time a user logs off. The log file is located in a user's profile root folder. The WEM agent writes information to the log file every time the user logs off. The information helps you monitor and troubleshoot issues related to external tasks.

External task examples

For a script (for example, PowerShell script):

- If neither the folder path nor the script name contains blank spaces:
  - In the **Path** field, type the following: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.
  - In the **Arguments** field, type the following: `C:\<folder path>\<script name>.ps1`.

  Alternatively, you can type the path to the script file directly in the **Path** field. For example: `C:\<folder path>\<script name>.ps1`. In the **Arguments** field, specify arguments if needed. However, whether the script file is run or opens with a different program depends on file type associations configured in the user environment. For information about file type associations, see File Associations.
- If the folder path or the script name contains blank spaces:
  - In the **Path** field, type the following: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.
  - In the **Arguments** field, type the following: `-file C:\<folder path>\<script name>.ps1`.

For an application (for example, iexplore.exe):

- In the **Path** field, type the following: `C:\Program Files\"Internet Explorer"\iexplore.exe`.
- In the **Arguments** field, type the URL of the website to open: `https://docs.citrix.com/`.

File System Operations

Controls the copying of folders and files into the user's environment.

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

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

File system operations list

A list of your existing file and folder operations. You can use **Find** to filter the list by name or ID against a text string.

To add a file system operation

1. Use the context menu **Add** command.
2. Enter details in the **New File System Operation** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the file or folder operation, as it appears in the list.

Description. Lets you specify additional information about the resource. This field appears only in the edition or creation wizard.

Filesystem Operation State. Controls whether the file system operation is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Source Path. The path to the source file or folder that is copied.

Target Path. The destination path for the source file or folder that is copied.

Overwrite Target if Existing. Controls whether the file or folder operation overwrites existing files or folders with the same names in the target location. If cleared, and a file or folder with the same name already exists at the target location, the affected files are not copied.

Run Once. By default, Workspace Environment Management™ runs a file system operation every time the agent refreshes. Select this option to let Workspace Environment Management run the operation only once, rather than on every refresh. This speeds up the agent refresh process, especially if you have many file system operations assigned to your users.

Action Type. Describes what type of action this file or folder action is: **Copy**, **Delete**, **Move**, **Rename** or **Symbolic Link** operation. For symbolic link creation, you need to give users the `SeCreateSymbolicLinkPrivilege` privilege for Windows to allow symbolic link creation.

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

Execution order. Determines the running order of operations, letting certain operations run before others. Operations with an execution order value of 0 (zero) run first, then those with a value of 1, then those with a value of 2, and so on.

User DSN

Controls the creation of user DSNs.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

User DSN list

A list of your existing user DSNs. You can use **Find** to filter the list by name or ID against a text string.

To add a user DSN

1. Use the context menu **Add** command.
2. Enter details in the **New User DSN** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the user DSN, as it appears in the user DSN list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

User DSN State. Toggles whether the user DSN is enabled or disabled. When disabled, it will not be processed by the agent even if assigned to a user.

DSN Name. The functional name of the user DSN.

Driver. The DSN driver. At present, only SQL server DSNs are supported.

Server Name. The name of the SQL server to which the user DSN is connecting.

Database Name. The name of the SQL database to which the user DSN is connecting.

Connect Using Specific Credentials. Allows you to specify credentials with which to connect to the server/database.

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

Run Once. By default, Workspace Environment Management™ will create a user DSN every time the agent refreshes. Tick this box to make Workspace Environment Management only create the user DSN once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many DSNs assigned to your users.

Action Type. Describes what type of action this resource is.

File Associations

IMPORTANT:

File type associations that you configure become default associations automatically. However, when you open an applicable file, the “How do you want to open this file?” window might still appear, prompting you to select an application to open the file. Click **OK** to dismiss the window. If you do not want to see a similar window again, do the following: Open the Group Policy Editor and enable the **Do not show the ‘new application installed’ notification** policy (**Computer Configuration > Administrative Templates > Windows Components > File Explorer**).

Controls the creation of file type associations in the user environment.

TIP:

You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

File association list

A list of your existing file associations. You can use **Find** to filter the list by name or ID.

To add a file association

1. Use the context menu **Add** command.
2. Enter details in the **New File Association** dialog tabs, then click **OK**.

Name. The display name of the file association, as it appears in the file association list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

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

File Association State. Toggles whether the file association is Enabled or Disabled. When disabled, it is not processed by the agent even if assigned to a user.

File Extension. The extension used for this file type association. If you select a file name extension from the list, the **ProgID** field automatically populates (if the file type is present on the machine where the administration console is running). You can also type the extension directly. However, for browser associations, you *must* type the extension directly. For more information, see Browser association.

ProgID. The programmatic identifier associated with an application (COM). This value automatically populates when you select a file extension from the list. You can also type the ProgID directly. To discover the ProgID of an installed application, you can use the OLE/COM Object Viewer (oleview.exe), and look in Object Classes/Ole 1.0 Objects. For more information about ProgID, see Programmatic identifier (ProgID).

Action. Lets you select the action type: open, edit, or print.

Target application. Lets you specify the executable used with this file name extension. Type the full path of the executable. For example, for UltraEdit Text Editor: `C:\Program Files\IDM Computer Solutions\UltraEdit\uedit64.exe`

Command. Lets you specify action types that you want to associate with the executable. For example:

- For an open action, type `“%1”`.
- For a print action, type `/p"%1"`.

Set as Default Action. Toggles whether the association is set as a default for that file name extension.

Overwrite. Toggles whether this file association overwrites any existing associations for the specified extension.

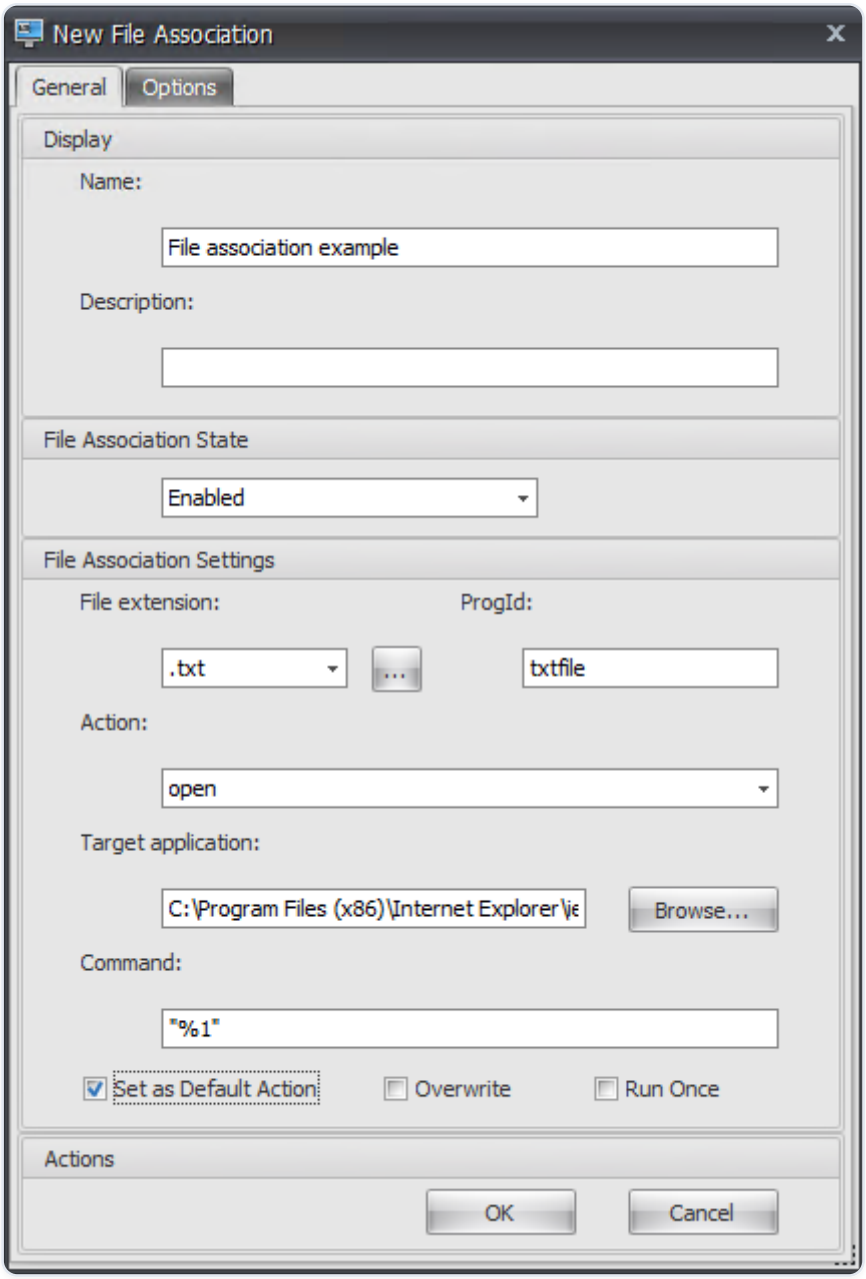
Run Once. By default, Workspace Environment Management™ (WEM) creates a file association every time the agent refreshes. Select this option to create the file association once, rather than on every refresh. This speeds up the agent refresh process, especially if you have many file associations assigned to your users.

Action Type. Describes what type of action this resource is.

For example, to add a new file type association for text (.txt) files for users to automatically open text files with the program you selected (here, iexplore.exe), complete the following steps.

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

1. On the **Administration Console \> Actions \> File Associations \> File Association List** tab, click **Add**.
2. In the **New File Association** window, type the information and then click **OK**.



- **File Association State**. Select **Enabled**.
- **File extension**. Type the file name extension. In this example, type .txt.
- **Action**. Select **Open**.
- **Target application**. Click **Browse** to navigate to the applicable executable (.exe file). In this example, browse to iexplore.exe located in the C:\Program Files (x86)\Internet Explorer folder.
- **Command**. Type “%1” and make sure to wrap %1 in double quotes.

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

- Select **Set as Default Action**.

3. Go to the **Administration Console \> Assignments \> Action Assignment** tab.
4. Double-click the user or user group to which you want to assign the action.
5. Go to the **Administration Console \> Administration \> Agents \> Statistics** tab and then click **Refresh**.
6. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.
7. Go to the machine on which the agent is running (user environment) to verify that the created file type association works.

In this example, if you double-click a file with a .txt extension in the end-user environment, that file automatically opens in Internet Explorer.

Good to know

Browser association

WEM supports creating an association for these browsers:

- Google Chrome
- Firefox
- Opera
- Internet Explorer (IE)
- Microsoft Edge
- Microsoft Edge Chromium

When creating browser associations, keep the following in mind:

- In the **File extension** field, type `http` or `https`.
- In the **ProgID** field, type the following (case sensitive) based on your choice:
  - `ChromeHTML` for Google Chrome
  - `firefox` for Firefox
  - `OperaStable` for Opera
  - `IE` for Internet Explorer (IE)
  - `edge` for Microsoft Edge
  - `edge` or `MSEdgeHTM` for Microsoft Edge Chromium

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

Programmatic identifier (ProgID)

You no longer have to fill out the following fields: **Action**, **Target application**, and **Command**. You can leave the fields empty as long as you can provide the correct **ProgID**. See below a list of ProgIDs for popular applications:

- Acrobat Reader DC: `AcroExch.Document.DC`
- Opera browser: `OperaStable`
- Google Chrome browser: `ChromeHTML`
- Internet Explorer: `htmlfile`
- Wordpad: `textfile`
- Notepad: `txtfile`
- Microsoft Word 2016: `Word.Document.12`
- Microsoft PowerPoint 2016: `PowerPoint.Show.12`
- Microsoft Excel 2016: `Excel.Sheet.12`
- Microsoft Visio 2016: `Visio.Drawing.15`
- Microsoft Publisher 2016: `Publisher.Document.16`

However, you must fill out the fields (**Action**, **Target application**, and **Command**) if:

- You cannot provide the correct **ProgID**.
- The target application (for example, UltraEdit Text Editor) does not register its own ProgID in the registry during installation.

Filters

Filters contain rules and conditions that let you make actions available (assign actions) to users. Set up rules and conditions before assigning actions to users.

Rules

Rules are composed of multiple conditions. You use rules to define when an action is assigned to a user.

Filter rule list

A list of your existing rules. You can use **Find** to filter the list by name or ID against a text string

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

To add a filter rule

1. Use the context menu **Add** command.
2. Enter details in the **New Filter Rule** dialog.
3. Move conditions you want configured in this rule from the **Available** list to the **Configured** list.
4. Click **OK**.

Fields and controls

Name. The display name of the rule, as it appears in the rule list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the rule.

Filter Rule State. Toggles whether the rule is enabled or disabled. When disabled, the agent does not process actions using this rule even if they are assigned.

Available Conditions. These are the filter conditions available to be added to the rule. Note. The **DateTime** filter expects results in the format: `YYYY/MM/DD HH:mm`

Multiple values can be separated with semicolons (;) and ranges can be separated with hyphens. When specifying a range between two times on the same date, the date must be included in both ends of the range, for example: 1969/12/31 09:00-1969/12/31 17:00

Configured Conditions. These are the conditions already added to the rule.

NOTE:

These conditions are **AND** statements, not **OR** statements. Adding multiple conditions requires them all to trigger for the filter to be considered triggered. The **OR** condition applies only to the WEM Webconsole, and the agent version must be greater than or equal to 2210.2.0.1. For more information, see Add a filter.

Conditions

Conditions are specific triggers which allow you to configure the circumstances under which the agent acts to assign a resource to a user.

Filter condition list

A list of your existing conditions. You can use **Find** to filter the list by name or ID against a text string.

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

To add a filter condition

1. Use the context menu **Add** command.
2. Enter details in the **New Filter Condition** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the condition, as it appears in the condition list and in the rule creation/edition wizard.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the condition.

Filter Condition State. Toggles whether the filter is enabled or disabled. When disabled, it will not appear in the rule creation/edition wizard.

Filter Condition Type. The type of filter condition type to use. See Filter conditions. Note: rules using the Always True condition will always trigger.

Settings. These are the specific settings for individual conditions. See Filter conditions.

> **NOTE:**
>
> When entering an IP address, you can either specify individual addresses or ranges.

If you specify a range, both bounds must be specified in full. Use the dash character (**-**) to separate IP range bounds (for example **192.168.10.1-192.168.10.5**). Separate multiple ranges or addresses using the semicolon character (**;**) . For example, **192.168.10.1-192.168.10.5;192.168.10.8-192.168.10;192.168.10.17** is a valid value which includes the ranges **.1-.5** and **.8-.10**, plus the individual address **.17**.

Assignments

> **TIP:**
>
> Before assigning actions to users, perform the following steps in the order given:

- Configure users, see Users in Active Directory Objects.
- Define conditions, see Conditions.
- Define filter rules, see Rules.

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

- Configure actions, described here.

Use assignments to make actions available to your users. This lets you replace a portion of your users' logon scripts.

Action assignment

Users

This is your list of configured users and groups (see Users in Active Directory Objects). Double-click a user or group to populate the assignments menu. Use **Find** to filter the list by name or ID.

TIP:

To simplify assigning actions for all users in Active Directory, use the "Everyone" default group to assign the actions. The actions that you assign to the "Everyone" default group do not appear on the **Resultant Actions** tab in the **Actions Modeling Wizard** for an individual user. For example, after you assign action1 to the "Everyone" default group, you might find that action1 does not appear on the **Resultant Actions** tab.

Assignments

Lets you assign actions to the selected user or group. Use **Find** to filter the list by name or ID.

Available. Displays actions available for you to assign to this user or group.

Double-click an action or click the arrow buttons to assign or unassign it. When you assign an action, you are prompted to select a rule to contextualize it.

Assigned. Displays actions already assigned to this user or group. You can expand individual actions to configure them (application shortcut locations, default printers, drive letter, and so on).

To assign actions to users/groups

1. In the **Users** list, double-click a user or group. This populates the Assignments lists.
2. In the **Available** list, select an action and click the right-arrow (**>**) button.
3. In the **Assign Filter** dialog, select a **Filter Rule** and click **OK**.
4. In the **Assigned list**, you can use the **Enable** and **Disable** context actions to fine-tune the behavior of the assignment.

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

NOTE:

For the **Pin To Start Menu** option to work, make sure that the application shortcut exists in the Start menu folder. If unsure, enable the **Create Start Menu** option as well.

For example, say you assign an action to start Notepad. In the Assigned list, the option "Autostart" is provided and set to "Disabled" by default. If you use the **Enable** option to enable Autostart, Notepad (local Notepad on the VDA) automatically launches when the user launches a published desktop session (local Notepad automatically starts when the desktop completes loading).

Modeling wizard

The **Actions Modeling Wizard** displays the resultant actions for a given user only (it does not work for groups).

Fields and controls

Actions Modeling Target User. The account name for the user you want to model.

Resultant Actions. The actions assigned to the user or to groups the user belongs to.

User Groups. The groups the user belongs to.

System Optimization

Workspace Environment Management™ system optimization consists of the following:

- CPU Management
- Memory Management
- I/O Management
- Fast Logoff
- Citrix Optimizer

These settings are designed to lower resource usage on the agent host. They help to ensure that freed-up resources are available for other applications. Doing so increases user density by supporting more users on the same server.

While system optimization settings are machine-based and apply to all user sessions, process optimization is user centric. This means that when a process triggers CPU Spike Protection in user

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

A's session, the event is recorded only for user A. When user B starts the same process, process optimization behavior is determined only by process triggers in user B's session.

CPU Management

The following settings let you optimize CPU usage.

CPU management settings

Processes can run across all cores and can use up as much CPU as they want. In Workspace Environment Management™ (WEM), **CPU Management Settings** lets you limit how much CPU capacity individual processes can use. CPU spike protection is not designed to reduce overall CPU usage. It is designed to reduce the impact on user experience by processes that consume an excessive percentage of CPU Usage.

When CPU spike protection is enabled, if a process reaches a specified threshold, WEM automatically lowers the priority of the process for a certain time. Then, when a new application is launched, it has a higher priority than the lower-priority process and the system will continue to run smoothly.

CPU spike protection examines each process in a quick "snapshot." If the average load of a process exceeds the specified usage limit for a specified sample time, its priority reduces immediately. After a specified time, the process' CPU priority returns to its previous value. The process is not "throttled." Unlike in **CPU Clamping**, only its priority is reduced.

CPU spike protection is not triggered until at least one instance of an individual process exceeds the threshold. In other words, even if total CPU consumption exceeds the specified threshold, CPU spike protection is not triggered unless at least one process instance exceeds the threshold. But when that process instance triggers CPU spike protection, new instances of the same process are (CPU) optimized when the option "Enable Intelligent CPU Optimization" is enabled.

Whenever a specific process triggers CPU spike protection, the event is recorded in the agent's local database. The agent records trigger events for each user separately. This means that CPU optimization for a specific process for user1 does not affect the behavior of the same process for user2.

For example, if Internet Explorer is sometimes consuming 50–60% of CPU, you can use CPU spike protection to target only those iexplore.exe instances that are threatening VDA performance. (By contrast, CPU clamping would apply to all processes.)

We recommend that you experiment with the sample time to decide the optimal value for your environment that does not affect other users logged on to the same VDA.

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

CPU Spike Protection

NOTE:

- *CPU usage* in the following settings is based on *logical processors* in the physical or virtual machine. The total number of logical processors can be obtained from the system information of either the physical machine or the virtual machine. If a physical machine or a VM has a total of 48 logical processors, restricting the processes that trigger CPU spike protection on the physical machine or the VM to use half of its cores, set the limit of the CPU core usage to 24.

Enable CPU Spike Protection. Lowers the CPU priority of processes for a period (specified in the **Idle Priority Time** field) if they exceed the specified percentage of CPU usage for a period (specified in the **Limit Sample Time** field).

- **Auto Prevent CPU Spikes**. Use this option to automatically reduce the CPU priority of processes that overload your CPU. This option automatically calculates the threshold value at which to trigger CPU spike protection based on the number of logical processors (CPU cores). For example, suppose that there are four cores. With this option enabled, if the overall CPU usage exceeds 23%, the CPU priority of processes that consume more than 15% of the overall CPU resources reduces automatically. Similarly, in the case of 8 cores, if the overall CPU usage exceeds 11%, the CPU priority of processes that consume more than 8% of the CPU resources reduces automatically.
- **Customize CPU Spike Protection.** Lets you customize settings for CPU spike protection.
    - **CPU Usage Limit**. The percentage of CPU usage that any process instance must reach to trigger CPU spike protection. This limit is global across all logical processors in the server, and is determined on an instance-by-process basis. Multiple instances of the same process do not have their CPU usage percentages added when determining CPU spike protection triggers. If a process instance never reaches this limit, CPU spike protection is not triggered. For example, on a Server VDA, in multiple concurrent sessions, suppose that there are many iexplore.exe instances. Each instance peaks at around 35% CPU usage for periods of time, so that cumulatively, iexplore.exe is consistently consuming a high percentage of CPU usage. However, CPU spike protection is never triggered unless you set the CPU Usage Limit at or below 35%.
    - **Limit Sample Time**. The length of time for which a process must exceed the CPU usage limit before its CPU priority is lowered.

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

    - **Idle Priority Time**. The length of time for which the CPU priority of the process is lowered. After that time, the priority returns to one of the following:
        - The default level (**Normal**) if the process priority is not specified on the **CPU Priority** tab and the **Enable Intelligent CPU Optimization** option is not selected.
        - The specified level if the process priority is specified on the **CPU Priority** tab, regardless of whether the **Enable Intelligent CPU Optimization** option is selected.
        - A random level depending on the behavior of the process. This case occurs if the process priority is not specified on the **CPU Priority** tab and the **Enable Intelligent CPU Optimization** option is selected. The more frequently the process triggers CPU spike protection, the lower its CPU priority is.

Enable CPU Core Usage Limit. Limits processes that trigger CPU spike protection to a specified number of logical processors on the machine. Type an integer in the range of 1 through X, where X is the total number of cores. If you type an integer greater than X, WEM limits the maximum consumption of isolated processes to X by default.

- **Limit CPU Core Usage**. Specifies the number of logical processors to which processes that trigger CPU spike protection are limited. In the case of VMs, the value you type limits the processes to the number of logical processors in the VMs rather than in the underlying physical hardware.

Enable Intelligent CPU Optimization. When enabled, the agent intelligently optimizes the CPU priority of processes that trigger CPU spike protection. Processes that repeatedly trigger CPU spike protection are assigned progressively lower CPU priority at launch than processes that behave correctly. Note that WEM does not perform CPU optimization for the following system processes:

- Taskmgr
- System Idle Process
- System
- Svchost
- LSASS
- Wininit
- services
- csrss
- audiodg

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

- MsMpEng
- NisSrv
- mscorsvw
- vmwareresolutionset

Enable Intelligent I/O Optimization. When enabled, the agent intelligently optimizes the process I/O priority of processes that trigger CPU spike protection. Processes that repeatedly trigger CPU spike protection are assigned progressively lower I/O priority at launch than processes that behave correctly.

Exclude Specified Processes. By default, WEM CPU management excludes all of the most common Citrix and Windows core service processes. You can, however, use this option to **Add** or **Remove** processes from an exclusion list for CPU spike protection by executable name (for example notepad.exe). Typically, antivirus processes would be excluded.

TIP:

- To stop antivirus scanning taking over disk I/O in the session, you can also set a static I/O Priority of Low for antivirus processes, see I/O Management.
- When processes trigger CPU spike protection, and process CPU priority is lowered, WEM logs a warning each time it lowers the CPU priority of a process. In the Event Log, in Application and Services Logs, WEM Agent Service, look for "**Initializing process limitation thread for process**".

CPU SPIKE PROTECTION OPTION

Choose how you want to enforce CPU spike protection:

- **Automatically prevent CPU spikes**. Use this option to let the agent perform CPU spike protection when the system CPU usage (relative to a single CPU core) exceeds 90% and the process CPU usage (relative to a single CPU core) exceeds 80%.
- **Customize CPU spike protection**. Lets you customize settings for CPU spike protection.
    - **CPU usage limit**. The percentage of CPU usage that any process instance must reach to trigger CPU spike protection. This limit is global across all logical processors on the server, and is determined on an instance-by-process basis. To configure the limit based on a single CPU core as a reference, use the **Set limit relative to single CPU core** option.

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

NOTE:

- Both integer and non-integer values are supported. By entering a non-integer value, for example 37.5%, you restrict processes that use more than three cores on an eight-core platform.
- **Set limit relative to single CPU core**. Lets you set a limit on CPU usage based on a single CPU core as a reference. The value can be greater than 100%, for example, 200% or 250%. Example: When the value is set to 200%, the agent optimizes processes that use two or more CPU cores. Both integer and non-integer values are supported. You can configure the **Set limit relative to single CPU core** setting only for the WEM Web console.
- With **Customize CPU spike protection** configured, CPU spike protection is triggered when either the global CPU usage limit or the CPU usage limit relative to a single CPU core is reached, whichever occurs first.

For processes that trigger CPU spike protection, the agent can do the following:

- If the **Enable CPU core usage limit** option is not selected: The agent lowers the CPU priority of those processes.
- If the **Enable CPU core usage limit** option is selected: The agent lowers the CPU priority of those processes and limits them to the specified number of logical processors on the machine.

When configuring CPU spike protection, keep the following in mind:

- Multiple instances of the same process do not have their CPU usage percentages added when determining CPU spike protection triggers. If a process instance never reaches this limit, CPU spike protection is not triggered. For example, in the case of a multi-session VDA with multiple concurrent sessions, there are multiple chrome.exe processes. Their CPU usage is not summed together when calculating the CPU usage.

SAMPLING TIME FOR CPU SPIKE PROTECTION

Sample time limit. The length of time for which a process must exceed the CPU usage limit before CPU spike protection is enforced.

PRIORITY LOWERING TIME FOR CPU SPIKE PROTECTION

Idle priority time. The length of time for which the CPU priority of the process is lowered. After that time, the priority returns to one of the following:

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

The default level (**Normal**), if the process priority is not specified in the **CPU priority** tile and the **Enable intelligent CPU optimization** option is not selected. The specified level, if the process priority is specified in the **CPU priority** tile, regardless of whether the **Enable intelligent CPU optimization** option is selected. The calculated random level, depending on the behavior of the process. This case occurs if the process priority is not specified in the CPU priority tile and the **Enable intelligent CPU optimization** option is selected. The more frequently the process triggers CPU spike protection, the lower its CPU priority is.

ADDITIONAL OPTIONS

Enable CPU core usage limit. Use this option to limit processes that trigger CPU spike protection to a specific number of logical processors on the machine.

CPU priority

These settings take effect if processes are competing for a resource. They let you optimize the CPU priority level of specific processes, so that processes that are contending for CPU processor time do not cause performance bottlenecks. When processes compete with each other, processes with lower priority are served after other process with a higher priority. They are therefore less likely to consume such a large share of the overall CPU consumption.

The process priority you set here establishes the "base priority" for all of the threads in the process. The actual, or "current," priority of a thread might be higher (but is never lower than the base). When a number of processes are running on a computer, the processor time is shared between them based on their CPU priority level. The higher the CPU priority level of a process is, the more the processor time is assigned to it.

NOTE:

The overall CPU consumption does not necessarily decrease if you set lower CPU priority levels on specific processes. There might be other processes (with higher CPU priority) still affecting percentage CPU usage.

Enable Process Priority. When selected, lets you set CPU priority for processes manually.

To add a process

1. Click **Add** and type details in the **Add Process CPU Priority** dialog box.
2. Click **OK** to close the dialog box.
3. Click **Apply** to apply the settings. Process CPU priorities you set here take effect when the agent receives the new settings and the process is restarted.

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

Process Name. The process executable name without the extension. For example, for Windows Explorer (explorer.exe) type "explorer".

CPU Priority. The "base" priority of all threads in the process. The higher the priority level of a process is, the more the processor time it gets. Select from Realtime, High, Above Normal, Normal, Below Normal, and Low.

To edit a process

Select the process and click **Edit**.

To remove a process

Select the process and click **Remove**.

CPU affinity

Enable Process Affinity. When enabled, lets you define how many "logical processors" a process uses. For example, you can restrict every instance of Notepad launched on the VDA to the number of cores defined.

CPU clamping

CPU clamping prevents processes using more than a specified percentage of the CPU's processing power. WEM "throttles" (or "clamps") that process when it reaches the specified CPU percentage you set. This lets you prevent processes from consuming large amounts of CPU.

NOTE:

- CPU clamping is a brute force approach that is computationally expensive. To keep the CPU usage of a troublesome process artificially low, it is better to use CPU spike protection, at the same time as assigning static CPU priorities and CPU affinities to such processes. CPU clamping is best reserved for controlling processes that are notoriously bad at resource management, but that cannot stand to be dropped in priority.
- After you apply a percentage of the CPU’s processing power for a process and configure a different percentage for the same process later, select **Refresh Agent Host Settings** for the change to take effect.

The clamping percentage you configure is applied to the total power of any individual CPU in the server, not to any individual core it contains. (In other words, 10% on a quad-core CPU is 10% of the entire CPU, not 10% of one core).

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

Enable Process Clamping. Enable process clamping.

Add. Add the process by executable name (for example, notepad.exe).

Remove. Remove the highlighted process from the clamping list.

Edit. Edit the values typed for a given process.

TIP:

- When WEM is clamping a process, it adds the process to its watchlist the WEM client initializes. You can verify that a process is clamped by viewing this.
- You can also verify that CPU clamping is working by looking at process monitor and confirming that CPU consumption never rises above the clamping percentage.

Memory Management

These settings let you optimize application memory usage through Workspace Environment Management™ (WEM).

Memory management

If these settings are enabled, WEM calculates how much memory a process is using and the minimum amount of memory a process needs without losing stability. WEM considers the difference as excess memory. When the process becomes idle, WEM releases the excess memory that the process consumes to the page file, and optimizes the process for subsequent launches. Usually, an application becomes idle when it is minimized to the task bar.

When applications are restored from the task bar, they initially run in their optimized state but can continue to consume additional memory as needed.

Similarly, WEM optimizes all applications that users are using during their desktop sessions. If there are multiple processes over multiple user sessions, all memory that is freed up is available for other processes. This behavior increases user density by supporting a greater number of users on the same server.

Optimize Memory Usage for Idle Processes. Forces processes that remain idle for a specified time to release excess memory until they are no longer idle.

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

Idle Sample Time (min). Lets you specify the length of time that a process is considered idle after which it is forced to release excess memory. During this time, WEM calculates how much memory a process is using and the minimum amount of memory a process needs without losing stability. The default value is 120 minutes.

Idle State Limit (percent). Lets you specify the percentage of CPU usage below which a process is considered idle. The default is 1%. We recommend that you do not use a value greater than 5%. Otherwise, a process being actively used can be mistaken for idle, causing its memory to be released.

Do Not Optimize When Total Available Memory Exceeds (MB). Lets you specify a threshold limit below which WEM optimizes memory usage for idle applications.

Exclude Processes from Memory Usage Optimization. Lets you exclude processes from memory usage optimization. Specify the process name, for example, notepad.exe.

WEM does not optimize application memory usage for the following system processes:

- `rdpshell`
- `wfshell`
- `rdpclip`
- `wmiprvse`
- `dllhost`
- `audiodg`
- `msdtc`
- `mscorsvw`
- `spoolsv`
- `smss`
- `winlogon`
- `svchost`
- `taskmgr`
- `System Idle Process`
- `System`
- `LSASS`
- `wininit`

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

- `msiexec`
- `services`
- `csrss`
- `MsMpEng`
- `NisSrv`
- `Memory Compression`

Memory usage limit

Enable Memory Usage Limit for Specific Processes. Lets you limit the memory usage of a process by setting an upper limit for the memory the process can consume.

WARNING:

Applying memory usage limits to certain processes might have unintended effects, including slow system responsiveness.

- **Add**. Lets you add a process to which you want to apply a memory usage limit.
- **Remove**. Lets you delete an item.
- **Edit**. Lets you edit an item.
- **Dynamic Limit**. Lets you apply a dynamic limit to the specified process. This setting dynamically limits the amount of memory allocated to the specified process. If applied, enforces memory usage limits depending on available memory. Therefore, the memory that the specified process consumes might exceed the specified amount.
- **Static Limit**. Lets you apply a static limit to the specified process. This setting always limits the amount of memory allocated to the specified process. If applied, restricts the process from consuming more than the specified amount of memory regardless of the amount of available memory. As a result, the memory that the specified process consumes is capped at the specified amount.

To add a process:

1. On the **Administration Console > System Optimization > Memory Management > Memory Usage Limit** tab, click **Add**.
2. In the **Add Process** window, type the name of the process you want to add (for example, notepad.exe.), configure the memory usage limit, select a limit mode from the drop-down menu, and then click **OK**.

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

To edit an item, select the item and click **Edit**.

To remove an item, select the item and click **Remove**.

To apply a dynamic limit to an item, select the item and click **Dynamic Limit**.

To apply a static limit to an item, select the item and click **Static Limit**.

I/O Management

These settings allow you to optimize the I/O priority of specific processes, so that processes which are contending for disk and network I/O access do not cause performance bottlenecks. For example, you can use I/O Management settings to throttle back a disk-bandwidth-hungry application.

The process priority you set here establishes the "base priority" for all of the threads in the process. The actual, or "current," priority of a thread might be higher (but is never lower than the base). In general, Windows give access to threads of higher priority before threads of lower priority.

I/O priority

Enable Process I/O Priority. Enables manual setting of process I/O priority.

To add a process to the I/O priority list

1. Click **Add** and type details in the **Add Process I/O Priority** dialog.
2. Click **OK** to close the dialog.
3. Click **Apply** to apply the settings. Process I/O priorities you set here take effect when the agent receives the new settings and the process is next restarted.

Process Name. The process executable name without the extension. For example, for Windows Explorer (explorer.exe) type "explorer".

I/O Priority. The "base" priority of all threads in the process. The higher the I/O priority of a process, the sooner its threads get I/O access. Choose from High, Normal, Low, Very Low.

To edit a process I/O priority item

Select the process name and click **Edit**.

To remove a process from the I/O priority list

Select the process name and click **Remove**.

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

Fast Logoff

Fast Logoff ends the HDX™ connection to a remote session immediately, giving users the impression that the session has immediately closed. However, the session itself continues through the session logoff phases in the background on the VDA.

NOTE:

Fast Logoff supports Citrix Virtual Apps™ and RDS resources only.

Settings

Enable Fast Logoff. Enables fast logoff for all users in this configuration set. Users are logged out immediately, while session logoff tasks continue in the background.

Exclude Specific Groups. Allows you to exclude specific groups of users from Fast Logoff.

Citrix Optimizer

Citrix optimizer optimizes user environments for better performance. It runs a quick scan of user environments and then applies template-based optimization recommendations. You can optimize user environments in two ways:

- Use built-in templates to perform optimizations. To do so, select a template applicable to the operating system.
- Alternatively, create your own customized templates with specific optimizations you want and then add the templates to Workspace Environment Management™ (WEM).

To get a template that you can customize, use either of the following approaches:

- Use the template builder feature that the standalone Citrix Optimizer offers. Download the standalone Citrix Optimizer at `<https://support.citrix.com/article/CTX224676>`. The template builder feature lets you build your own custom templates to be uploaded to WEM.
- On an agent host (machine where the WEM agent is installed), navigate to the `<C:\Program Files (x86)>\Citrix\Workspace Environment Management Agent\Citrix Optimizer\Templates` folder, select a default template file, and copy it to a convenient folder. Customize the template file to reflect your specifics and then upload the custom template to WEM.

Settings

Enable Citrix Optimizer. Controls whether to enable or disable Citrix optimizer.

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

Run Weekly. If selected, WEM runs optimizations on a weekly basis. If **Run Weekly** is not selected, WEM behaves as follows:

- The first time you add a template to WEM, WEM runs the corresponding optimization. WEM runs the optimization only once unless you make changes to that template later. Changes include applying a different template to OS and moving optimization entries around between the **Available** and **Configured** panes.
- Each time you make changes to a template, WEM runs the optimization once.

NOTE:

For a non-persistent VDI environment, WEM follows the same behavior – all changes to the environment are lost when the machine restarts. In the case of Citrix Optimizer, WEM runs optimizations each time the machine restarts.

Automatically Select Templates to Use. If you are unsure which template to use, use this option to let WEM select the best match for each OS.

- **Enable Automatic Selection of Templates Starting with Prefixes**. Use this option if custom templates with different name formats are available. Type a comma-separated list of prefixes. Custom template follows this name format:
  - `prefix_<os version>_<os build>`
  - `prefix_Server_<os version>_<os build>`

The **Citrix Optimizer** tab displays a list of templates you can use to perform system optimizations. The **Actions** section displays the actions available to you:

- **Add**. Lets you add a custom template.
- **Remove**. Lets you delete an existing custom template. You cannot delete built-in templates.
- **Edit**. Lets you edit an existing template.
- **Preview**. Lets you have an itemized view of the optimization entries that the selected template contains.

To add a custom template:

1. On the **Administration Console > System Optimization > Citrix Optimizer > Citrix Optimizer** tab, click **Add**.

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

2. In the **New Custom Template** window, click **Browse** to select the applicable template, select the applicable OS from the list, configure groups contained in the template, and then click **OK**.

IMPORTANT:

- Citrix optimizer does not support exporting custom templates. Retain a local copy of your custom template after you add it.

To edit a template, select the applicable template and then click **Edit**.

To remove a template, select the applicable template and then click **Remove**.

To view details of a template, select the applicable template and then click **Preview**.

Fields and controls

Template Name. The display name of the selected template.

Applicable OSs. A list of operating systems. Select one or more operating systems to which the template applies. You can add custom templates applicable to Windows 10 OSs that are not available on the list. Add those OSs by typing their build numbers. Be sure to separate the OSs with semicolons (;). For example, 2001;2004.

IMPORTANT:

You can apply only one template to the same OS.

Groups. The **Available** pane displays a list of grouped optimization entries. The entries are grouped by category. Double-click a group or click the arrow buttons to move the group around.

State. Toggles the template between enabled and disabled states. If disabled, the agent does not process the template, and WEM does not run optimizations associated with the template.

Changes to Citrix optimizer settings take some time to take effect, depending on the value that you specified for the **SQL Settings Refresh Delay** option on the **Advanced Settings > Configuration > Service Options** tab.

For the changes to take effect immediately, navigate to the context menu of the **Administration > Agents > Statistics** tab and then select **Process Citrix Optimizer**.

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

TIP:

- New changes might fail to take effect immediately. We recommend that you select **Refresh Agent Host Settings** before you select **Process Citrix Optimizer**.

Multi-session Optimization

Multi-session OS machines run multiple sessions from a single machine to deliver applications and desktops to users. A disconnected session remains active and its applications continue to run. The disconnected session can consume resources needed for connected desktops and applications that run on the same machine. These settings let you optimize multi-session OS machines with disconnected sessions for better user experience with connected sessions.

Settings

Enable Multi-session Optimization. If enabled, optimizes multi-session OS machines where disconnected sessions are present. By default, this option is disabled. This option improves the user experience of connected sessions by limiting the number of resources disconnected sessions can consume. After a session stays disconnected for one minute, the WEM agent lowers the CPU and the I/O priorities of processes or applications associated with the session. The agent then imposes limits on the amount of memory resources the session can consume. If the user reconnects to the session, WEM restores the priorities and removes the limitations.

Exclude Specified Groups. Lets you specify which groups to exclude from multi-session optimization. Specify at least one group.

Exclude Specified Processes. Lets you specify which processes to exclude from multi-session optimization. Type the name of the process you want to exclude. Specify at least one process.

Policies and Profiles

These settings let you replace user GPOs and configure user profiles.

- Environmental Settings
- Microsoft USV Settings
- Citrix Profile Management Settings

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

Environmental Settings

These options modify the user's environmental settings. Some of the options are processed at logon, while some others can be refreshed in session with the agent refresh feature.

Start menu

These options modify the user's Start menu.

Process Environmental Settings. This check box toggles whether the agent processes environmental settings. If it is cleared, no environmental settings are processed.

Exclude Administrators. If enabled, environmental settings are not processed for administrators, even if the agent is launched.

User Interface: Start Menu. These settings control which Start menu functions are disabled by the agent.

IMPORTANT:

On operating systems other than Windows 7, the options under **User Interface: Start Menu** might not work, except **Hide System Clock** and **Hide Turnoff Computer**.

User Interface: Appearance. These settings allow you to customize the user's Windows theme and desktop. Paths to resources must be entered as they are accessed from the user's environment.

Desktop

User Interface: Desktop. These settings control which desktop elements are disabled by the agent.

User Interface: Edge UI. These settings allow you to disable aspects of the Windows 8.x Edge user interface.

Windows Explorer

These settings control which Windows Explorer functionalities are disabled by the agent.

User Interface: Explorer. These options allow you to disable access to **regedit** or **cmd**, and hide certain elements in Windows Explorer.

Hide Specified Drives from Explorer. If enabled, the listed drives are hidden from the user's My Computer menu. They are still accessible if browsed to directly.

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

Restrict Specified Drives from Explorer. If enabled, the listed drives are blocked. Neither the users nor their applications can access them.

Control Panel

Hide Control Panel. This option is enabled by default to secure the user environment. If disabled, the users have access to their Windows control panel.

Show only specified Control Panel Applets. If enabled, all control panel applets except the ones listed here are hidden from the user. Additional applets are added using their canonical name.

Hide specified Control Panel Applets. If enabled, only the listed control panel applets are hidden. Additional applets are added using their canonical name.

See Common Control Panel applets along with their canonical names.

Known folders management

Disable Specified Known Folders. Prevents the creation of the specified user profile known folders at profile creation.

SBC/HVD tuning

SBC/HVD (Session-Based Computing/Hosted Virtual Desktop) tuning allows you to optimize the performance of sessions running on Citrix Virtual Apps and Desktops. While designed to improve performance, some of the options might result in slight degradation of the user experience.

User Environment: Advanced Tuning. These options allow you to optimize performance in SBC/HVD environments.

Disable Drag Full Windows. Disables dragging maximized windows.

Disable SmoothScroll. Disables the smooth scrolling effect while browsing pages.

Disable Cursor Blink. Disables the cursor flickering effect.

Disable MinAnimate. Disables the animation effect when minimizing or maximizing windows.

Enable AutoEndTasks. Automatically ends the tasks after they time out.

WaitToKillApp Timeout. The timeout value (in milliseconds) for ending the applications. The default value is 20,000 milliseconds.

Set Cursor Blink Rate. Changes the cursor blink rate.

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

Set Menu Show Delay. Specifies a delay (in milliseconds) before the menu appears after logon.

Set Interactive Delay. Specifies a delay (in milliseconds) before a submenu appears.

Microsoft USV Settings

These settings allow you to optimize Microsoft User State Virtualization (USV).

Roaming profiles configuration

These settings allow you to configure Workspace Environment Management's integration with Microsoft roaming profiles.

Process User State Virtualization Configuration. Controls whether the agent processes USV settings. If disabled, no USV settings are processed.

Exclude Administrators. If enabled, USV settings you configure do not apply to administrators. When using this option, consider the following:

- Settings on the **Roaming Profiles Configuration** and **Roaming Profiles Advanced Configuration** tabs are machine-level and still apply regardless of whether the option is enabled.
- Settings on the **Folder Redirections** tabs are user-level. The option controls whether the settings apply to administrators.

Set Windows Roaming Profile Path. Lets you specify the path to your Windows profiles.

Set RDS Roaming Profiles Path. Lets you specify the path to your RDS roaming profiles.

Set RDS Home Drive Path. Lets you specify the path to your RDS home drive and the drive letter it appears with in the user environment.

Roaming profiles advanced configuration

The following are the advanced roaming profile optimization options.

Enable Folder Exclusions. If enabled, the listed folders are not included in a user's roaming profile. This allows you to exclude specific folders known to contain large amounts of data which the user does not need to have as part of their roaming profile. The list is pre-populated with default Windows 7 exclusions, and can be pre-populated with default Windows XP exclusions instead.

Delete Cached Copies of Roaming Profiles. If enabled, the agent deletes cached copies of the roaming profiles.

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

Add Administrators Security Group to Roaming User Profiles. If enabled, the Administrators group is added as owner to roaming user profiles.

Do Not Check for User Ownership of Roaming Profiles Folders. If enabled, the agent does not check to see if the user owns the roaming profiles folder before acting.

Do Not Detect Slow Network Connections. If enabled, connection speed detection is skipped.

Wait for Remote User Profile. If enabled, the agent waits for the remote user profile to be fully downloaded before processing its settings.

Profile Cleansing. Opens the **Profiles Cleanser** wizard, which allows you to delete existing profiles.

To delete existing profiles, click **Browse** to navigate to the folder where user profiles are stored, click **Scan Profiles Folder**, and then select the profile folder that you want to clean up on the Profiles Cleanser window. After that, click **Cleanse Profiles** to start the cleanup.

Cleanse Profiles. This button cleans the selected profiles per the Folder Exclusion settings.

Scan Profiles Folder. Scans the specified folder with the specified recursion settings to find user profiles, then displays all profiles found.

Profiles Root Folder. The root folder of your user profiles. You can also browse to this folder if you like.

Search Recursivity. Controls how many levels of recursion the user profile search goes through.

Folder redirection

Process Folder Redirection Configuration. This check box toggles whether the agent processes folder redirections. If it is cleared, no folder redirections are processed. Select the options to control whether and where the user's folders are redirected.

Delete Local Redirected Folders. If enabled, the agent deletes the local copies of the folders selected for redirection.

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

Citrix Profile Management Settings

NOTE:

Some options work only with specific versions of Profile Management. Consult the Profile Management documentation for details.

Workspace Environment Management™ (WEM) supports the features and operation of the current version of Citrix Profile Management. In the WEM administration console, the **Citrix Profile Management Settings** (in Policies and Profiles) supports configuring all settings for the current version of Citrix Profile Management.

In addition to using WEM to configure Citrix Profile Management features, you can use Active Directory GPOs, Citrix Studio policies, or .ini files on the VDA. We recommend that you use the same method consistently.

Main Citrix Profile Management settings

Get started with Profile Management by applying basic settings. Basic settings include processed groups, excluded groups, user store, and more.

Enable Profile Management Configuration. When enabled, you can configure and apply your settings. Enabling this option creates Profile Management related registries in the user environment. The option controls whether WEM deploys Profile Management settings you configure in the console to the agent. If disabled, none of the Profile Management settings are deployed to the agent.

Enable Profile Management. Controls whether to enable the Profile Management service on the agent machine. If disabled, the Profile Management service does not work.

You might want to disable Profile Management completely so that settings already deployed to the agent will no longer be processed. To achieve the goal, do the following:

1. Clear the **Enable Profile Management** check box and wait for the change to apply automatically or apply the change manually for immediate effect.

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

> **NOTE:**
>
> The change takes some time to take effect, depending on the value you specified for **SQL Settings Refresh Delay** in Advanced Settings. For the change to take effect immediately, refresh agent host settings and then reset Profile Management settings for all related agents. See Administration.

2. After the change takes effect, clear the **Enable Profile Management Configuration** check box.

Set processed groups. Lets you specify which groups are processed by Profile Management. Only the specified groups have their Profile Management settings processed. If left empty, all groups are processed.

Set excluded groups. Lets you specify which groups are excluded from Profile Management.

Process logons of local administrators. If enabled, local administrator logons are treated the same as non-administrator logons for Profile Management.

Set path to user store. Lets you specify the path to the user store folder.

Migrate user store. Lets you specify the path to the folder where the user settings (registry changes and synchronized files) were saved. Type the user store path that you previously used. Use this option along with the **Set path to user store** option.

Enable active write back. If enabled, profiles are written back to the user store during the user's session, preventing data loss.

- **Enable active write back registry**. If enabled, registry entries are written back to the user store during the user's session, preventing data loss.
- **Enable active write back on session lock and disconnection**. If enabled, profile files and folders are written back only when a session is locked or disconnected. If both this option and the **Enable active write back registry** option are enabled, registry entries are written back only when a session is locked or disconnected.

Enable offline profile support. If enabled, profiles are cached locally for use while not connected.

Profile container settings

These options control Profile Management profile container settings.

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

Enable Profile Container. If enabled, Profile Management maps the listed folders to the profile disk stored on the network, thus eliminating the need to save a copy of the folders to the local profile. Specify at least one folder to include in the profile container.

Enable folder exclusions. If enabled, Profile Management excludes the listed folders from the profile container. Specify at least one folder to exclude from the profile container.

Enable folder inclusions. If enabled, Profile Management keeps the listed folders in the profile container when their parent folders are excluded. Folders on this list must be subfolders of the excluded folders. This means that you must use this option in combination with the **Enable Folder Exclusions for Profile Container** option. Specify at least one folder to include in the profile container.

Enable exclusive access to profile container. If enabled, the profile container allows one access at a time.

Enable VHD auto-expansion for profile container. If enabled, when the profile container reaches 90% utilization, it automatically expands by 10 GB, with a maximum capacity of 80 GB. Depending on your needs, you can adjust the default auto-expansion settings using the following options:

- **Auto-expansion trigger threshold (%).** Lets you specify the utilization percentage of storage capacity at which the profile container triggers auto-expansion.
- **Auto-expansion increment (GB).** Lets you specify the amount of storage capacity (in GB) by which the profile container automatically expands when auto-expansion is triggered.
- **Auto-expansion limit (GB).** Lets you specify the maximum storage capacity (in GB) to which the profile container can automatically expand when auto-expansion is triggered.

Set users and groups to access profile container. Lets you specify which AD domain users and groups have Read & Execute permission on profile containers. By default, a profile container is accessible only to its owner.

Profile handling

These settings control Profile Management profile handling.

Delete local cached profiles on logoff. If enabled, locally cached profiles are deleted when the user logs off.

Set delay before deleting cached profiles. Lets you specify a delay (in seconds) before cached profiles are deleted on logoff.

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

Enable Migration of Existing Profiles. If enabled, existing Windows profiles are migrated to Profile Management on logon.

Automatic migration of existing application profiles. If enabled, existing application profiles are migrated automatically. Profile Management performs the migration when a user logs on and there are no user profiles in the user store.

Enable local profile conflict handling. Configures how Citrix Workspace™ Environment Management handles cases where Profile Management and Windows profiles conflict.

Enable template profile. If enabled, this uses a template profile at the indicated location.

Template profile overrides local profile. If enabled, the template profile overrides local profiles.

Template profile overrides roaming profile. If enabled, the template profile overrides roaming profiles.

Template profile used as Citrix mandatory profile for all logons. If enabled, the template profile overrides all other profiles.

Advanced settings

These options control advanced Profile Management settings.

Applications

Enable search index roaming for Microsoft Outlook users. If enabled, the user-specific Microsoft Outlook offline folder file (*.ost) and Microsoft search database are roamed along with the user profile. This feature improves the user experience when searching mail in Microsoft Outlook.

- **Outlook search index database – backup and restore**. If enabled, Profile Management automatically saves a backup of the last known good copy of the search index database. When there is a corruption, Profile Management reverts to that copy. As a result, you no longer must manually reindex the database when the search index database becomes corrupted.
- **Enable concurrent session support**. Provides native Outlook search experience in concurrent sessions. If enabled, each concurrent session uses a separate Outlook OST file.
    - **Maximum number of VHDX disks for storing Outlook OST files**. Lets you specify the maximum number of VHDX disks for storing Outlook OST files. If unspecified, only two VHDX disks can be used to store Outlook OST files (one file per disk). If more sessions start, their Outlook OST files are stored in the local user profile. Supported values: 1–10.

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

Enable OneDrive container. If enabled, Profile Management roams OneDrive folders with users by storing the folders on a VHDX disk. The disk is attached during logons and detached during logoffs.

Enable UWP app roaming. If enabled, UWP (Universal Windows Platform) apps roam with users. As a result, users can access the same UWP apps from different devices.

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 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.

Enable use of application definition files. Lets you enter the path to the definition files. If enabled, only the settings included in the definition file are synchronized. Specify a folder where the Citrix virtual apps optimization definition files are located. For more information about creating definition files, see Create a definition file.

VHD settings

Default capacity of VHD containers (GB). Lets you specify the default storage capacity (in GB) of each VHD container.

Customize storage path for VHDX files. Lets you specify a separate path to store VHDX files. By default, VHDX files are stored in the user store. Policies that use VHDX files include the following: Profile container, Search index roaming for Outlook, and Accelerate folder mirroring. If enabled, VHDX files of different policies are stored in different folders under the storage path.

Enable VHD disk compaction. If enabled, VHD disks are automatically compacted on user logoff when certain conditions are met. This policy enables you to save the storage space consumed by the profile container, OneDrive container, and mirror folder container. Depending on your needs and the resources available, you can adjust the default VHD compaction settings and behavior using the **Disable defragmentation for VHD disk compaction**, **Set free space ratio to trigger VHD disk compaction**, and **Set number of logoffs to trigger VHD disk compaction** options in Advanced settings.

- **Set freeable space ratio to trigger VHD disk compaction**. Applicable when Enable VHD disk compaction is enabled. Lets you specify the freeable space ratio to trigger VHD disk compaction. When the freeable space ratio exceeds the specified value on user logoff, disk compaction is triggered.

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

- Freeable 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.

- **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.
- **Set 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, the disk compaction is triggered again.

Enable exclusive access to profile container. If enabled, the profile container allows one access at a time.

Enable exclusive access to OneDrive container. If enabled, the OneDrive container allows one access at a time.

User store

Set number of retries when accessing locked files. Configures the number of times the WEM agent retries accessing locked files. Supported values: 0–100.

Replicate user stores. If enabled, Profile Management replicates a user store to multiple paths on each logoff, in addition to the path that the **Set path to user store** option specifies. To synchronize to the user stores files and folders modified during a session, enable active write-back. Enabling the option can increase system I/O and might prolong logoffs.

By default, when multiple user stores are available, Profile Management selects the store with the latest profile data. If more than one store has the latest profile, Profile Management selects the one configured earliest. With the **User store selection method** option, you can now enable Profile Management to select the store with the best access performance.

When you enable the **Replicate user stores** policy for the container-based profile solution, the **Enable in-session policy container failover among user stores** policy is automatically enabled to ensure profile redundancy for the entire session. With this policy enabled, if Profile Management loses connection to the active profile container during a session, it automatically switches to another available one. If you disable this policy, profile container failover occurs only at user logon.

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

NOTE:

Enabling this policy requires that only the profile container is enabled in your deployment. If any other containers, such as **OneDrive**, **UWP**, **Outlook**, **folder mirroring**, or **Profile streaming for pending area**, is enabled, this policy doesn't take effect.

Limit number of user stores synced at logoff By default, profiles are synchronized to all user stores during user logoff, which can extend the logoff process and delay subsequent logons. Enabling this option lets you specify how many user stores are synced during logoff. The specified number includes the main user store, while the remaining user stores (if any) are synced after logoff is complete. Supported values: 1–8.

Enable credential-based access to user store. If disabled, Profile Management impersonates the current user to access user stores. Thus, make sure that the current user can directly access the user stores. If enabled, Profile Management accesses the user stores on behalf of the user through the connections configured for relevant services in Advanced Settings > File Shares > SMB shares. (When needed, Profile Management accesses the selected SMB shares that host the user stores.) Enabling this setting lets you put user stores in file shares (for example, Azure Files) that the current user has no permission to access. When using this option, consider the following:

- To add SMB shares hosting your user stores, go to **Advanced Settings > File Shares > SMB shares**.
- SMB shares you select in **File Shares** for relevant services appear here. Profile Management accesses the selected SMB shares as needed.

IMPORTANT:

Disabling this setting deletes all user store connections that the WEM agent previously established.

- When adding or editing credentials, complete the following fields:
  - **Server share**. Enter a UNC path that specifies a server share.
  - **User name**. Enter the name in the form `domain\username`.
  - **Password**. Enter the password to be used to access the server share.
  - **Show password**. Control whether to show or hide the password.

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

Other options

Disable automatic configuration. If enabled, dynamic configuration is disabled.

Enable asynchronous processing for user Group Policy on logon. If enabled, Profile Management roams with users a registry value that Windows uses to determine the processing mode for the next user logon — synchronous or asynchronous processing mode. If the registry value does not exist, synchronous mode is applied. Enabling the option ensures that the actual processing mode is applied each time users log on. If disabled, asynchronous mode can't 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 option is enabled.

Process Internet cookie files on logoff. If enabled, stale cookies are deleted on logoff.

Alert user when profile size exceeds quota. If enabled, users receive a notification message when their profile size exceeds a quota. With this feature, you can customize the quota limit and the notification content based on the default settings. The supported quota range is 0–100,000 MB.

Set profile loading timeout. Lets you configure how long Citrix Profile Management waits for a user profile to load before switching to a temporary profile. It helps ensure a smoother, more efficient logon experience tailored to your needs. The valid timeout range is 0–1,800.

Typical use cases:

- **Non-persistent multi-session VDAs running Citrix Apps.** In such environments, loading user-specific data might not be necessary. You can set the timeout to 0 seconds to bypass profile loading and use a temporary profile.
- **Network disruption handling.** This policy mitigates network disruptions by automatically switching to a temporary profile if profile loading exceeds the timeout setting.

NOTE:

- This setting doesn't apply to the *profile migration* and *profile reset* processes.
- We recommend setting the timeout to greater than 10 seconds unless there is a strong need. A short timeout might cause users to unexpectedly log on to a temporary profile, even in normal conditions.

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

Log off user if problems occur. If enabled, users are logged off rather than switched to a temporary profile if a problem occurs.

Join the Citrix Customer Experience Improvement Program. If enabled, Profile Management uses the Customer Experience Improvement Program (CEIP) to help improve the quality and performance of Citrix products by collecting anonymous statistics and usage information. For more information on the CEIP, see About the Citrix Customer Experience Improvement Program (CEIP).

Log settings

These options control Profile Management logging.

Enable Logging. Enables/disables logging of Profile Management operations.

Configure Log Settings. Lets you specify which types of events to include in the logs.

Set Maximum Size of Log File. Lets you specify a maximum size in bytes for the log file.

Set Path to Log File. Lets you specify the location at which the log file is created.

Registry

These options control Profile Management registry settings.

NTUSER.DAT Backup. If selected, Profile Management maintains a last known good backup of the NTUSER.DAT file. If Profile Management detects corruption, it uses the last known good backup copy to recover the profile.

Enable Default Exclusion List. Default list of registry keys in the HKCU hive that are not synchronized to the user's profile. If selected, registry settings which are selected in this list are forcibly excluded from Profile Management profiles.

Enable Registry Exclusions. Registry settings in this list are forcibly excluded from Profile Management profiles.

Enable Registry Inclusions. Registry settings in this list are forcibly included in Profile Management profiles.

File system

These options control file system exclusions for Profile Management.

Enable Logon Exclusion Check. If enabled, configures what Profile Management does when a user logs on when a profile in the user store contains excluded files or folders. (If disabled, the

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

default behavior is **Synchronize excluded files or folders**). You can select one of the following behaviors in the list:

Synchronize excluded files or folders (default). Profile Management synchronizes these excluded files or folders from the user store to local profile when a user logs on.

Ignore excluded files or folders. Profile Management ignores the excluded files or folders in the user store when a user logs on.

Delete excluded files or folder. Profile Management deletes the excluded files or folders in the user store when a user logs on.

Enable Default Exclusion List - Directories. Default list of directories ignored during synchronization. If selected, folders which are selected in this list are excluded from the Profile Management synchronization.

Enable File Exclusions. If enabled, the listed files are not included in a user's Profile Management profile. This allows you to exclude specific folders known to contain large amounts of data which the user does not need to have as part of their Profile Management profile. The list is pre-populated with default Windows 7 exclusions, and can be pre-populated with default Windows XP exclusions instead.

Enable Folder Exclusions. If enabled, the listed folders are not included in a user's Profile Management profile. This allows you to exclude specific folders known to contain large amounts of data which the user does not need to have as part of their Profile Management profile. The list is pre-populated with default Windows 7 exclusions, and can be pre-populated with default Windows XP exclusions instead.

Profile Cleansing. Opens the **Profiles Cleanser** wizard, which allows you to delete existing profiles.

To delete existing profiles, click **Browse** to navigate to the folder where user profiles are stored, click **Scan Profiles Folder**, and then select the profile folder that you want to clean up in the **Profiles Cleanser** window. After that, click **Cleanse Profiles** to start the cleanup.

Cleanse Profiles. Cleans the selected profiles per the folder exclusion settings.

Scan Profiles Folder. Scans the specified folder with the specified recursion settings to find user profiles and then displays all profiles found.

Profiles Root Folder. The root folder of your user profiles. You can also browse to this folder if you like.

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

Search Recursivity. Controls how many levels of recursion the user profile search goes through.

Synchronization

These options control Profile Management synchronization settings.

Enable Directory Synchronization. If enabled, the listed folders are synchronized to the user store.

Enable File Synchronization. If enabled, the listed files are synchronized to the user store, ensuring that users always get the most up-to-date versions of the files. If files have been modified in more than one session, the most up-to-date files are kept in the user store.

Enable Folder Mirroring. If enabled, the listed folders are mirrored to the user store on logoff, ensuring that files and subfolders in mirrored folders stored in the user store are the same as the local versions. See below for more information about how folder mirroring works.

- Files in mirrored folders will always overwrite files stored in the user store on session logoff, irrespective of whether they are modified.
- If extra files or subfolders are present in the user store compared to the local versions in mirrored folders, those extra files and subfolders are deleted from the user store on session logoff.

Enable Large File Handling. If enabled, large files are redirected to the user store, thereby eliminating the need to synchronize those files over the network.

NOTE:

Some applications do not allow concurrent file access. Citrix recommends that you take application behavior into consideration when you define your large file handling policy.

Streamed user profiles

These options control streamed user profile settings.

Enable Profile Streaming. If disabled, none of the settings in this section are processed.

Enable Profile Streaming for Folders. If enabled, folders are fetched only when they are being accessed. This setting eliminates the need to traverse all folders during user logons, thus saving bandwidth and reducing the time to synchronize files.

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

Enable Profile Streaming for Pending Area. If enabled, files in the pending area are fetched to the local profile only when they are requested. This ensures optimum logon experience in concurrent session scenarios. 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 option is disabled. All files and folders in the pending area are fetched to the local profile during logon.

Always Cache. If enabled, files of the specified size (in MB) or larger will always be cached.

Set timeout for pending area lock files: Frees up files so they are written back to the user store from the pending area after the specified time if the user store remains locked when a server becomes unresponsive.

Set streamed user profile groups. This list determines which user groups streamed profiles are used for.

Enable Profile Streaming Exclusion List - Directories. If selected, Profile Management does not stream folders in this list, and all the folders are fetched immediately from the user store to the local computer when users log on.

File deduplication

These options control Profile Management file deduplication settings.

Identical files can exist among various user profiles. Separating those files from the user store and storing them in a central location saves storage space by avoiding duplicates. You can specify files that you want to include in the shared store on the server hosting the user store. Specify the file names with paths relative to the user profile.

Enable File Inclusions. If enabled, Profile Management generates the shared store automatically. It then centrally stores the specified files in the shared store rather than in each user profile in the user store. Doing so reduces the load on the user store by avoiding file duplication, thus reducing your storage cost.

Enable File Exclusions. If enabled, Profile Management excludes the specified files from the shared store. You must use this option along with the **Enable File Inclusions** option. Specify at least one file to exclude from the shared store.

Cross-platform settings

These options control cross-platform settings.

Enable cross-platform settings. If disabled, none of the settings in this section are processed.

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

Set cross-platform settings groups. Lets you specify the user groups for which cross-platform profiles are used.

Set path to cross-platform definitions. Lets you specify the path to your cross-platform definition files.

Set path to cross-platform setting store. Lets you specify the path to your cross-platform setting store.

Enable source for creating cross-platform settings. Enables a source platform for cross-platform settings.

App access control

This feature lets you add rules to control end user access to applications or to enforce machine-level redirections for files, folders, and registry values and keys.

There are two ways that you can create rules:

- GUI-based tool - Citrix Environment Tool Hub > Rule Generator for App Access Control
- PowerShell tool – available with the Profile Management installation package

Folder redirection

This feature lets you configure rule sets to redirect the paths of local folders to new locations. Each rule set specifies where you want to redirect the folders based on the users accessing them. A rule set mainly includes:

- **Redirection rules.** Specify which local folders you want to redirect and where to redirect them (such as a network location).
- **Assignments.** Specify the users to whom you assign the redirection rules.

To add a rule set for a configuration set, follow these steps:

1. Go to the **Profile Management Settings** page of the target configuration set.
2. Click the **Folder redirection** link above the search box.
3. On the **Folder redirection** page that appears, click **Add rule set**.
4. On the **Add rule set** page that appears, follow these steps to complete the settings:

    a. On the **Redirection rules** page, select the folders to redirect, specify the redirection destinations, and then click **Next**.

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

- You can redirect a folder to a network location, the user's home directory (only for certain folders), or the local user profile location.
- By default, the **Move contents to new location** option is selected, identifying that after you set or modify a redirection target path, contents from the previous path are automatically moved to the new one. To prevent this behavior, clear the option.

b. On the **Assignments** page, select users, groups, or OUs to which you want to assign the redirection rules, and then click **Next**. Default groups include **Everyone** and **Administrators**. To add a group, click **Add new target**.

c. On the **Additional settings** page, specify the following settings for the rule set, and then click **Next**:

- **Grant access to administrators:** Whether to grant the **local Administrators** group access to the redirection target paths. By default, those paths are accessible exclusively to the profile owner.
- **Grant access to specific users and groups:** Whether to grant specific users and groups access to the redirection target paths. After selecting this option, click Add user/group to specify the users and groups as needed.
- **Include domain name:** Whether to include the %userdomain% environment variable as part of the UNC path.
- Set a priority for this rule set by entering a numeric value. Greater numbers indicate higher priority. When multiple rule sets apply to the same target, the one with the higher priority wins.

d. Enter a descriptive name for this rule set and review settings. To adjust, click the corresponding step in the left pane.

e. Click **Done**.

NOTE:

Currently, end users must log on twice for newly deployed rule sets to take effect.

Security

These settings let you control user activities within Workspace Environment Management.

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

Application security

IMPORTANT:

To control which applications users can run, use the Windows AppLocker interface or Workspace Environment Management. You can switch between these approaches at any time but we recommend that you do not use both approaches at the same time.

These settings let you control the applications users are permitted to run by defining rules. This functionality is similar to Windows AppLocker.

When you use Workspace Environment Management to manage Windows AppLocker rules, the agent processes (converts) Application Security tab rules into Windows AppLocker rules on the agent host. If you stop the agent processing rules, they are preserved in the configuration set and AppLocker continues running by using the last set of instructions processed by the agent.

Application security

This tab lists the application security rules in the current Workspace Environment Management configuration set. You can use **Find** to filter the list according to a text string.

When you select the top-level item "Application Security" in the **Security** tab, the following options become available to enable or disable rule processing:

- **Process Application Security Rules**. When selected, the **Application Security** tab controls are enabled and the agent processes rules in the current configuration set, converting them into AppLocker rules on the agent host. When not selected, the **Application Security** tab controls are disabled and the agent does not process rules into AppLocker rules. (In this case AppLocker rules are not updated.)

  NOTE:

  This option is not available if the Workspace Environment Management administration console is installed on Windows 7 SP1 or Windows Server 2008 R2 SP1 (or earlier versions).

- **Process DLL Rules**. When selected, the agent processes DLL rules in the current configuration set into AppLocker DLL rules on the agent host. This option is only available when you select **Process Application Security Rules**.

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

IMPORTANT:

If you use DLL rules, you must create a DLL rule with "Allow" permission for each DLL that is used by all the allowed apps.

Caution:

If you use DLL rules, users may experience a reduction in performance. This happens because AppLocker checks each DLL that an app loads before it is allowed to run.

- The **Overwrite** and **Merge** settings let you determine how the agent processes application security rules.
  - **Overwrite**. Lets you overwrite existing rules. When selected, the rules that are processed last overwrite rules that were processed earlier. We recommend that you apply this mode only to single-session machines.
  - **Merge**. Lets you merge rules with existing rules. When conflicts occur, the rules that are processed last overwrite rules that were processed earlier. If you need to modify the rule enforcement setting during merging, use overwrite mode because merge mode will keep the old value if it differs.

Rule collections

Rules belong to AppLocker rule collections. Each collection name indicates how many rules it contains, for example (12). Click a collection name to filter the rule list to one of the following collections:

- **Executable Rules**. Rules which include files with the .exe and .com extensions that are associated with an application.
- **Windows Rules**. Rules which include installer file formats (.msi, .msp, .mst) which control the installation of files on client computers and servers.
- **Script Rules**. Rules which include files of the following formats: .ps1, .bat, .cmd, .vbs, .js.
- **Packaged Rules**. Rules which include packaged apps, also known as Universal Windows apps. In packaged apps, all files within the app package share the same identity. Therefore, one rule can control the entire app. Workspace Environment Management supports only publisher rules for packaged apps.
- **DLL Rules**. Rules which include files of the following formats: .dll, .ocx.

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

When you filter the rule list to a collection, the **Rule enforcement** option is available to control how AppLocker enforces all rules in that collection on the agent host. The following rule enforcement values are possible:

Off (default). Rules are created and set to "off," which means they are not applied.

On. Rules are created and set to "enforce," which means they are active on the agent host.

Audit. Rules are created and set to "audit," which means they are on the agent host in an inactive state. When a user runs an app that violates an AppLocker rule, the app is allowed to run and the information about the app is added to the AppLocker event log.

To import AppLocker rules

You can import rules exported from AppLocker into Workspace Environment Management. Imported Windows AppLocker settings are added to any existing rules in the **Security** tab. Any invalid application security rules are automatically deleted and listed in a report dialog.

1. In the ribbon, click **Import AppLocker Rules**.
2. Browse to the XML file exported from AppLocker containing your AppLocker rules.
3. Click **Import**.

The rules are added to the Application Security rules list.

To add a rule

1. Select a rule collection name in the sidebar. For example, to add an executable rule select the "Executable Rules" collection.
2. Click **Add Rule**.
3. In the **Display** section, type the following details:
    - **Name**. The display name of the rule as it appears in the rule list.
    - **Description**. Additional information about the resource (optional).
4. In the **Type** section, click an option:
    - **Path**. The rule matches a file path or folder path.
    - **Publisher**. The rule matches a selected publisher.
    - **Hash**. The rule matches a specific hash code.

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

5. In the **Permissions** section, click whether this rule will **Allow** or **Deny** applications from running.
6. To assign this rule to users or user groups, in the **Assignments** pane, choose users or groups to assign this rule to. The "Assigned" column shows a "check" icon for assigned users or groups.

   TIP:

   - You can use the usual Windows selection modifier keys to make multiple selections, or use **Select All** to select all rows.
   - Users must already be in the Workspace Environment Management Users list.
   - You can assign rules after the rule is created.

7. Click **Next**.
8. Specify the criteria that the rule matches, depending on the rule type you choose:

   - **Path**. Specify a file path or folder path that you want the rule to match. When you choose a folder, the rule matches all files inside and below that folder.
   - **Publisher**. Specify a signed reference file that you want to use as a reference for the rule, and then use the Publisher Info slider to tune the level of property matching.
   - **Hash**. Specify a file or folder from which you want to create a hash. The rule matches the hash code of the file.

9. Click **Next**.
10. Add any exceptions you require (optional). In Add exception, choose an exception type then click **Add**. (You can **Edit** and **Remove** exceptions as required.)
11. To save the rule, click **Create**.

To assign rules to users

Select one or more rules in the list, then click **Edit** in the toolbar or context menu. In the editor, select the rows containing the users and user groups you want to assign the rule to, then click **OK**. You can also unassign the selected rules from everyone using **Select All** to clear all selections.

Note: If you select multiple rules and click **Edit**, any rule assignment changes for those rules are applied to all users and user groups you select. In other words, existing rule assignments are merged across those rules.

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

To add default rules

Click **Add Default Rules**. A set of AppLocker default rules is added to the list.

To edit rules

Select one or more rules in the list, then click **Edit** in the toolbar or context menu. The editor appears allowing you to adjust settings which apply to the selection you made.

To delete rules

Select one or more rules in the list, then click **Delete** in the toolbar or context menu.

To back up application security rules

You can back up all application security rules in your current configuration set. Rules are all exported as a single XML file. You can use **Restore** to restore the rules to any configuration set. In the ribbon, click **Backup** then select **Security Settings**.

To restore application security rules

You can restore application security rules from XML files created by the Workspace Environment Management backup command. The restore process replaces the rules in the current configuration set with those rules in the backup. When you switch to or refresh the **Security** tab, any invalid application security rules are detected. Invalid rules are automatically deleted and listed in a report dialog, which you can export.

During the restore process, you can choose whether you want to restore rule assignments to users and user groups in your current configuration set. Reassignment only succeeds if the backed-up users/groups are present in your current configuration set/active directory. Any mismatched rules are restored but remain unassigned. After restore, they are listed in a report dialog which you can export in CSV format.

1\. In the ribbon, click **Restore** to start the restore wizard.

2\. Select Security settings, then click **Next** twice.

3\. In **Restore from folder**, browse to the folder containing the backup file.

4\. Select **AppLocker Rule Settings**, then click **Next**.

5\. Confirm whether you want to restore rule assignments or not:

Yes. Restore rules and reassign them to the same users and user groups in your current configuration set.

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

No. Restore rules and leave them unassigned.

6\. To start restoring, click **Restore Settings**.

Process management

These settings allow you to add specific processes to the allow list or block list.

Process management

Enable Process Management. Toggles whether process on the allow list or block list are in effect. If disabled, none of the settings on the **Process BlackList** and **Process WhiteList** tabs are taken into account.

> **NOTE:**
>
> This option only works if the session agent is running in the user's session. To do this use the **Main Configuration** Agent settings to set the **Launch Agent** options (**at Logon/at Reconnect/for Admins**) to launch according to the user/session type, and set **Agent Type** to "UI". These options are described in Advanced Settings.

Process block list

These settings let you add specific processes to the block list.

Enable Process Blacklist. Enable processing of processes on the block list. You must add processes by using their executable name (for example, cmd.exe).

Exclude Local Administrators. Excludes local administrator accounts.

Exclude Specified Groups. Lets you exclude specific user groups.

Process allow list

These settings let you add specific processes to the allow list. Process block lists and process allow lists are mutually exclusive.

Enable Process Whitelist. Enable processing of processes on the allow list. You must add processes by using their executable name (for example, cmd.exe). **Note** If enabled, **Enable Process Whitelist** automatically adds all processes not in the allow list to the block list.

Exclude Local Administrators. Excludes local administrator accounts (they are able to run all processes).

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

Exclude Specified Groups. Lets you exclude specific user groups (they are able to run all processes).

Privilege elevation

> **NOTE:**
>
> This feature does not apply to Citrix virtual apps.

The privilege elevation feature lets you elevate the privileges of non-administrative users to an administrator level necessary for some executables. As a result, the users can start those executables as if they are members of the administrators group.

Privilege elevation

When you select the **Privilege Elevation** pane in **Security**, the following options appear:

- **Process Privilege Elevation Settings**. Controls whether to enable the privilege elevation feature. When selected, enables agents to process privilege elevation settings and other options on the **Privilege Elevation** tab become available.
- **Do Not Apply to Windows Server OSs**. Controls whether to apply privilege elevation settings to Windows Server operating systems. If selected, rules assigned to users do not work on Windows Server machines. By default, this option is selected.
- **Enforce RunAsInvoker**. Controls whether to force all executables to run under the current Windows account. If selected, users are not prompted to run executables as administrators.

This tab also displays the complete list of rules that you have configured. Click **Executable Rules** or **Windows Installer Rules** to filter the rule list to a specific rule type. You can use **Find** to filter the list. The **Assigned** column displays a check mark icon for assigned users or user groups.

Supported rules

You can apply privilege elevation using two types of rules: executable rules and Windows installer rules.

- **Executable Rules**. Rules that include files with .exe and .com extensions associated with an application.
- **Windows Installer Rules**. Rules that include installer files with.msi and .msp extensions associated with an application. When you add Windows installer rules, keep the following scenario in mind:

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

- Privilege elevation applies only to Microsoft's msiexec.exe. Make sure that the tool you use to deploy `.msi` and `.msp` Windows installer files is msiexec.exe.
- Suppose that a process matches a specified Windows installer rule and its parent process matches a specified executable rule. The process cannot get elevated privileges unless the **Apply to Child Processes** setting is enabled in the specified executable rule.

After you click the **Executable Rules** or the **Windows Installer Rules** tab, the **Actions** section displays the following actions available to you:

- **Edit**. Lets you edit an existing executable rule.
- **Delete**. Lets you delete an existing executable rule.
- **Add Rule**. Lets you add an executable rule.

To add a rule

1. Navigate to **Executable Rules** or **Windows Installer Rules** and click **Add Rule**. The **Add Rule** window appears.
2. In the **Display** section, type the following:
   - **Name**. Type the display name of the rule. The name appears in the rule list.
   - **Description**. Type additional information about the rule.
3. In the **Type** section, select an option.
   - **Path**. The rule matches a file path.
   - **Publisher**. The rule matches a selected publisher.
   - **Hash**. The rule matches a specific hash code.
4. In the **Settings** section, configure the following if needed:
   - **Apply to Child Processes**. If selected, applies the rule to all child processes that the executable starts. To manage privilege elevation at a more granular level, use the following options:
     - **Apply only to executables in the same folder**. If selected, applies the rule only to executables that share the same folder.
     - **Apply only to signed executables**. If selected, applies the rule only to executables that are signed.

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

- **Apply only to executables of the same publisher**. If selected, applies the rule only to executables that share the same publisher information. This setting does not work with Universal Windows Platform (UWP) apps.

> **NOTE:**
>
> When you add Windows install rules, the **Apply to Child Processes** setting is enabled by default and you cannot edit it.

- **Start Time**. Lets you specify a time for agents to start applying the rule. The time format is HH:MM. The time is based on the agent time zone.
- **End Time**. Lets you specify a time for agents to stop applying the rule. The time format is HH:MM. From the specified time onward, agents no longer apply the rule. The time is based on the agent time zone.
- **Add Parameter**. Lets you restrict privilege elevation to executables that match the specified parameter. The parameter works as a match criterion. Make sure that the parameter you specify is correct. For an example of how to use this feature, see Executables running with parameters. If this field is empty or contains only blank spaces, the agent applies privilege elevation to relevant executables whether or not they run with parameters.
- **Enable Regular Expressions**. Lets you control whether to use regular expressions to further expand the criterion.

5. In the **Assignments** section, select users or user groups to which you want to assign the rule. If you want to assign the rule to all users and user groups, select **Select All**.

> **TIP:**
>
> - You can use the usual Windows selection modifier keys to make multiple selections.
> - Users or user groups must already be in the list displayed on the **Administration > Users** tab.
> - You can choose to assign the rule later (after the rule is created).

6. Click **Next**.
7. Do either of the following. Different actions are needed depending on the rule type you selected in the preceding page.

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

IMPORTANT:

WEM provides you with a tool named **AppInfoViewer** to obtain the following information and more from executable files: publisher, path, and hash. The tool can be useful if you want to provide relevant information for applications to be configured in the management console. For example, you can use the tool to extract relevant information from applications when using the application security feature. The tool is located in the agent installation folder.

- **Path**. Type the path to the file or folder to which you want to apply the rule. The WEM agent applies the rule to an executable according to the executable file path.
- **Publisher.** Fill out the following fields: **Publisher**, **Product name**, **File name**, and **File version**. You cannot leave any of the fields empty, but you can type an asterisk (*) instead. The WEM agent applies the rule according to publisher information. If applied, users can run executables that share the same publisher information.
- **Hash**. Click **Add** to add a hash. In the **Add Hash** window, type the file name and the hash value. You can use the **AppInfoViewer** tool to create a hash from a selected file or folder. The WEM agent applies the rule to identical executables as specified. As a result, users can run executables that are identical to the specified one.

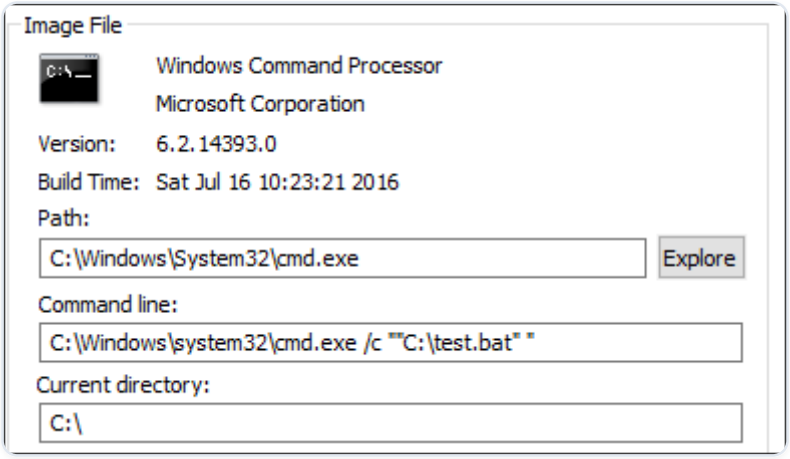
8. Click **Create** to save the rule and to exit the window.

Executables running with parameters

You can restrict privilege elevation to executables that match the specified parameter. The parameter works as a match criterion. To see parameters available to an executable, use tools such as Process Explorer or Process Monitor. Apply the parameters that appear in those tools.

Suppose you want to apply the rule to an executable (for example, cmd.exe) according to the executable file path. You want to apply privilege elevation only to `test.bat`. You can use Process Explorer to get the parameters.

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



In the **Add Parameter** field, you can type the following:

- `/c ""C:\test.bat""`

You then type the following in the **Path** field:

- `C:\Windows\System32\cmd.exe`

In this case, you elevate the privilege of the specified users to an administrator level only for `test.bat`.

To assign rules to users

Select one or more rules in the list and then click **Edit** in the **Actions** section. In the **Edit Rule** window, select users or user groups to which you want to assign the rule and then click **OK**.

To delete rules

Select one or more rules in the list and then click **Delete** in the **Actions** section.

To back up privilege elevation rules

You can back up all privilege elevation rules in your current configuration set. All rules are exported as a single XML file. You can use **Restore** to restore the rules to any configuration set.

To complete the backup, use the **Backup** wizard, available in the ribbon. For more information about using the **Backup** wizard, see Ribbon.

To restore privilege elevation rules

You can restore privilege elevation rules from XML files exported through the Workspace Environment Management Backup wizard. The restore process replaces the rules in the current configuration set with those rules in the backup. When you switch to or refresh the **Security > Privilege Elevation** pane, any invalid privilege elevation rules are detected. Invalid rules are automatically deleted and listed in a report that you can export. For more information about using the **Restore** wizard, see Ribbon.

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

Self-elevation

With self-elevation, you can automate privilege elevation for certain users without the need to provide the exact executables beforehand. Those users can request self-elevation for any applicable file simply by right-clicking the file and then selecting **Run with administrator privileges** in the context menu. After that, a prompt appears, requesting that they provide a reason for the elevation. The WEM agent does not validate the reason. The reason for the elevation is saved to the database for auditing purposes. If the criteria are met, the elevation is applied, and the files run successfully with administrator privileges.

The feature also gives you flexibility to choose the best solution for your needs. You can create allow lists for files you permit users to self-elevate or block lists for files you want to prevent users from self-elevating.

Self-elevation applies to files of the following formats: `.exe`, `.msi`, `.bat`, `.cmd`, `.ps1`, and `.vbs`.

NOTE:

By default, certain applications are used to run some files. For example, cmd.exe is used to run .cmd files and powershell.exe is used to run .ps1 files. In those scenarios, you cannot change the default behavior.

When you select **Security > Self-elevation**, the following options appear:

- **Enable self-elevation**. Controls whether to enable the self-elevation feature. Select the option to:
  - Enable agents to process self-elevation settings.
  - Make other options on the **Self-elevation** tab available.
  - Make the **Run with administrator privileges** option available in the context menu when users right-click a file. As a result, users can request self-elevation for files that match the conditions you specify on the **Self-elevation** tab.
- **Permissions**. Lets you create allow lists for files you permit users to self-elevate or block lists for files you want to prevent users from self-elevating.
  - **Allow**. Creates allow lists for files you permit users to self-elevate.
  - **Deny**. Creates block lists for files you want to prevent users from self-elevating.
- You can perform the following operations:

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

  - **Edit**. Lets you edit an existing condition.
  - **Delete**. Lets you delete an existing condition.
  - **Add**. Lets you add a condition. You can create a condition based on a path, a selected publisher, or a specific hash code.

- **Settings**. Lets you configure additional settings that control how agents apply self-elevation.
  - **Apply to Child Processes**. If selected, applies self-elevation conditions to all child processes that the file starts.
  - **Start Time**. Lets you specify a time for agents to start applying conditions for self-elevation. The time format is HH:MM. The time is based on the agent time zone.
  - **End Time**. Lets you specify a time for agents to stop applying conditions for self-elevation. The time format is HH:MM. From the specified time onward, agents no longer apply the conditions. The time is based on the agent time zone.
- **Assignments**. Lets you assign the self-elevation condition to applicable users or user groups. To assign the condition to all users and user groups, click **Select All** or select **Everyone**. The **Select All** check box is useful in scenarios where you want to clear your selection and reselect users and user groups.

Process hierarchy control

The process hierarchy control feature controls whether certain child processes can be started from their parent processes in parent-child scenarios. You create a rule by defining parent processes and then designating an allow list or a block list for their child processes. Review this entire section before using the feature.

NOTE:

- This feature applies only to Citrix virtual apps.

To understand how the rule works, keep the following in mind:

- A process is subject to only one rule. If you define multiple rules for the same process, only the rule with the highest priority is enforced.
- The rule you defined is not restricted only to the original parent-child hierarchy but also applies to each level of that hierarchy. Rules applicable to a parent process prevail over rules

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

applicable to its child processes regardless of the priority of the rules. For example, you define the following two rules:

- Rule 1: Word cannot open CMD.
- Rule 2: Notepad can open CMD.

With the two rules, you cannot open CMD from Notepad by first opening Word and then opening Notepad from Word regardless of the priority of the rules.

This feature relies on certain process-based parent-child relationships to work. To visualize the parent-child relationships in a scenario, use the process tree feature of the Process Explorer tool. For more information about Process Explorer, see `<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>`.

To avoid any potential issues, we recommend that you add an executable file path that points to **VUEMAppCmd.exe** in Citrix Studio. **VUEMAppCmd.exe** ensures that the WEM agent finishes processing settings before published applications start. In Citrix Studio, complete the following steps:

1. In **Application**, select the application, click **Properties** in the action pane, and then go to the **Location** page.
2. Type the path of the local application on the end-user operating system.
   - Under the **Path to the executable file** field, type the following: <%ProgramFiles%>\Citrix\Workspace Environment Management Agent\VUEMAppCmd.exe.
3. Type the command-line argument to specify an application to open.
   - Under the **Command-line argument** field, type the full path to the application that you want to launch through **VUEMAppCmd.exe**. Make sure that you wrap the command line for the application in double quotes if the path contains blank spaces.
   - For example, suppose you want to launch iexplore.exe through **VUEMAppCmd.exe**. You can do so by typing the following: `%ProgramFiles(x86)%\"Internet Explorer"\iexplore.exe`.

Considerations

For the feature to work, you need to use the **AppInfoViewer** tool on each agent machine to enable the feature. (The tool is located in the agent installation folder.) Every time you use the tool to

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

enable or disable the feature, a machine restart is required. With the feature enabled, you must restart the agent machine after upgrading or uninstalling the agent.

To verify that the process hierarchy control feature is enabled, open the **Registry Editor** on the agent machine. The feature is enabled if the following registry entry exists:

- 32-bit OS
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\WEM Hook`
- 64-bit OS
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\WEM Hook`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_Dlls\WEM Hook`

Prerequisites

To use the feature, make sure that the following prerequisites are met:

- A Citrix virtual apps deployment.
- The agent is running on Windows 10 or Windows Server.
- The agent host has been restarted after in-place upgrade or fresh install.

Process hierarchy control

When you select **Process Hierarchy Control** in **Security**, the following options appear:

- **Enable Process Hierarchy Control**. Controls whether to enable the process hierarchy control feature. When selected, other options on the **Process Hierarchy Control** tab become available and configured settings there can take effect. You can use this feature *only* in a Citrix virtual apps deployment.
- **Hide Open With from Context Menu**. Controls whether to show or hide the **Open With** option from the Windows right-click context menu. When enabled, the menu option is hidden from the interface. When disabled, the option is visible and users can use it to start a process. The process hierarchy control feature does not apply to processes started through the **Open With** option. We recommend that you enable this setting to prevent applications from starting processes through system services that are unrelated to the current application hierarchy.

The **Process Hierarchy Control** tab also displays the complete list of rules that you have configured. You can use **Find** to filter the list. The **Assigned** column displays a check mark icon for assigned users or user groups.

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

The **Actions** section displays the following actions:

- **Edit**. Lets you edit a rule.
- **Delete**. Lets you delete a rule.
- **Add Rule**. Lets you add a rule.

To add a rule

1. Navigate to **Process Hierarchy Control** and click **Add Rule**. The **Add Rule** window appears.
2. In the **Display** section, type the following:
    - **Name**. Type the display name of the rule. The name appears in the rule list.
    - **Description**. Type additional information about the rule.
3. In the **Type** section, select an option.
    - **Path**. The rule matches a file path.
    - **Publisher**. The rule matches a selected publisher.
    - **Hash**. The rule matches a specific hash code.
4. In the **Mode** section, select either of the following options:
    - **Add Child Processes to Block List**. If selected, lets you define a block list for applicable child processes after configuring a rule for their parent processes. A block list prohibits only the processes you specified from running and other processes are allowed to run.
    - **Add Child Processes to Allow List**. If selected, lets you define an allow list for applicable child processes after configuring a rule for their parent processes. An allow list allows only the processes you specified to run and other processes are prohibited from running.

    NOTE:

    A process is subject to only one rule. If you define multiple rules for the same process, the rules are enforced in order of priority.

5. In the **Priority** section, set the priority for the rule. When configuring the priority, consider the following: The priority determines the order in which the rules you configured are processed. The greater the value, the higher the priority. Type an integer. If there is a conflict, the rule with the higher priority prevails.

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

6. In the **Assignments** section, select users or user groups to which you want to assign the rule. If you want to assign the rule to all users and user groups, select **Select All**.

   NOTE:

   - You can use the usual Windows selection keys to make multiple selections.
   - Users or user groups must already be in the list displayed on the **Administration > Users** tab.
   - You can choose to assign the rule later (after the rule is created).

7. Click **Next**.
8. Do either of the following to configure the rule for parent processes. Different actions are needed depending on the rule type you selected on the previous page.

   - **Path**. Specify a file path or folder path that you want the rule to match. If you specify a folder path, the rule applies to all files and subfolders in that folder. The WEM agent applies the rule to an executable according to the executable file path. We do not recommend that you type only asterisk (*) to indicate a path match. Doing that might cause unintended performance issues.
   - **Publisher**. Specify a signed reference file that you want to use as a reference for the rule. Use the Publisher Info slider to tune the level of property matching. Move the slider up or down to make the rule less or more specific. If you move the slider to the Any publisher position, the rule applies to all signed files. The WEM agent applies the rule to parent processes according to publisher information. If applied, users can run executables that share the same publisher information. If necessary, you can select **Use custom values** to customize information.
   - **Hash**. Specify a file or folder from which you want to create a hash. The rule matches the hash code of the file. The WEM agent applies the rule to identical executables as specified. As a result, users can run executables that are identical to the specified one.

9. Click **Next** to configure child process settings.
10. Do either of the following to define an allow list or a block list for applicable child processes.

    a. Select a rule type from the menu and then click **Add**. The **Child Process** window appears.

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

b. In the **Child Process** window, configure settings as needed. The user interface of the **Child Process** window is different depending on the rule type you selected. For a child process, the following rule types are available: **Path**, **Publisher**, and **Hash**.

c. Click **OK** to return to the **Add Rule** window. You can add more child processes or click **Create** to save the rule and to exit the window.

To assign rules to users

Select one rule in the list and then click **Edit** in the **Actions** section. In the **Edit Rule** window, select users or user groups to which you want to assign the rule and then click **OK**.

To delete rules

Select one or more rules in the list and then click **Delete** in the **Actions** section.

To back up rules

You can back up all process hierarchy control rules in your current configuration set. All rules are exported as a single XML file. You can use **Restore** to restore the rules to any configuration set.

To complete the backup, use the **Backup** wizard, available in the ribbon. For more information about using the **Backup** wizard, see Ribbon.

To restore rules

You can restore process hierarchy control rules from XML files exported through the Workspace Environment Management Backup wizard. The restore process replaces the rules in the current configuration set with those rules in the backup. When you switch to or refresh the **Security > Process Hierarchy Control** pane, any invalid rules are deleted and listed in a report that you can export. For more information about using the **Restore** wizard, see Ribbon.

Active Directory Objects

Use these pages to specify the users, computers, groups, and organizational units you want Workspace Environment Management™ (WEM) to manage.

NOTE:

Add users, computers, groups, and OUs to WEM so that the agent can manage them.

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

Users

A list of your existing users and groups. You can use **Find** to filter the list by name or ID against a text string.

To add a user

1. Select **Add** from the context menu.
2. Enter a user or group name in the Windows Select Users dialog, then click **OK**.

Name. The name of the user or group.

Description. Only shown in the **Edit Item** dialog. Lets you specify additional information about the user or group.

Item Priority. Lets you configure priority between different groups and user accounts. The priority determines the order in which the actions that you assign are processed. Type an integer to specify a priority. The greater the value, the higher the priority. If there is a conflict (for example, when mapping different network drives with the same drive letter), the group or user account with the higher priority prevails.

IMPORTANT:

When assigning Group Policy settings, the priority you configure here does not work. To set the priority for them, use **Administration console > Assignments**. For more information, see Contextualize Group Policy settings.

Item State. Lets you choose whether a user or group is enabled or disabled. If disabled, you cannot assign actions to it.

To add multiple users

1. Select **Add** from the context menu.
2. Add multiple users or group names in the textbox, separate them with semicolons, and then click **OK**.

Machines

A list of computers which have been added to the current site (configuration set). Only computers listed here are managed by Workspace Environment Management. When agents on these computers register with the infrastructure server it sends them the necessary machine-dependent

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

settings for the configuration set. You can use **Find** to filter the list by name or ID against a text string.

TIP:

To check whether agents on these machines are correctly registered with the infrastructure server, see Agents in the Administration section.

To add a computer or computer group to the current configuration set

1. Use the **Add Object** context menu command or button.
2. In the Select Computers or Groups dialog, select a computer or computer group, then click **OK**.

To add computers in an organizational unit to the configuration set

1. Use the **Add OU** context menu command or button.
2. In the Organizational Units dialog, select an organizational unit, then click **OK**.

To edit computer, computer group, or OU details

1. Select an item in the list.
2. Use the **Edit** context menu command or button.
3. In the Edit item dialog, any of the following details (which are not read-only), then click **OK**.

Name*. The computer, computer group, or OU name.

Distinguished Name*. The distinguished name (DN) of the selected computer or computer group. This field allows you to differentiate different OUs if they have the same Name.

Description. Additional information about the computer, computer group, or OU.

Type*. The selected type (Computer, Group, or Organizational Unit)

Item State. The state of the computer, computer group, or OU (enabled or disabled). If disabled, the computer, computer group, or OU is not available to assign actions to.

Item Priority. This allows you to configure priority between different groups and user accounts. The priority determines the order in which the actions you assign are processed. The greater the value, the higher the priority. Type an integer. If there is a conflict (for example, when mapping different network drives with the same drive letter), the group or user account with the higher priority prevails.

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

* Read-only details reported from Active Directory.

Advanced

Active Directory search timeout

Configure Active Directory behavior.

- **Active Directory search timeout**. Specify the timeout, in milliseconds, after which Active Directory searches end. The default value is 1000. We recommend using a value equal to or greater than 500 to avoid timeouts before searches complete.

Unbound agent site settings

Control whether to apply settings to unbound agents. Unbound agents are those agents that are not bound to any configuration set.

The following setting applies to your entire WEM deployment. It is not associated with any configuration sets (sites). After you enable the setting, go to the "Unbound Agents" configuration set and then configure settings there so that you can control how unbound agents behave.

- **Apply settings to unbound agents**. Lets you apply the settings of the "Unbound Agents" configuration set to agents that you have not yet added in **Active Directory Objects**.

Enforce LDAPS to encrypt Active Directory connections

By default, WEM uses *LDAP* for Active Directory queries. To enforce secure communication over *LDAPS*, select **Enable LDAPS to encrypt Active Directory connections**.

Transformer settings

These options let you configure the Transformer feature. Transformer lets agents connect as web or application launchers that redirect users to the configured remote desktop interface. Use Transformer to convert any Windows PC into a high performance thin client using a fully reversible "kiosk" mode.

General

General settings

These settings control the appearance and basic settings for Transformer.

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

Enable Transformer. If enabled, Agent Hosts connected to this site automatically goes into *kiosk mode*. While in kiosk mode, the Agent Host becomes a web or application launcher that redirects the user to the configured remote desktop interface. The user environment is locked down and the user is only allowed to interact with the agent. If you disable this option, none of the settings in either the **General** or **Advanced** pages are processed.

Web Interface URL. This URL is used as the web front end for the user's virtual desktop. This is the access URL for your Citrix Virtual Apps or Citrix Virtual Desktops™ environment.

Custom Title. If enabled, the Workspace Environment Management™ Agent kiosk window is given a custom title-bar.

Enable Window Mode. If enabled, the Workspace Environment Management Agent kiosk starts in windowed mode. The user is still locked out of their Windows environment.

Allow Language Selection. If enabled, allows users to select what language the Transformer interface is in.

Show Navigation Buttons. If enabled, the "Forward", "Back", and "Home" web navigation buttons appear in the Agent kiosk window. "Home" sends users back to the web interface URL defined above.

Display Clock. If enabled, displays a clock in the Transformer UI.

Show 12 Hour Clock. If enabled, displays a 12-hour clock (AM/PM). By default, the Transformer clock is a 24-hour clock.

Enable Application Panel. If enabled, displays a panel with the user's applications as assigned in Workspace Environment Management.

Auto-Hide Application Panel. If enabled, the application panel auto-hides itself when not in use.

Change Unlock Password. Allows you to specify the password that can be used to unlock the user's environment by pressing **Ctrl+Alt+U**. This is designed to allow administrators and to support agents to troubleshoot the user environment without restrictions.

Site settings

Enable Site List. If enabled, adds a list of URLs to the kiosk interface.

Tool settings

Enable Tool List. If enabled, adds a list of tools to the kiosk interface.

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

Advanced

Process launcher

These options allow you to turn the Workspace Environment Management Agent kiosk mode into a process launcher rather than presenting a web interface.

Enable Process Launcher. If enabled, puts the Workspace Environment Management agent into process launcher mode. While in process launcher mode, the Workspace Environment Management agent launches the process specified in **Process Command Line**. If terminated, the process is relaunched.

Process Command Line. Allows you to enter the command line for a specific process (for example, the path to mstsc.exe to launch an RDP connection).

Process Arguments. Allows you to specify any arguments to the command line listed above (for example, in the case of mstsc.exe, the IP address of the machine to connect to).

Clear Last Username for VMware View. If enabled, clears the user name of the previous user on the logon screen when you launch a VMware desktop session.

Enable VMware View Mode. If enabled, allows the process launcher to monitor the virtual applications or desktops running on a user's machine in VMware View mode and to run **End of Session Options** when they are all closed.

Enable Microsoft RDS Mode. If enabled, allows the process launcher to monitor the virtual applications or desktops running on a user's machine in Microsoft Remote Desktop Services (RDS) mode and to run **End of Session Options** when they are all closed.

Enable Citrix Mode. If enabled, allows the process launcher to monitor the virtual applications or desktops running on a user's machine in Citrix mode and to run **End of Session Options** when they are all closed.

Advanced & administration settings

Fix Browser Rendering. If enabled, forces the kiosk window to run in a browser mode compatible with the version of Internet Explorer (IE) that is currently installed on agent host machines. By default, this forces the kiosk window to run in IE7 compatibility mode.

Log Off Screen Redirection. If enabled, automatically redirects the user to the logon page whenever they land on the logoff page.

Suppress Script Errors. If enabled, suppresses any script errors it encounters.

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

Fix SSL Sites. If enabled, hides SSL warnings entirely.

Hide Kiosk While in Citrix Session. If enabled, hides the Citrix Workspace™ Environment Management Agent kiosk while the users are connected to their Citrix sessions.

Always Show Admin Menu. If enabled, always displays the kiosk admin menu – this gives all users access to the kiosk admin menu.

Hide Taskbar & Start Button. If enabled, hides the user's taskbar and start menu. Otherwise, the user is still able to access their desktop.

Lock Alt-Tab. If enabled, ignores alt tab commands, preventing the user from switching away from the agent.

Fix Z-Order. If enabled, adds a "hide" button to the kiosk interface that allows the user to push the kiosk to the background.

Lock Citrix Desktop Viewer. If enabled, switches the desktop viewer to a locked down mode. This is equivalent to the lockdown that happens when Citrix Workspace app for Windows Desktop Lock is installed. This allows better integration with local applications. This option works only when all of the following conditions are met:

- The user logging on to the agent host is not a member of the administrators group.
- The **Enable Transformer** option on the **General Settings** tab is enabled.
- The **Enable Autologon Mode** option on the **Logon/Logoff & Power Settings** tab is enabled.

Hide Display Settings. If enabled, hides **Display** under **Settings** in the Transformer UI.

Hide Keyboard Settings. If enabled, hides **Keyboard** under **Settings** in the Transformer UI.

Hide Mouse Settings. If enabled, hides **Mouse** under **Settings** in the Transformer UI.

Hide Volume Settings. If enabled, hides **Volume** under **Settings** in the Transformer UI.

Hide Client Details. If enabled, hides **Client Details** under the exclamation mark icon in the Transformer UI. From **Client Details**, you can see information such as the version number.

Disable Progress Bar. If enabled, hides the embedded web browser progress bar.

Hide Windows Version. If enabled, hides **Windows Version** under the exclamation mark icon in the Transformer UI.

Hide Home Button. If enabled, hides the Home icon in the menu in the Transformer UI.

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

Hide Printer Settings. If enabled, hides the Printer icon in the menu in the Transformer UI. Users are not able to manage printers in the Transformer UI.

Prelaunch Receiver. If enabled, launches Citrix Workspace app and wait for it to load before bringing up the kiosk mode window.

Disable Unlock. If enabled, the agent cannot be unlocked through the **Ctrl+Alt+U** unlock shortcut.

Hide Logoff Option. If enabled, hides **Log Off** under the shutdown icon in the Transformer UI.

Hide Restart Option. If enabled, hides **Restart** under the shutdown icon in the Transformer UI.

Hide Shutdown Option. If enabled, hides **Shutdown** under the shutdown icon in the Transformer UI.

Ignore Last Language. The Transformer UI supports multiple languages. In the **General pane**, if the **Allow Language Selection** option is enabled, users can select a language for the Transformer UI. The agent remembers the selected language until this option is enabled.

Logon/logoff and power settings

Enable Autologon Mode. If enabled, users automatically log on to the desktop environment by the agent, bypassing the Windows logon screen.

Log Off Web Portal When a session is launched. If enabled, the web front end specified in the General Settings page is logged off when the user's desktop session is launched.

End of Session Options. Allows you to specify which action the agent takes with the environment that it is running in when the user ends their session.

Shut Down at Specified Time. If enabled, the agent automatically shuts off the environment that it is running in at the specified local time.

Shut Down When Idle. If enabled, the agent automatically shuts off the environment that it is running in after running idle (no user input) for the specified length of time.

Don't Check Battery Status. In Transformer use cases, the agent checks battery status and alerts the user if the battery is running low. If enabled, the agent does not perform this check.

Advanced settings

These settings modify how and when the agent processes actions.

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

Configuration

These options control basic agent behavior.

Main configuration

Agent Actions. These settings determine whether the agent processes actions configured in the Actions tab. These settings apply on logon, and on refresh - automatic or manual refresh (user or administrator triggered).

Process Applications. When selected, the agent processes application actions.

Process Printers. When selected, the agent processes printer actions.

Process Network Drives. When selected, the agent processes network drives actions.

Process Virtual Drives. When selected, the agent processes virtual drive actions. (Virtual drives are Windows virtual drives or MS-DOS device names which map a local file path to a drive letter.)

Process Registry Values. When selected, the agent processes registry entry actions.

Process Environment Variables. When selected, the agent processes environment variable actions.

Process Ports. When selected, the agent processes port actions.

Process Ini Files Operations. When selected, the agent processes .ini file actions.

Process External Tasks. When selected, the agent processes external task actions.

Process File System Operations. When selected, the agent processes file system operation actions.

Process File Associations. When selected, the agent processes file association actions.

Process User DSNs. When selected, the agent processes user DSN actions.

Agent Service Actions. These settings control how the agent service behaves on endpoints.

Launch Agent on Logon. Controls whether the agent runs on logon.

Launch Agent on Reconnect. Controls whether the agent runs when a user reconnects to a machine where the agent is running.

Launch Agent for Admins. Controls whether the agent runs when a user is an administrator.

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

Agent Type. Controls whether a user is presented with a user interface (UI) or a command-line prompt (CMD) when interacting with the agent.

Enable (Virtual) Desktop Compatibility. Ensures that the agent is compatible with desktops where it is running. This setting is necessary for the agent to launch when the user logs on to a session. If you have users on physical or VDI desktops, select this option.

Execute Only CMD Agent in Published Applications. If enabled, the agent launches in CMD mode rather than in UI mode in published applications. CMD mode displays a command prompt instead of an agent splash screen.

Cleanup actions

Options present on this tab control whether the agent deletes the shortcuts or other items (network drives and printers) when the agent refreshes. If you assign actions to a user or user group, you might find that you can also control the creation of the shortcuts or items. You can do so by configuring the options for the actions in the **Assigned** pane of the **Assignments > Action Assignment > Action Assignment** tab. Workspace Environment Management™ processes these options according to a specific priority:

1. The options present on the **Cleanup Actions** tab
2. The options configured for the assigned actions in the **Assigned** pane

For example, suppose you have enabled the **Create Desktop** option for the assigned application in the **Assigned** pane, and the application shortcut is already created on the desktop. The shortcut is still on the desktop when the agent refreshes, even though you enabled the **Delete Desktop Shortcuts** option on the **Cleanup Actions** tab.

Shortcut Deletion at Startup. The agent deletes all shortcuts of the selected types when it refreshes.

Delete Network Drives at Startup. If enabled, the agent deletes all network drives whenever it refreshes.

Delete Network Printers at Startup. If enabled, the agent deletes all network printers whenever it refreshes.

Preserve Auto-created Printers. If enabled, the agent does not delete auto-created printers.

Preserve Specific Printers. If enabled, the agent does not delete any of the printers in this list.

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

Agent options

These options control the agent settings.

Enable Agent Logging. Enables the agent log file.

Log File. The log file location. By default, this is the profile root of the logged-in user.

Debug Mode. This enables verbose logging for the agent.

Enable Offline Mode. If disabled, the agent does not fall back on its cache when it fails to connect to the infrastructure service.

Use Cache Even When Online. If enabled, the agent always reads its settings and actions from its cache (which is built whenever the agent service cycles).

Use Cache to Accelerate Actions Processing. If enabled, the agent processes actions by retrieving relevant settings from the agent local cache instead of from the infrastructure services. Doing so speeds up the processing of actions. By default, this option is enabled. Disable this option if you want to revert to the previous behavior.

IMPORTANT:

- The agent local cache is synchronized with the infrastructure services on a periodic basis. Therefore, changes to action settings take some time to take effect, depending on the value that you specified for the **Agent Cache Refresh Delay** option (on the **Advanced Settings > Configuration > Service Options** tab).
- To reduce delays, specify a lower value. For the changes to take effect immediately, navigate to the **Administration > Agents > Statistics** tab, right-click the applicable agent, and then select **Refresh Cache** in the context menu.

Refresh Environmental Settings. If enabled, the agent triggers a refresh of user environment settings when an agent refresh occurs. For information about environment settings, see Environmental Settings.

Refresh System Settings. If enabled, the agent triggers a refresh of Windows system settings (for example, Windows Explorer and Control Panel) when an agent refresh occurs.

Refresh When Environmental Settings Change. If enabled, the agent triggers a Windows refresh on endpoints when any environment setting changes.

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

Refresh Desktop. If enabled, the agent triggers a refresh of desktop settings when an agent refresh occurs. For information about desktop settings, see Desktop.

Refresh Appearance. If enabled, the agent triggers a refresh of Windows theme and desktop wallpaper when an agent refresh occurs.

Asynchronous Printer Processing. If enabled, the agent processes printers asynchronously, without awaiting the completion of the processing of other actions.

Asynchronous Network Drive Processing. If enabled, the agent processes network drives asynchronously, without awaiting the completion of the processing of other actions.

Initial Environment Cleanup. If enabled, the agent cleans up the user environment during the first logon. Specifically, it deletes the following items:

- User network printers.
    - With **Preserve Auto-created Printers** on the **Cleanup Actions** tab enabled, the agent does not delete auto-created printers.
    - With **Preserve Specific Printers** on the **Cleanup Actions** tab enabled, the agent does not delete any of the printers specified in the list.
- All network drives except the network drive that is the home drive.
- All non-system desktop, Start menu, Quick Launch, and Start-button-context-menu shortcuts.
- All taskbar and Start menu pinned shortcuts.

Initial Desktop UI Cleanup. If enabled, the agent cleans up the session desktop during the first logon. Specifically, it deletes the following items:

- All non-system desktop, Start menu, Quick Launch, and Start-button-context-menu shortcuts.
- All taskbar and Start menu pinned shortcuts.

Check Application Existence. If enabled, the agent does not create a shortcut unless it confirms that the application exists on the machine the user signs in to.

Expand App Variables. If enabled, variables are expanded by default (see Environment variables for normal behavior when the agent encounters a variable).

Enable Cross-Domain User Group Search. If enabled, the agent queries user groups in all Active Directory domains. **Note**: This is an extremely time-intensive process which should only be selected if necessary.

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

Broker Service Timeout. The timeout value after which the agent switches to its own cache, when it fails to connect to the infrastructure service. The default value is 15000 milliseconds.

Directory Services Timeout. The timeout value for directory services on the Agent Host machine, after which the agent uses its own internal cache of user group associations. The default value is 15000 milliseconds.

Network Resources Timeout. The timeout value for resolving network resources (network drives or file/folder resources located on the network), after which the agent considers the action has failed. The default value is 500 milliseconds.

Agent Max Degree of Parallelism. The maximum number of threads the agent can use. Default value is 0 (as many threads as physically allowed by the processor), 1 is single-threaded, 2 is dual-threaded, and so on. Usually, this value does not need changing.

Enable Notifications. If enabled, the agent displays notification messages on the agent host when the connection to the infrastructure service is lost or restored. Citrix® recommends that you do not enable this option on poor-quality network connections. Otherwise, connection state change notifications might appear frequently on the endpoint (agent host).

Advanced options

Enforce Execution of Agent Actions. If these settings are enabled, the Agent Host always refreshes those actions, even if no changes have been made.

Revert Unassigned Actions. If these settings are enabled, the Agent Host deletes any unassigned actions when it next refreshes.

Automatic Refresh. If enabled, the Agent Host refreshes automatically. By default, the refresh delay is 30 minutes.

Reconnection actions

Action Processing on Reconnection. These settings control what actions the Agent Host processes upon reconnection to the user environment.

Advanced processing

Filter Processing Enforcement. If enabled, these options force the Agent Host to reprocess filters at every refresh.

Service options

These settings configure the Agent Host service.

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

Agent Cache Refresh Delay. This setting controls how long the Citrix WEM Agent Host Service waits to refresh its cache. The refresh keeps the cache in sync with the WEM service database. The default is 30 minutes.

SQL Settings Refresh Delay. This setting controls how long the Citrix WEM Agent Host Service waits to refresh its SQL connection settings. The default is 15 minutes.

Agent Extra Launch Delay. This setting controls how long the Citrix WEM Agent Host Service waits to launch the agent host executable.

TIP:

In scenarios where you want the agent host to complete the necessary work first, you can specify how long the agent application launcher (VUEMAppCmd.exe) waits. VUEMAppCmd.exe ensures that the agent host finishes processing an environment before Citrix Virtual Apps and Desktops published applications are started. To specify the wait time, configure the VUEMAppCmd extra sync delay setting, available in the Agent Host Configuration group policy. For more information, see Install and configure the WEM agent.

Enable Debug Mode. This enables verbose logging for all Agent Hosts connecting to this site.

Bypass ie4uinit Check. By default, the Citrix WEM Agent Host Service awaits ie4uinit to run before launching the Agent Host executable. This setting forces the Agent Host service to not wait for ie4uinit.

Agent Launch Exclusions. If enabled, the Citrix WEM Agent Host is not launched for any user belonging to the specified user groups.

Console settings

Forbidden Drives. Any drive letter added to this list is excluded from the drive letter selection when assigning a drive resource.

Allow drive letter reuse in assignment process. If enabled, a drive letter used in an assignment is still available for use by other assignments.

StoreFront™

Use this tab to add a StoreFront store to Workspace Environment Management. You can then navigate to the **Actions > Applications > Application List** tab to add applications available in those stores. Doing so lets you assign published applications as application shortcuts to endpoints. For more information, see Applications. In Transformer (kiosk) mode, assigned StoreFront

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

application actions appear on the **Applications** tab. For more information about StoreFront stores, see StoreFront documentation.

To add a store

1. Click **Add**.
2. Enter details in the **Add Store** dialog, then click **OK**. The store is saved in your configuration set.

Store URL. The URL of the store on which you want to access resources using Workspace Environment Management. The URL must be specified in the form http://hostname, where hostname is the fully qualified domain name of the store and port is the port used for communication with the store if the default port for the protocol is not available.

IMPORTANT:

- The store URL you use must be directly accessible from external networks, and must not be behind any solutions such as Citrix ADC.
- This feature does not work with StoreFront using multifactor authentication.

Description. Optional text describing the store.

To edit a store

Select a store in the list and click **Edit** to change the store URL or description.

To remove a store

Select a store in the list and click **Remove** to remove a store from your configuration set.

To apply changes

Click **Apply** to apply store settings immediately to your agents.

Agent switch

Options present on this tab let you switch from the on-premises agent to the service agent.

IMPORTANT:

Agent switch works at a configuration set level. The switch operation you perform affects only the agents in the configuration set.

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

Switch to Service Agent. If enabled, the agent switches from the on-premises agent to the service agent. You can then specify Citrix Cloud™ Connectors to which the agent connects. This is useful when you want to migrate your existing on-premises deployment to the WEM service.

WARNING:

Enable this option only if you want to move your on-premises deployment to the WEM service. This move cannot be reversed through the WEM administration console.

Configure Citrix Cloud Connectors. Lets you configure the Citrix Cloud Connectors by typing the FQDN or IP address of the Cloud Connector. Click **Add** to add one Cloud Connector at a time. To ensure high service availability, Citrix recommends that you install at least two Cloud Connectors in each resource location. Therefore, you need to configure at least two Citrix Cloud Connectors.

Skip Citrix Cloud Connector™ Configuration. Select this option if you want to configure Citrix Cloud Connectors using Group Policy.

IMPORTANT:

It might take some time for the agent switch settings to take effect, depending on the **SQL Settings Refresh Delay** setting you configured on the **Advanced Settings > Configuration > Service Options** tab.

The agent might fail to connect to the WEM service after you switch from the on-premises agent to the service agent, and you might want to roll back. To do so, use the AgentConfigurationUtility.exe command line; for example:

- `<WEM agent installation folder path>AgentConfigurationUtility.exe switch -o --server <server name> --agentport <port number> --syncport <port number>`
- `<WEM agent installation folder path>AgentConfigurationUtility.exe switch -o --server <server name>`
- `<WEM agent installation folder path>AgentConfigurationUtility.exe switch --usegpo -o`

Wake on LAN

Use this tab to remotely turn on agent hosts. WEM automatically selects agents that reside on the same subnet as the target agents and uses those agents as Wake on LAN messengers. This

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

feature requires hardware compatible with Wake on LAN. To use this feature, verify that the target machines satisfy the hardware requirements and relevant BIOS settings are configured.

Enable Wake on LAN for Agents. Controls whether to configure settings on Windows operating systems to enable Wake on LAN for the agent hosts. If selected, the agents configure the following system settings:

- Disable **Energy Efficient Ethernet** for the network adapter
- Enable **Wake on Magic Packet** for the network adapter
- Enable **Allow this device to wake the computer** for the network adapter
- Enable **Only allow a magic packet to wake the computer** for the network adapter
- Disable **Turn on fast startup**

After enabling this option, navigate to the **Administration > Agents > Statistics** tab, select one or more agents from the list, and then click **Wake Up Agents** to wake up your selected agents.

UI agent personalization

These options let you personalize the look and feel of the agent in UI mode. These options determine how the UI agent appears in the user environment.

NOTE:

These options apply only to the agent in UI mode. They do not apply to the agent in CMD mode.

UI agent options

These settings let you customize the appearance of the session agent (in UI mode only) in the user's environment.

Custom Background Image Path. If specified, displays a custom splash screen instead of the Citrix Workspace Environment Management logo when the agent launches or refreshes. The image must be accessible from the user environment. We recommend that you use a 400*200 px .bmp file.

Loading Circle Color. Lets you modify the color of the loading circle to fit your custom background.

Text Label Color. Lets you modify the color of the loading text to fit your custom background.

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

UI Agent Skin. Lets you select a preconfigured skin you want to use for dialogs that open from the UI agent. For example, the **Manage applications** dialog and the **Manage Printers** dialog. **Note**: This setting does not change the splash screen.

Hide Agent Splashscreen. If enabled, hides the splash screen when the agent is loading or refreshing. This setting does not take effect the first time the agent refreshes.

Hide Agent Icon in Published Applications. If enabled, published applications do not display the agent icon.

Hide Agent Splashscreen in Published Applications. If enabled, hides the agent splash screen for published applications where the agent is running.

Only Admins Can Close Agent. If enabled, only administrators can exit the agent. As a result, the **Exit** option in the agent menu is disabled on endpoints for non-administrators.

Allow Users to Manage Printers. If enabled, the **Manage Printers** option in the agent menu is available to users on endpoints. Users can click the option to open the **Manage printers** dialog to configure a default printer and to modify print preferences. By default, the option is enabled.

Allow Users to Manage Applications. If enabled, the **Manage Applications** option in the agent menu is available to users on endpoints. Users can click the option to open the **Manage applications** dialog and configure the following options. By default, the option is enabled.

- **Desktop**. Adds the application shortcut to the desktop.
- **Start Menu**. Creates the application shortcut in the Start menu folder.
- **QuickLaunch**. Adds the application to the quick launch toolbar.
- **Taskbar (P)**. Creates the application shortcut in the taskbar.
- **Start Menu (P)**. Pins the application to the Start menu.

> **NOTE:**
>
> Shortcuts created in self-healing mode cannot be deleted using this menu. The QuickLaunch option is available only in Windows XP and Windows Vista.

Prevent Admins From Closing Agent. If enabled, administrators cannot exit the agent.

Enable Applications Shortcuts. If enabled, controls whether to display the **My Applications** option in the agent menu. Users can run applications from the **My Applications** menu. By default, the option is enabled.

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

Disable Administrative Refresh Feedback. If enabled, this option does not display a notification in the user environment when an administrator forces an agent refresh through the administration console.

Allow Users to Reset Actions. Controls whether to display the **Reset Actions** option in the agent menu. By default, the option is disabled. The **Reset Actions** option lets current users specify what actions to reset in their environment. After a user selects **Reset Actions**, the **Reset actions** dialog appears. In the dialog, the user can have granular control over what to reset. The user can select applicable actions and then click **Reset**. Doing so purges the corresponding action-related registry entries.

NOTE:

- The following two options are always available in the agent menu: **Refresh** and **About**. The **Refresh** option triggers an immediate update of the WEM agent settings. As a result, settings configured in the administration console take effect immediately. The **About** option opens a dialog displaying version details about the agent in use.

Helpdesk options

These options control help desk functionalities available to users on endpoints.

Help Link Action. Controls whether the **Help** option is available to users on endpoints and what happens when a user clicks it. Type a website link through which users can ask for help.

Custom Link Action. Controls whether to display the **Support** option in the agent menu and what happens when a user clicks it. Type a website link through which users can access support-related information.

Enable Screen Capture. Controls whether to display the **Capture** option in the agent menu. Users can use the option to open a screen capture tool. The tool provides the following options:

- **New capture**. Takes a screenshot of errors in the user environment.
- **Save**. Saves the screenshot.
- **Send to support**. Sends the screenshot to support staff.

Enable Send to Support Option. Controls whether to display the **Send to support** option in the screen capture tool. If enabled, users can use the option to send screenshots and log files directly

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

to the specified support email address, in the specified format. This setting requires a working, configured email client.

Custom Subject. If enabled, lets you specify an email subject template that the screen capture tool uses to send support emails.

Email Template. Lets you specify an email content template that the screen capture tool uses to send support emails. This field cannot be empty.

> **NOTE:**
>
> For a list of hash-tags that you can use in the email template, see Dynamic tokens. Users are only presented with the option to enter a comment if the **##UserScreenCaptureComment## hash-tag** is included in the email template.

Use SMTP to Send Email. If enabled, sends a support email using SMTP instead of MAPI.

Test SMTP. Tests the SMTP settings as typed above to verify that they are correct.

Power saving

Shut Down At Specified Time. If enabled, lets the agent automatically shuts down the machine where it is running at the specified time. The time is based on the agent time zone.

Shut Down When Idle. If enabled, lets the agent automatically shut down the machine where it is running after the machine remains idle (no user input) for the specified length of time.

Administration

The **Administration** pane consists of the following:

- **Administrators**. Lets you define Workspace Environment Management™ administrators (users or groups) and give them permissions to access configuration sets through the administration console.
- **Users**. Lets you view user statistics.
- **Agents**. Lets you view agent statistics and perform administrative tasks such as refreshing cache, resetting settings, and uploading statistics.
- **Logging**. Lets you view administrative activities in Workspace Environment Management. You can use the logs to:
    - Diagnose and troubleshoot problems after configuration changes are made.

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

- Assist change management and track configurations.
- Report administrative activities.

Administrators

These options let you define Workspace Environment Management administrators (users or groups) and give them permissions to access configuration sets through the administration console.

Configured administrators list

A list of configured administrators showing their permission level (**Full Access**, **Read Only** or **Granular Access**, see details below). You can use **Find** to filter the list by name or ID against a text string.

To add an administrator

1. Use the context menu **Add** command.
2. Enter details in the Select Users or Groups dialog, then click **OK**.

Name. The name of the user or group you are currently editing.

Description. Additional information about the user or group.

Global Administrator. Select to specify that the selected user/group is a Global Administrator. Clear to specify that the selected user/group is a Site Administrator. Global Administrators have their permissions applied to all sites (configuration sets). Site Administrators have their permissions configured on a per-site basis.

Permissions. This allows you to specify one of the following levels of access to the selected user/group. **Note**: Administrators can only view settings which they have access to.

Full Access administrators have full control over every aspect of the specified sites (configuration sets). Only Global Administrators with Full Access can add/delete Workspace Environment Management administrators. Only Global Full Access and Global Read Only administrators can see the **Administration** tab.

Read Only administrators can view the entire console, but cannot modify any settings at all. Only Global Full Access and Global Read Only administrators can see the **Administration** tab.

Granular Access indicates that the administrator has one or more of the following permission sets:

Action Creators can create and manage actions.

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

Action Managers can create, manage, and assign actions. They cannot edit or delete actions.

Filter Managers can create and manage conditions and rules. Rules that are in use on assigned applications cannot be edited or deleted by Filter Managers.

Assignment Managers can assign resources to users or groups.

System Utilities Managers can manage the System Utilities settings (CPU, RAM and process management).

Policies and Profiles Managers can manage Policies and Profiles settings.

Configured Users Managers can add, edit, and remove users or groups from the configured users list. Users or groups with assigned actions cannot be edited or deleted by Configured Users Managers.

Transformer Managers can manage Transformer settings.

Advanced Settings Managers can manage advanced settings (enabling or disabling action processing, cleanup actions, and so on).

Security Managers can access all controls in the Security tab.

State. This controls whether the selected user/group is enabled or disabled. When disabled, the user/group is not considered to be a Workspace Environment Management administrator and cannot use the administration console.

Type. This field is read only and indicates whether the selected entity is a user or a group.

If the **Global Administrator** is cleared, the following controls are enabled:

Site Name. All Workspace Environment Management sites (configuration sets) belonging to the database this infrastructure service is connected to.

Enabled. Select to enable this administrator for the specified Workspace Environment Management site (configuration set). When disabled, the user/group is not considered to be an administrator for that site and cannot access it.

Permissions. Select a permission level for the selected user/group for each Workspace Environment Management site (configuration set) attached to this infrastructure service.

Users

This page displays statistics about your Workspace Environment Management deployment.

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

Statistics

This page displays a summary of users whose agent hosts have connected to the database.

Users Summary. Displays a count of total users who have reserved a Workspace Environment Management license, for both the current site (configuration set) and all sites (configuration sets). Also displays a count of new users in the last 24 hours and in the last month.

Users History. This displays connection information for all the users associated with the current site (configuration set), including the last connection time, the name of the machine from which they last connected and the session agent type (UI or CMD) and version. You can use **Find** to filter the list by name or ID against a text string.

Agents

This page displays statistics about the agents in your Workspace Environment Management deployment.

Statistics

This page displays a summary of the Workspace Environment Management agents recorded in the Workspace Environment Management database.

Agents Summary. Displays a count of total agents that have reserved a Workspace Environment Management license, for both the current configuration set and all configuration sets. It also reports agents added in the last 24 hours and in the last month.

Agents History. Displays connection information for all agents registered with the configuration set, including the last connection time, the name of the device from which they last connected, and the agent version. You can use **Find** to filter the list by name or ID.

In the **Synchronization State** column, the following icons indicate the result of the last synchronization of the agent cache with the Workspace Environment Management database.

- Successful (check mark icon). Indicates that the last synchronization was successful, with the synchronization result reported to the administration console.
- Unknown (question mark icon). Indicates that synchronization is in progress, synchronization has not started yet, or the synchronization result is not reported to the administration console.
- Failed (X icon). Indicates that the last synchronization failed.

In the **Profile Management Health Status** column, you can view the health status of Profile Management in your deployment.

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

Profile Management health status performs automated status checks on your agent hosts to determine whether Profile Management is configured optimally. You can view the results of these checks to identify specific issues from the output file on each agent host (`%systemroot%\temp\UpmConfigCheckOutput.xml`). The feature performs status checks every day or each time the WEM agent host service starts. To perform the status checks manually, right-click the selected agent in the administration console, and then select the **Refresh Profile Management Configuration Check** in the context menu. Each status check returns a status. To view the most recent status, click **Refresh**. The icon in the **Profile Management Health Status** column provides general information about the health status of Profile Management:

- Good (check mark icon). Indicates that Profile Management is in good shape.
- Warning (triangle exclamation point icon). Informs about a suboptimal state of Profile Management. The suboptimal settings might affect the user experience with Profile Management in your deployment. This status does not necessarily require action on your part.
- Error (X icon). Indicates that Profile Management is configured incorrectly, causing Profile Management not to function properly.
- Unavailable (question mark icon). Appears when Profile Management is not found or not enabled.

If the status checks do not reflect your experience or if they do not detect the issues you are having, contact Citrix Technical Support.

In the **Recently Connected** column, the following icon indicates that the agent uploaded statistics to the Workspace Environment Management database within a certain interval. The agent is online. A blank column field indicates that the agent is offline.

- Online (check mark icon)

Clear Expired Records. Lets you delete the expired records from the Workspace Environment Management database. If a user's last logon time dates back more than 24 hours, the corresponding record expires.

Wake Up Agents. Lets you wake up the selected agents.

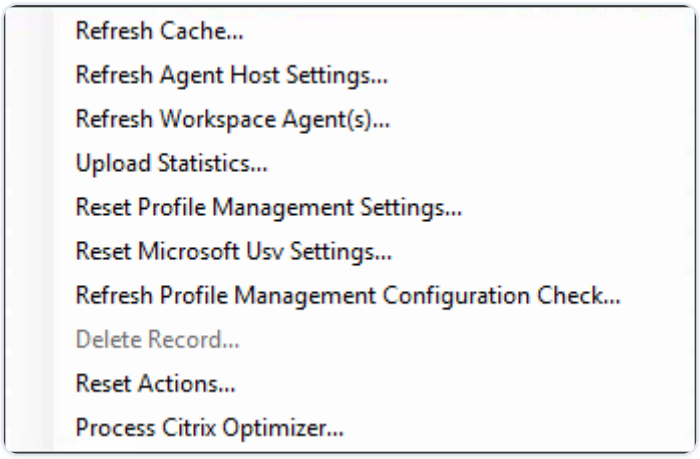
To refresh agents

When you refresh an agent it communicates with the infrastructure server. The infrastructure server validates the agent host identity with the Workspace Environment Management database.

1. Click **Refresh** to update the list of agents.
2. In the context menu select **Refresh Workspace Agent(s)**.

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

Options in the context menu



Refresh Cache. Triggers a refresh of the agent local cache (an agent-side replica of the WEM configuration database). Refreshing the cache synchronizes the agent local cache with the infrastructure services.

Refresh Agent Host Settings. Applies the agent service settings. Those settings include advanced settings, optimization settings, transformer settings, and other non-user assigned settings.

Refresh Workspace Agents. Applies the user-assigned actions to the WEM agents. Those actions include network drives, printers, applications, and more.

IMPORTANT:

- The **Refresh Workspace Agents** option works only with the agents in UI mode that are automatically launched (not launched by end users or by using scripts). The option does not work with the agents in CMD mode.
- Not all settings can be refreshed. Some settings (for example, environment settings and group policy settings) are applied only on startup or logon.

Upload Statistics. Uploads statistics to the infrastructure service.

Reset Profile Management Settings. Clears the registry cache and updates the associated configuration settings. If Profile Management Settings are not applied to your agent, click **Reset Profile Management Settings**. You might need to click **Refresh** for this option to become available.

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

NOTE:

If the settings are not applied to the agent after configuring **Reset Profile Management Settings** from the WEM administration console, see CTX219086 for a workaround.

Reset Microsoft USV Settings. Clears the registry cache and updates the associated configuration settings. If Microsoft USV Settings are not applied to your agent, click **Reset Microsoft Usv Settings**, and then click **Refresh**.

Refresh Profile Management Configuration Check. Performs status checks on your agent host(s) to determine whether Profile Management is configured optimally.

Delete Record. Enables deletion of the agent record from the database. If the agent is still active, this option is grayed out.

Reset Actions. Lets you reset all actions you assigned by purging all action-related registry entries on the applicable machine.

Process Citrix Optimizer. Applies the settings to the agents so that changes to Citrix optimizer settings take effect immediately.

Run delivery task. To enable this option, select agents bound to the same configuration set. To run a delivery task quickly, you can choose to run a delivery task from this page. Click **Run delivery task** and choose the delivery task from the drop-down list to run the selected delivery task on the agent. If you configure rules in the task to determine which agents must run the task, those rules get ignored when you select specific agents to run the on demand tasks.

Registrations

This page shows the registration status of the Workspace Environment Management agents recorded in the database.

IMPORTANT:

Agents must register only with one configuration set.

The following information is reported:

Machine Name. Name of computer on which the agent is running.

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

State. Registration status of agent on the agent host computer, indicated by icons and the following description giving more information about registration success or failure:

Agent is not bound to any site. The infrastructure server cannot resolve any site (configuration set) for this agent because the agent is not bound to any site (configuration set).

Agent is bound to one site. The infrastructure server is sending the necessary machine-dependent settings to the agent for that site (configuration set).

Agent is bound to multiple sites. The infrastructure server cannot resolve a site (configuration set) for this agent because the agent is bound to more than one site (configuration set).

To resolve registration errors

Either

- edit the Active Directory hierarchy (relations between computers, computer groups, and OUs)

OR

- edit the Workspace Environment Management hierarchy (in the Active Directory Objects section of the administration console) so that a computer binds to only one site (configuration set).

After making these changes, refresh agents with the infrastructure server.

Logging

Administrative

This tab displays a list of all changes made to the Workspace Environment Management settings in the database. By default, the log is unpopulated until the log is refreshed manually.

Filtering Options. These options allow you to filter the log by site (configuration set), and date range.

Export Log. Exports the log in XLS format.

Refresh Log. Refreshes the log.

Clear Log. Clears the log for all configuration sets. ***This cannot be undone***. Clearing the log adds one event in the new log indicating this has been done. This option is only available to Global Full Access administrators.

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

Agent

This tab lists all changes made to your Workspace Environment Management agents. The log is unpopulated until you click **Refresh**.

Filtering Options. These options allow you to filter the log by site (configuration set), and date range.

Export Log. Exports the log in XLS format.

Refresh Log. Refreshes the log.

Clear Log. Clears the log for all configuration sets. ***This cannot be undone***. Clearing the log adds one event in the new log indicating this has been done. This option is only available to Global Full Access administrators.

Monitoring

These pages contain detailed user login and machine boot reports. You can **Export** all reports in various formats.

Daily reports

Daily Login Report. A daily summary of login times across all users connected to this site. You can double-click a category for a detailed view showing individual logon times for each user on each device.

Daily Boot Report. A daily summary of boot times across all devices connected to this site. You can double-click a category for a detailed view showing individual boot times for each device.

User trends

Login Trends Report. This report displays overall login trends for each day over the selected period. You can double-click each category of each day for a detailed view.

Boot Trends Report. This report displays overall boot trends for each day over the selected period. You can double-click each category of each day for a detailed view.

Device Types. This report displays a daily count of the number of devices of each listed operating system connecting to this site. You can double-click each device type for a detailed view.

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

User & device reports

User Report. This report allows you to view login trends for a single user over the selected period. You can double-click each data point for a detailed view.

Device Report. This report allows you to view boot trends for a single device over the selected period. You can double-click each data point for a detailed view.

Profile container insights

This feature monitors profile containers for Profile Management and FSLogix. It provides insights into the basic usage data of the profile containers, the status of sessions using the profile containers, the issues detected, and more.

Use this feature to stay on top of space usage for profile containers and to identify problems that prevent profile containers from working.

Summary

Includes two doughnut charts:

- **Used Space**. The chart on the left side shows the space usage of profile containers over the specified time period.
- **Session Status**. The chart on the right side shows results of attaching profile containers for sessions established over the specified time period.

After specifying the time period (for example, last 6 days), click **Refresh** to trigger a refresh of the charts.

High when used space is more than (GB). Lets you type a threshold value above which to treat the space usage of the profile containers as high. Type a positive integer.

Low when used space is less than (GB). Lets you type a threshold value below which to treat the space usage of the profile containers as low. Type a positive integer.

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

NOTE:

- The high threshold value must be greater than the low threshold value.
- After specifying the high and the low threshold values, click **Refresh** to trigger a refresh of the **Used Space** chart.
- After specifying the high and the low threshold values, space usage in between defaults to **Medium**.

Profile container status

Displays a list of status records for profile containers over a specified time period. After specifying the time period (for example, last 6 days), click the **Refresh** button to filter records.

You can trigger the collection of data for the container the selected record pertains to. Doing so brings you up to date with the user's container status. To achieve that, right-click a status record and then select **Refresh**. The refresh operation results in a sequence of tasks. First, a task is immediately sent to the associated agent host. The agent receives the task and then collects status-related data if the container is in use on the agent host. Then, the latest attach record is updated with the collected data. It might take a while for the status to be updated. Click the **Refresh** button for the up-to-date record to appear.

The **Status** column displays information about status and error codes. For information about error codes, see the Microsoft documentation at `<https://docs.microsoft.com/en-us/fslogix/fslogix-error-codes-reference>`.

Configuration

Report options

These options allow you to control the reporting period and work days. You can also specify minimum **Boot Time** and **Login Time** (in seconds) below which values are not reported.

Back up and restore

The **Backup and restore** page displays a list of your existing backups. There are two types of backups: automatic backup and manual backup (configuration set and settings). You can differentiate automatic backups from manual backups by the **Content type** column.

For each backup, you can perform the following operations:

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

- **Restore**. Lets you restore a configuration from the backup. Restoring a configuration from a backup replaces all settings related to the selected configuration set with those from the backup.

  NOTE:

  - To restore Profile Management settings to a configuration set, you can also use the quick setup feature on the **Profiles > Profile Management Settings** page under that configuration set.
  - When restoring Profile Management settings from a backup, the SMB shares selected for relevant services to use are also restored.

- **Download.** Lets you save a copy of the backup to your local machine. The backup is saved to the default download location of your browser. The backup file is in JSON format.
- **Delete**. Lets you delete an existing backup.

You can also perform the following operations:

- Click the Refresh icon next to the **Upload** button to refresh the current page
- Upload a configuration file
- Manage automatic backup
- Back up a configuration set
- Back up Profile Management settings

Upload a configuration file

You can upload a JSON file used to revert to a previous backup. A JSON file can contain a configuration set or Profile Management settings. To upload a file, perform the following steps:

1. Click **Upload**. The **Upload backup file** wizard appears.
2. Click **Browse**, browse to the file you want to upload, select the file, and then click **Open**. You are returned to the **Upload backup file** wizard.
3. Specify a name for your file.
4. Click **Upload** to start the upload.

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

NOTE:

- You can upload only JSON files.
- You can upload only files whose size is smaller than 5 MB.

Manage automatic backup

You can save a backup of a configuration set automatically. The feature supports storing up to 5 backup files for each configuration set before starting to overwrite the oldest existing file. You cannot back up the following items related to a configuration set:

- Directory objects related to machines (single machines, machine groups, and OUs)
- Monitoring data (statistics and reports)
- Process management
- Agents registered with the configuration set

To configure automatic backup, perform the following steps:

1. Click **Manage automatic backup**. The **Manage automatic backup** wizard appears.
2. Locate the configuration set you want to back up automatically.
3. Select one of the following three options for that configuration set.
    - **Not configured**. If selected, WEM does not back up automatically.
    - **Daily**. If selected, WEM performs backups on a daily basis.
    - **Weekly**. If selected, WEM performs backups every Monday.
4. Repeat steps 2 and 3 for other configuration sets if needed.
5. Click **Save** to save your changes and to exit the wizard.

Back up a configuration set

IMPORTANT:

We limit the number of manual backups to 10 per account. If you have reached the limit, delete existing backups and try again.

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

You can save a backup copy of your configuration set and then use the backup for restore purposes. You can back up the following items related to a configuration set:

- Actions
- Application security, privilege elevation, and process hierarchy control
- Assignments (related to actions and action groups)
- Filters
- Scripted task settings
- Users
- WEM settings

You cannot back up the following items related to a configuration set:

- Directory objects related to machines (single machines, machine groups, and OUs)
- Monitoring data (statistics and reports)
- Process management
- Agents registered with the configuration set

To back up a configuration set, perform the following steps:

1. Click **Back up**. The **Back up** wizard appears.
2. Select the target configuration set.
3. Select from the list the configuration set you want to back up.
4. Specify a name for your backup.
5. Optionally, select **Save a copy of the backup to your local machine** to save the backup locally.

   NOTE:

   The backup is saved to the default download location of your browser.

6. Click **Back up** to start the backup.

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

Back up Profile Management settings

IMPORTANT:

We limit the number of manual backups to 10 per account. If you have reached the limit, delete existing backups and try again.

To back up Profile Management settings, perform the following steps:

1. Click **Back up**. The **Back up** wizard appears.
2. Select the target configuration set.
3. Select **Settings** from the **What to back up** list.
4. Select **Profile Management settings**.
5. Specify a name for your backup.
6. Optionally, select **Save a copy of the backup to your local machine** to save the backup locally.

   NOTE:

   The backup is saved to the default download location of your browser.

7. Click **Back up** to start the backup.

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

Reference

Use the following articles to perform specific tasks:

- Agent event logs
- Agent Insights
- Agent in CMD and UI mode
- Citrix Environment Tool Hub
- Common Control Panel applets
- Dynamic tokens
- Environmental Settings registry values
- Filter conditions
- FIPS support
- Load balancing with Citrix ADC
- Log parser
- Port information
- View log files
- Troubleshoot WEM LAS issues
- WEM health check tool
- WEM Integrity Condition List Manager
- XML printer list configuration

Agent event logs

This article provides a list of WEM event logs, along with their corresponding, and distinct event IDs.

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

WEM configuration set

EVENT ID	LEVEL	MESSAGE
1001	Info	Agent successfully registered with configuration set: name: `configuration set name` (ID: `configuration set ID`) .
1002	Warning	Agent not registered with any configuration set

WEM agent connection to infrastructure services

EVENT ID	LEVEL	MESSAGE
2001	Info	Connecting to infrastructure service: address: `service address`
2002	Error	Invalid infrastructure service address
2003	Error	Unable to connect to WEM service
2020	Info	Connecting to WEM service: address: `service address`
2021	Info	Getting Cloud Connectors configured for WEM:`Cloud Connector list`
2022	Info	Discovering Cloud Connectors from Citrix DaaS™:`Cloud Connector list`
2023	Error	All Cloud Connectors unreachable

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

EVENT ID	LEVEL	MESSAGE
2024	Info	Cloud Connector operational: `Cloud Connector address`
2025	Warning	Cloud Connector unreachable: `Cloud Connector address`
2026	Error	Unable to connect to WEM service through Cloud Connector

Agent configuration refresh events

EVENT ID	LEVEL	MESSAGE
3001	Info	Initiating agent configuration settings refresh
3002	Error	Agent configuration settings refresh failed with exception: `exception code`
3003	Info	Agent configuration settings refreshed successfully

Directory service events

EVENT ID	LEVEL	MESSAGE
4001	Warning	Unable to retrieve user token groups list
4002	Warning	Unable to retrieve user directory services groups
4003	Warning	Unable to retrieve all groups to which the user belongs
4004	Warning	Unable to retrieve all OUs to which the user belongs

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

EVENT ID	LEVEL	MESSAGE
4005	Warning	Unable to retrieve local computer group list
4006	Warning	Unable to retrieve local computer OU list

Machine policy events

EVENT ID	LEVEL	MESSAGE
5001	Info	Initiating processing of computer group policies
5002	Info	Skipping processing of machine policies due to unmet prerequisites
5003	Info	Skipping machine policy processing: Group Policy settings processing not enabled
5004	Warning	Unable to retrieve the groups or OUs to which the computer belongs. Group policy processing terminated
5005	Info	Computer group policies applied successfully
5006	Warning	Unable to apply computer group policies. List of failed GPOs: `GPO list`

User policy events

EVENT ID	LEVEL	MESSAGE
5501	Info	Initiating processing of user group policies for `user name`

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

EVENT ID	LEVEL	MESSAGE
5502	Info	Skipping processing of user policies due to unmet prerequisites
5503	Info	Skipping user policy processing: Group Policy settings processing not enabled
5504	Info	Policy processing skipped for local user `user identity name`, as no mapped account found
5505	Warning	Unable to retrieve the groups or OUs to which the user belongs. Group policy processing terminated
5506	Info	User group policies applied successfully
5507	Warning	Unable to apply user group policies. List of failed GPOs: `GPO list`

Cache sync events

EVENT ID	LEVEL	MESSAGE
6001	Info	Initiating automatic agent cache sync
6002	Info	Initiating on-demand agent cache sync
6003	Warning	Network unavailable, agent cache sync skipped
6004	Warning	Agent cache sync skipped: invalid cloud service settings

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

EVENT ID	LEVEL	MESSAGE
6005	Warning	Agent cache sync skipped: invalid infrastructure service address
6006	Error	Agent cache sync failed with unexpected error
6007	Info	Agent cache sync completed successfully
6008	Info	Starting file-based cache synchronization.
6009	Warning	Cache file is too large to save to persistent data location. File size: `{size}`.
6010	Info	File-based cache synchronization completed.
6011	Info	File-based cache information: Sync mode: `{sync mode}`, Cache location: `{location}`
6012	Error	File-based cache synchronization failed. Error: `{error message}`
6013	Error	Unable to save cache to persistent data location. Error: `{error message}`
6014	Info	No persistent cache file found. Cache will not be restored from persistent data location.
6015	Error	Unable to restore cache from persistent data location. Error: `{error message}`

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

EVENT ID	LEVEL	MESSAGE
6016	Info	Removing invalid persistent cache file.
6017	Error	Unable to create basic settings cache for basic deployment mode. Error: `{error message}`
6018	Info	File-based cache synchronization succeeded. Cache location: `{location}`

Optimization events

CPU optimization

For messages with event IDs starting from 7003 through 7008 to be written, add the following registry.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Agent Host

Name: EnableExtraLoggingForOptimization

Type: REG_DWORD

Value: 1

CAUTION:

Editing the registry incorrectly can cause serious problems that 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.

EVENT ID	LEVEL	MESSAGE
7001	Info	Initializing CPU spike protection for process `process name`

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

EVENT ID	LEVEL	MESSAGE
		(ID:`process ID`), created by user `user name`. The sum of average CPU usage per each core detected at `percentage value`, with a total system CPU usage of `percentage value`.
7002	Info	Initializing CPU spike protection for process `process name` (ID:`process ID`), created by user `user name`. Average CPU usage detected at `percentage value`, with a sum of average CPU usage per each core detected at `percentage value`.
7003	Info	Changed priority to `priority value` for process `process name` (ID:`process ID`), created by user `user name`.
7004	Warning	Unable to change priority to `priority value` for process `process name` (ID:`process ID`), created by user `user name`. Error code:`error code`.
7005	Info	Affinity (`affinity value`) processed successfully for process `process name` (ID:`process ID`), created by user `user name`.
7006	Warning	Unable to configure affinity (`affinity value`) for process `process name`

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

EVENT ID	LEVEL	MESSAGE
		(ID: `process ID`), created by user `user name`.
7007	Info	Changed I/O priority to `priority value` for process `process name` (ID: `process ID`), created by user `user name`.
7008	Warning	Unable to change I/O priority to `priority value` for process `process name` (ID: `process ID`), created by user `user name`.

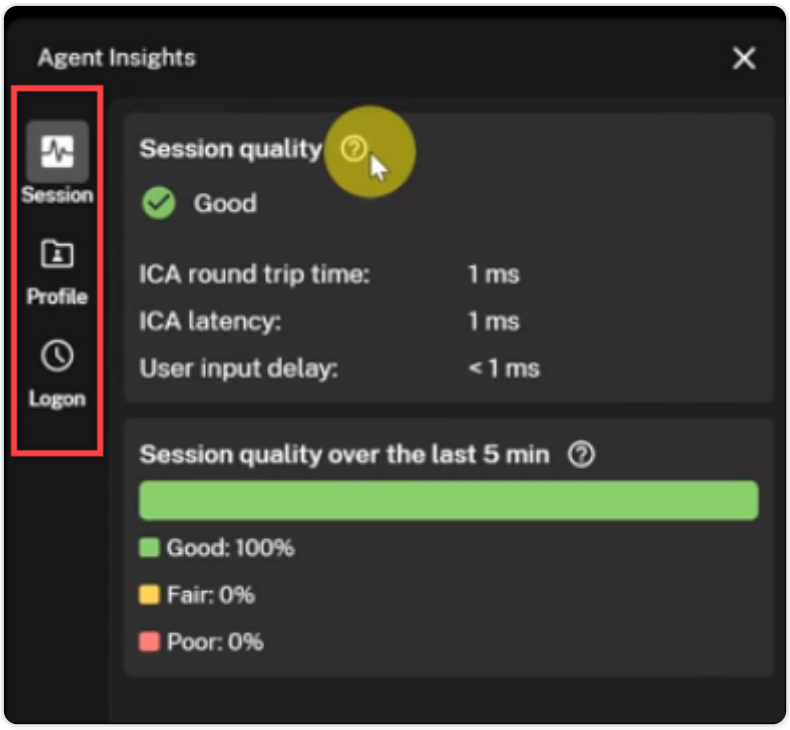
Memory optimization

EVENT ID	LEVEL	MESSAGE
8001	Info	Initializing memory optimization for process `process name` (ID: `process ID`), created by user `user name`.
8002	Info	Memory Optimization succeeded for process `process name` (ID: `process ID`), created by user `user name`.
8003	Warning	Unable to optimize memory for process `process name` (ID: `process ID`), created by user `user name`.

Agent Insights

Agent Insights is a tool provided with the WEM agent that helps you monitor and troubleshoot session performance, profile container usage, and logon activity in real time.

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



With Agent Insights, you can review the following details on your machine:

- **Session**: The current session status and session quality over the last five minutes.
- **Profile**: Profile container details, including profile type, storage path, capacity, and a list of large files.
- **Logon**: Logon duration, start and end times, and key logon metrics.

WEM Administrators: Enable and configure Agent Insights in the WEM console

If the agent runs in a mode other than **Basic mode**, enable and configure Agent Insights for your machines using the WEM web console. To do so:

1. In the WEM web console, open your configuration set in **Configuration sets**.
2. Go to **Advanced settings > UI agent personalization > User interaction**, and select **Show Agent Insights in agent menu**.

   For more information, see Advanced settings.
3. To ensure that profile container data and logon data are displayed correctly, go to **Advanced settings > Monitoring preferences > Additional settings**, and select **Save reports locally to display in Agent Insights**.

   For more information, see Additional settings.

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

4. To show a large file list in the **Profile** tab, go to **Advanced settings > Monitoring preferences**, and ensure that **Enable large file scanning** is selected.

   For more information, see Monitoring preferences.

If the agent runs in **Basic mode**, use Group Policy to enable these Agent Insights settings:

- `enableAgentInsightsManagement`
- `enableLargeFileScan`

For more information, see Manage Basic Deployment Agents.

Users: Enable and open Agent Insights on machines

After WEM administrators enable and configure Agent Insights in the WEM web console, as end users, you can access the feature from your machines.

Enable and open the Agent Insights panel to view detailed session performance, profile container usage, and logon activity. To do so:

1. Run the agent in **UI mode**.

   For more information, see Agent in CMD and UI mode.
2. Right-click the agent icon in the notification area, and select **Enable Agent Insights**.

   To disable Agent Insights, right-click the icon again and select **Disable Agent Insights**.
3. Click the agent icon in the notification area. The Agent Insights panel opens.
4. Use the tabs on the left side of the panel to view insights into:

   - Session
   - Profile
   - Logon

Reference

The following tabs in the Agent Insights panel provide detailed metrics to help troubleshoot session performance, profile container usage, and logon activity:

- Session
- Profile
- Logon

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

Session tab

The **Session** tab provides insight into the current session status and session quality over the last five minutes.

NOTE:

This tab displays data only for Citrix virtual desktops. It doesn't apply to physical machines.

Current session status

METRIC	DESCRIPTION
ICA® Round Trip Time	The time between a user action and the graphical response. Includes ICA latency, endpoint delay, and host delay.
ICA Latency	Measures network latency.
User Input Delay	The time that user input (such as mouse clicks or keystrokes) waits before being processed. High values might indicate resource contention or performance issues.

Session quality

The **Session Quality** section summarizes the user experience over the last five minutes.

QUALITY	DESCRIPTION
Good	The session is responsive.
Fair	Some performance degradation is present.
Poor	High latency or delays, likely due to network or system issues.

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

Profile tab

NOTE:

This tab applies only to profile container deployments using Citrix Profile Management or Microsoft FSLogix.

The **Profile** tab displays:

- Profile type
- Profile size
- Capacity
- List of large files (if available)

NOTE:

Large file data updates only when Agent Insights loads. Select **Refresh** to update the data.

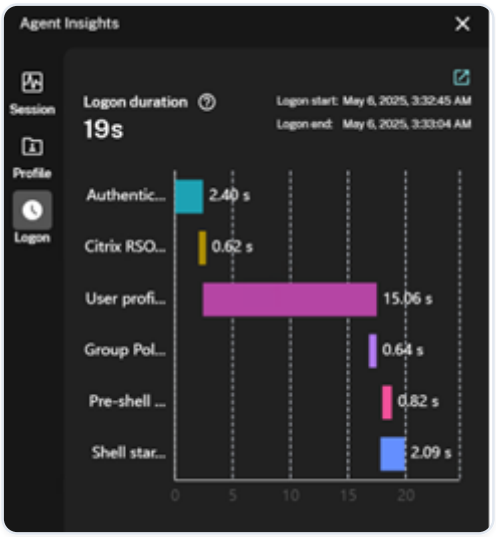
Logon tab

The **Logon** tab shows the following metrics:

METRIC	DESCRIPTION
Logon Duration	Total time required for the logon process.
Start and End Time	Time stamps for logon start and end.
Basic Metrics	Key indicators of logon performance.

A waiting page appears before the logon data loads. After the user logs on, the summary appears.

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



TIP:

If **Citrix Environment Tool Hub** is installed, select the data area or the icon in the top-right corner of the panel to view more details. If it isn't installed, a download link appears in the same location. Install **Citrix Environment Tool Hub** to access extended diagnostics and monitoring features.

Agent in CMD and UI mode

The Workspace Environment Management™ agent can run in CMD mode and UI mode.

When you configure the agent to run on logon, you can control whether to start it in CMD mode or UI mode. To do that, use the **Agent Type** setting, available on the **Administration Console > Advanced Settings > Configuration > Main Configuration** tab. For more information, see Advanced settings.

If you do not configure the agent to run automatically on logon, you (administrators or end users) can start the agent in CMD mode or UI mode on the agent machine. To do that, navigate to the agent installation folder and identify the following two .exe files:

- **VUEMCmdAgent.exe**. Lets you run the agent in CMD mode.
- **VUEMUIAgent.exe**. Lets you run the agent in UI mode.

Differences between CMD mode and UI mode

For CMD mode, be aware of the following considerations:

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

- When running automatically on logon, CMD mode displays a command prompt. CMD mode exits automatically after startup.
- On startup, CMD mode applies the user-assigned actions to the agent. Those actions include network drives, printers, applications, and more.
- Currently, CMD mode does not support any command-line operations.

For UI mode, be aware of the following considerations:

- When running automatically on logon, UI mode displays an agent splash screen.
- UI mode can present the following options:
  - **My Applications**. Lets you view applications assigned to you.
  - **Capture Screen**. Lets you open a screen capture tool. This option requires **Enable Screen Capture** on the **Administration Console > Advanced Settings > UI Agent Personalization > Helpdesk Options** tab to be enabled. For more information, see Helpdesk Options.
  - **Reset Actions**. Lets you open the **Reset actions** tool to specify what actions to reset in the environment.

  This option requires **Allow Users to Reset Actions** on the **Administration Console > Advanced Settings > UI Agent Personalization > UI Agent Options** tab to be enabled. For more information, see UI Agent Options.

  - **Manage Applications**. Lets you open the **Manage applications** tool to manage applications.

  This option requires **Allow Users to Manage Applications** on the **Administration Console > Advanced Settings > UI Agent Personalization > UI Agent Options** tab to be enabled. For more information, see UI Agent Options.

  - **Manage Printers**. Lets you open the **Manage printers** tool to configure a default printer and modify printing preferences.

  This option requires **Allow Users to Manage Printers** on the **Administration Console > Advanced Settings > UI Agent Personalization > UI Agent Options** tab to be enabled. For more information, see UI Agent Options.

  - **Refresh**. Refreshes the agent, applying the user-assigned actions to the agent. Those actions include network drives, printers, applications, and more.
  - **Help**. Lets you open a website through which you can ask for help.

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

This option requires **Help Link Action** on the **Administration Console > Advanced Settings > UI Agent Personalization > Helpdesk Options** tab to be specified. For more information, see Helpdesk Options.

- **About**. Displays information about the agent version.
- **Exit**. Lets you close the agent.

To reset actions and manage applications and printers, you can directly use the following tools (available in the agent installation folder) without the need to use the agent in UI mode:

- **ResetActionsUtil.exe**. Lets you open the **Reset actions** tool.
- **AppsMgmtUtil.exe**. Lets you open the **Manage applications** tool.
- **PrnsMgmtUtil.exe**. Lets you open the **Manage printers** tool.

Key differences between CMD mode and UI mode:

- The CMD agent applies settings and then exits. You can configure the WEM agent service (Citrix WEM Agent Host Service or Citrix WEM User Logon Service) to start the CMD agent at a particular point in time (for example, logon or reconnect). If necessary, administrators can invoke the CMD agent manually.
- The UI agent keeps running. The Citrix WEM Agent Host Service starts or stops the UI agent. The UI agent provides self-service options to end users. We recommend that administrators do not launch the UI agent manually.

NOTE:

You cannot run the CMD agent and the UI agent at the same time in a session.

Citrix Environment Tool Hub

Citrix Environment Tool Hub is a collection of tools that aims to simplify the configuration experience for Workspace Environment Management™ (WEM) administrators. You can download the tool from the on-premises web console or using or Tools and Utilities > Citrix Environment Tool Hub.

The prerequisites for running Citrix Environment Tool Hub are as follows:

- .NET Framework 4.7.1 or later
- Microsoft Edge WebView2 Runtime version 98 or later

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

- Local administrator privilege

This article describes the tools available in Citrix Environment Tool Hub and how to use them.

NOTE:

- Citrix Environment Tool Hub does not save data for you. Data will be cleared after you exit a tool. To avoid potential data loss, be sure to save your work.
- To paste data copied from Citrix Environment Tool Hub into the web console, ensure that the browser allows data copying. Example: For Microsoft Edge, be sure to have the **Site permissions > Clipboard > Ask when a site wants to see text and images copied to the clipboard** option enabled.

Download and launch the tool hub

1. Download the tool hub `.zip` file from one of the following URLs:
   - `<https://wem-production-ui.wem.cloud.com/utilities>`
   - `<https://www.citrix.com/downloads/citrix-tools/citrixtoolspage/CitrixEnvironmentToolHub.html>`
2. Extract the `.zip` file.
3. Double-click `Citrix.WEM.Admin.ToolHub.exe` to launch the tool hub.

Application Assistant

Use this tool to prepare configuration information for icons and Citrix Workspace™ resources that you want to use when adding applications in the management console.

Workspace resources

NOTE:

This tool requires Citrix Workspace app to be installed on the machine.

When adding an application of type "Citrix Workspace resource" to the web console, you need to specify a resource. To get information for a resource, complete the following steps:

1. Enter a Store URL or Workspace URL.

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

2. Click **Browse resources** to browse your resources. Resources are then counted and listed.
3. From the list, select the target application and copy its information.

In the web console, paste the information you copied by clicking **Paste resource info**. See Add an application.

Icons

When setting the icon for an application in the web console, you can add new icons. To get data for an icon, complete the following steps:

1. Click **Browse** to browse to a file that contains the icon. Icons in the file are then loaded. Supported file types: `.exe`, `.dll`, `.ico`.
2. Select the icon and copy the icon data.

In the web console, paste the icon data you copied by clicking **Paste icon data**. See Add an application.

Start Menu Configurator for Windows 11

Use this tool to configure Start menu layouts for Windows 11 and generate configurations in JSON format that you can assign as actions in the management console.

To customize the Start menu layout for Windows 11, complete the following steps.

1. Click **Start Menu Configurator for Windows 11** in Citrix Environment Tool Hub. Select applications that you prefer to add to the **Pinned** section of the **Start** menu and arrange the layout as needed.
2. Click **Generate configuration** and copy the result.
3. In the web console, click **Add a new JSON object** and select **Start menu configuration for Windows 11**. Paste the configuration in the **Add JSON object** page and click **Done**.
4. Assign JSON file configuration to the users by selecting the required assignment target in the **Manage assignments** page and click **Save**.

Add applications

To add applications using Citrix Environment Tool Hub, complete the following steps.

1. Click **Add applications** in the **Start Menu Configurator for Windows 11** page.
2. Choose the applications from the **Add applications** page by selecting the required applications that you intend to add to the Start menu, and click **Add**.

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

3. You can change the order of the applications by dragging the applications as needed under the **Pinned** layout section.
4. Click **Generate configuration** and after the configuration is generated, click **Copy**. While generating the configuration, the selected layout is applied to the Start menu.

Windows Logon analysis

You can use this tool to view logon duration reports and get the tips for logon duration optimization and troubleshooting.

To receive complete reports, **enable log collection** for relevant Windows event logs on the machine.

- Click **Windows Logon analysis > Get reports** to access the **Get latest reports** wizard.
- Select the time range by choosing one of the options from the drop down list and click **Get reports**. The default range is **Last 24 hours**.
- The phase and description are displayed in the form of a chart based on the following table.

The following table lists all the metrics, submetrics, and tips in detail.

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
Pre-logon	Time taken before windows logon.	-	Citrix pre-logon	Pre-Windows Duration	-
			HDX connection	-	-
Authentication	Time taken to complete authentication to the session.	• **Use Windows Hello:** Windows	Session Arbitration	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		Hello is a biometric authentication feature that allows you to log in to your PC using your face or fingerprint. • **Network/ Active Directory Speed:** Please ensure that	Network Provider	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		there is a good network communication between the current machine and the Active Directory. You can use tool to check it, such as Dcdiag).	Windows authentication	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		• **Efficient Input of Username and Password:** Incorrect or delayed input of username and password can lead to an overall extension of the authenticati	VDA authentication	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		on time.			
Citrix RSOP	Time taken to complete Citrix RSOP(Resultant Set of Policy).	-	-	-	-
User profile Loading	Time taken to load the profile settings for the user logging on.	• **Check for low disk space and free up space:** If your hard drive is almost full, it can slow down your PC's	Temp File Traverse	-	This metric is available only when a PML exists.

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		login process. Make sure you have enough free space on your hard drive. • **Use Proc Mon tool:** To analyze the details, use Proc Mon tool to capture the file IOs	User profile	Time taken to load Windows user profile files and settings.	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		inside user profiles during user logon. • **Citrix Profile Management:** If you are using Citrix Profile Management, you can optimize the logon process by either	SMB client	Time taken to initialize the SMB client for remote connections.	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		using container-based solution or using file-based solution with Profile streaming for folders and Accelerate folder mirroring enabled. Learn more • **Use Citrix WEM**	Citrix Profile Management	Time taken to process Profile Management setting.	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		to configure Profile Management health check: Workspace Environment Management (WEM) can check whether Citrix Profile Management is config	Citrix Layering Service	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		ured optimally on your agent machine. Learn more	Default Profile Replication	Time taken to copy the Default User profile during the user's first logon.	This metric is available only for the first logon.
			FSLogix load profile	Time taken to load FSLogix profile container.	-
Group Policy Processing	Time taken to process Group Policy settings.	• **Disable the GPO cache:** Run gpedit.msc and locate to path: "Computer Configuration >	Folder redirection	Time taken to apply folder redirection policies and link user folders to the network location.	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		Administrative Templates > System > Group Policy" then disable the GPO cache. • **Decrease the number of GPOs:** Decrease the number of GPOs that are	Wmi Filter	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		processed at once: Group Policy processing is done in parallel, but there are limits to how many GPOs can be processed simultaneously. Decreasing the numb	Winlogon notification packages	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		er of GPOs that are processed at once can help speed up Group Policy processing. • **Use Citrix WEM to process group policy asynch:** Use Citrix WEM to	Logon scheduled task	Time taken to run the Group Policy Scheduled Task.	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		process group policy async, it can process group policy before user logon and make group policy processing faster. Learn more. The Current processing status of Wind	Single Logon Scheduled Task	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		ows group policy is sync.	Group Policy Script	-	-
			Group Policy Script (Async)	-	-
			Group Policy Cse	Time taken to process Group Policy Client Side Extension .	-
			Group Policy	-	-
			Group Policy Cache Write	Time taken to write group policy to local.	-
			Citrix WEM total time	-	-
			Citrix WEM User Group Policy	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
			Citrix WEM Machine Group Policy	-	-
			Citrix WEM Read Configuration	-	-
			Citrix WEM startup scripted tasks	-	-
			Citrix WEM cache (Sync)	-	-
			Citrix WEM Checking Host Service Status	-	-
			Citrix WEM Json File	-	-
			Citrix RSOP	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
			Group policy objects	Time taken to load group policy objects.	-
Pre-shell (Userinit)	Time from the "userinit.exe" to the "explorer.exe" startup.	-	-	-	-
Logon script processing	Time taken to run logon scripts.	• **Optimize your logon script:** You can optimize your logon script by removing unnecessary	User Logon Script	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		commands and reducing the size of the script. • **Use Group Policy Preferences:** Group Policy Preferences can be used to replace logon scripts. They are			

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		easier to manage and can be processed faster than logon scripts. • **Use Citrix WEM external tasks:** Set up your logon scripts using external tasks. You can specif			

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		y whether to wait for the task to complete and how long the wait timeout is. Limiting the wait time helps speed up user logon. To learn more about external			

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		tasks, see the product documentation.			
Shell startup	Time taken to run shell startup.	• **Disable startup programs:** You can disable the programs that automatically launch when you turn on your	Shell Start	Time taken to run the shell after loading the windows user profile	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		PC. To disable startup programs on Win11/Win10/Win Server 2022, use these steps: 1. Press the **Windows + I** short cut to open **Settings**, and then select	FSLogix Shell Start	Time taken to run the shell after loading the FSLogix profile container.	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		Apps > Start up. 2. Turn off apps or programs that you don't want to start automatically. 3. Remove unnecessary programs from the global startup folder	Active setup	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		: `%allusersprofile%\Microsoft\Windows\Start Menu\Programs\StartUp`. 4. Remove unnecessary programs from the user startup folder: `%userprofile%`	Appx associations	-	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		`\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`. • **Disable startup programs:** Fast startup is a feature that allows your computer to start	Appx load packages	Time taken to load AppX packages.	-

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		up faster after shutdown. To enable fast startup on Windows 10, use these steps: 1. Open **Control Panel** in **Icon view** and choose **Power Options**. 2. Click **Choo**			

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		se what the power buttons do in the sideb ar. 3. Unde r **Shut down settin gs**, select the **Turn on fast start up** check box. • **Disa ble start up progr ams:** Adjus t the			

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		appearance and performance of Windows. To do this, 1. Right-click **My Computer** and select **Properties**. 2. Select **Advanced system settings**. 3. Under **Performan**			

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

BASE-METRIC	BASE-METRICS DESCRIPTION	TIPS	SUB-METRICS	SUB-METRICS DESCRIPTION	DETAILS
		ce, select **Settings**. 4. Adjust the options to improve appearance and performance.			

Process activity and details

The process activity data captured with Process Monitor during user logon can provide additional information and help administrators identify issues that cause slow logons. This feature incorporates the process data into the logon reports and allows administrators to examine the process activity in the context of user logon. **Citrix Environment Tool Hub** auto triggers and stops the **Windows Process Monitor** application after configuring the **Process Monitor** settings in the **Windows Logon Analysis** tool.

To collect the process data during user logon, complete the following steps.

- Use the main session to configure **Process Monitor** settings in the **Windows Logon Analysis** tool. This session starts the **Process Monitor** application automatically with special settings, where you can also automatically stop the Process Monitor application.
- Trigger the target user logon in the sub-session.

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

- Generate and analyze the logon report in the main session that includes the related process activities in it.

User Store Creation Tool

Use this tool to create the user stores with Citrix Profile Management on the current machine or a different machine. You can specify the folder path and share the name for a user store. When the user store is created, the recommended configuration for the path to the user store is provided, allowing you to use it directly in your **Profile Management** settings.

To create a user store on the current machine or a different machine, follow these steps:

1. Specify the machine on which you want to install the user store:
    - To create a user store on a different machine, specify the machine name and enter the credentials of a domain user with the local administrator privilege on that machine. Make sure that the PowerShell remoting is enabled on the machine.
    - To create a user store on the current machine, skip this step.
2. Specify the **Folder path** that you want to set as the user store location.
3. Choose **Stop and let me know** or **Use the existing folder**, if the folder exists.
4. Optionally, specify a name for the file share. By default, the name of the folder is used as the share name.
5. Choose **Stop and let me know** or **Stop sharing the existing item and take the name**, if a share with the same name exists.
6. (Optional) By default, the **Administrator** group is granted full control access to this user store. To give full control to more users or groups, follow these steps:
    a. In the **User store administrators (optional)** section, click **Add**. The native AD selector appears.
    b. Select **Users or Groups** as the object type.
    c. Specify the names of the users or groups in the **Enter the object names to select** field.
    d. Click **OK**.
7. Click **Create user store**.

Errors

The following error messages appear in the related sections.

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

- Incorrect user credentials
- Insufficient user privilege
- Folder already exists
- Share name in use

If you receive an error message apart from the ones listed, you can view the error details at the bottom of the page with the title **An error occurred. View details below**.

To create another user store, click **Create another**. This choice redirects you to the starting page with all the inputs cleared and reset.

File Info Viewer

You can now use Citrix Environment Tool Hub to quickly retrieve data such as that of path, publisher, and hash value to configure an executable rule in the web console. The process includes the following steps:

- Select **Citrix Environment Tool Hub** > **All Tools** > **File Info Viewer**.
- Choose a file or folder to get its relevant information.
- Copy the data from one of the criteria, such as, path information, publisher information, or file hash.
- Paste the data in the **Create Windows installer** rule page.

File Type Association Assistant

Use this tool to get the information needed for configuring FTAs to add them as assignable actions in the management console.

Selecting **File Type Association Assistant** leads you to the **File Type Association Assistant** page in Citrix Environment Tool Hub. You can configure an FTA by completing the following steps.

- When you type a file name extension, you can choose from the matching file name extension options that begins with your input.
- Check if the extension entered has an associated **ProgID** and whether the **ProgID** has associated actions in the registry.
- Click **Browse** to list all the applications that have the entered **ProgID** registered.
- Configure the application that you want to associate it with.
- You can also select **Customize action** to perform the **Open**, **Edit**, and **Print** actions.

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

- You can copy the configured FTA data by clicking the **Copy** button.

For more details, see File Type Associations.

Printer Assistant

Use this tool to get a list of printers from your print server so that you can add them as assignable actions in the management console.

When adding printers from a network print server, you need printer information to add them. To get the printer information, complete the following steps:

1. Enter the full name of the print server.
2. Specify whether to connect to the print server using specific credentials.
3. Click **Connect** to view the printer list.
4. Select one or more printers from the list and copy the printer information.

In the web console, paste the information you copied by clicking **Paste printer info**. See Add printers from a print server.

Profile Migration Tool

Use this tool to migrate other profiles to the Citrix container-based profile solution. The process includes the following steps:

1. Select any of the following source profiles:
    - **FSLogix profile container**
    - **Citrix file-based solution**
    - **Windows roaming profile**
    - **Local machine**
2. Configure the location of the source profiles:
    a. If you chose **FSLogix profile container** in step 1, configure this field:
        - **VHD location**: Enter the file share location where FSLogix profiles are stored. (*Example*: `\\<storage-account-name>.file.core.windows.net\<share-name>`). Or, click **Browse** and select the file share.
    b. If you chose **Citrix file-based solution** or **Windows roaming profile** in step 1, configure these fields:

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

- **File share**: Click **Browse** and select the required source file share location or directly enter the location.
- **Subpath**: If you are not using the default container folder, enter the subpath.

> **NOTE:**
>
> If you chose **Local machine** in step 1, skip this step because Profile Migration Tool automatically retrieves the default configuration of the local machine profiles.

3. Configure the location of the target Citrix user store:
   - **File share**: Click **Browse** and select the required target file share location or directly enter the location.
   - **Subpath**: Enter the required target subpath.
4. Click **Check access** to verify the required permissions. This action performs the following checks:
   - Verifies if your current account or the alternate account has read access to the source and full control over the target file share.
   - Verifies that the target file share meets the permission requirements for Citrix Profile Management. For more information, see this Microsoft article.

   If your current account doesn't have sufficient access, select the **Use alternate credentials** checkbox to enter the alternate username and password. If the target Citrix user store doesn't meet the security requirements, click **Add permissions** to grant the necessary permissions.
5. Specify the users and groups whose profiles are to be migrated. If no users or groups are specified, all the profiles in the source location are migrated.
6. Select the **OS version** of the source profiles.
7. Click **Start migration**.

   Profile Migration Tool migrates one profile at a time. If you choose to stop the migration, click **Stop**. This action completes the migration for the current profile and stops the migration for the remaining profiles. You can choose to retry the migration by clicking **Retry selected**. Otherwise, to perform another migration, click **Do another migration**.

   If there is a failure, you can click **View log** to see the error logs. You have the option to retry the migration for failed profiles by clicking **Retry selected**.

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

Rule Generator for App Access Control

Use this tool to generate rules for App Access Control or Redirection. The general workflow is as follows:

1. Create rules
2. To reuse existing configurations in FSLogix, Import FSLogix rule sets and edit them to quickly create equivalent App Access Control rules.
3. Generate raw data for rules
4. Validate rules

NOTE:

You must use the App Access Control policy in Citrix Profile Management to enforce these rules. For more information, see App access control.

About the rules

You can use this tool to create the following rules:

- **Hide rules**. Control user access to files, folders, registry values, and keys.
- **Redirect rules**. Redirect files, folders, and registry values and keys for users.

The rules are implemented through Citrix Profile Management. Typical use cases include:

- Control user access to apps installed on machines — whether to make apps invisible to relevant users.
- Implement data roaming. Redirect non-user-profile data to a file share, ensuring users can access the same data regardless of which machines they sign into.
- Enhance data protection. Redirect critical data to alternative locations or values, protecting it from unauthorized access.
- Customize the user experience. Tailor app experience based on specific requirements.

Create rules

To create a rule for app access control or redirections, complete the following steps:

1. Click **Create rule** in the action bar, and then select **Hide** or **Redirect**.
2. On the **Rule details** page, configure the following settings:

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

- **App rule name**. Specify a name to help you identify the rule.
- **Objects to hide**. Add target objects. Target objects can be files, folders, and registry keys and values related to the app that you want to hide. Click **Scan** for apps installed on the current machine and objects associated with each app.
- **Redirections**. You can redirect files, folders, and registry values and keys. For each redirection, specify the source and destination paths.

NOTE:

- You cannot add paths for items on which certain Citrix and Windows services rely. Otherwise, those services might stop working properly. For a complete list of those paths, see Paths not allowed to be added.

3. On the **Assignments** page, add users, computers (organizational units), and processes you want to assign the rule to.

   a. Select an assignment type from Users, Machines, or Processes.

   b. In the **Apply to** section, specify the assignment objects. If no objects are selected, the rule applies to all objects of that assignment type.

   c. To specify exclusions, go to the **Exclude** section and add the necessary assignment objects.

   d. If needed, repeat steps a to c for another assignment type.

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

NOTE:

- Without assignments specified, this rule always takes effect on the target objects.
- Assignments come in three categories: users, computers, and processes. The `OR` operator is used between items within a category, and the `AND` operator is used between categories.
- You cannot add users and computers when running the tool on a non-domain-joined or Azure Active Directory joined machine.
- You can add bulk processes. Enter process names (including the .exe extension), separated by line breaks.
- To assign rules to the AAD users or groups and NDJ machines, use the **AAD/NDJ object selector** in the WEM web console to select the target objects. For more information, see Assign app access rules to AAD users/groups and NDJ machines.

4. After you finish, click **Done**.

Paths not allowed to be added

You cannot add the following paths and their parent paths for items on which certain Citrix and Windows services rely.

Profile Management related registries:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\UserProfileManager`
- `HKLM:\SOFTWARE\Policies\Citrix\UserProfileManager`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\UserProfileManager`
- `HKLM:\SOFTWARE\Citrix\UserProfileManager`

WEM related registries:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Norskale`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\WEM`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale`
- `HKLM:\SOFTWARE\Policies\Norskale`
- `HKLM:\SOFTWARE\Citrix\WEM`
- `HKLM:\SYSTEM\CurrentControlSet\Control\Norskale`

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

Virtual Delivery Agent (VDA) related registries:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`
- `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`

Windows related registries:

- `HKCU:`
- `HKEY_CURRENT_USER`
- `HKU:`
- `HKEY_USERS`

Windows and Citrix service related folders:

- `c:\windows\system32`
- `\Citrix\User Profile Manager\`
- `\Citrix\Workspace Environment Management Agent\`
- `\Citrix\XenDesktopVdaSetup\`
- `\%windir\%\system32`

Generate raw data for rules

To have Citrix Profile Management enforce the configured rules, you must first generate their raw data and then enter it into the **App access control** policy setting in Profile Management using GPO or WEM.

To generate raw data for rules, follow these steps:

1. Select the desired rules or click **Select all** to select all rules.
2. Click **Generate raw data** in the action bar. The raw data is then generated for the selected rules.
3. In the **Generate raw data** window, save the raw data to a file for later restoration or copy the raw data to your clipboard.

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

NOTE:

- Use the raw data when adding rules in the WEM administration console or when configuring the Profile Management policy **App access control**, depending on how you want to get the rules deployed.
- After you save the raw data to a file, you can restore the rules from the file. To achieve that, use **Import** in the action bar.

4. After you finish, click **Done**.

Validate rules

You can validate the app access control rules on the local machine before deploying in the testing or production environment.

To test app access rules, complete the following steps:

1. Select the desired rules or click **Select all** to select all rules.
2. Click **Test** in the action bar.

    a. Click **Deploy to local machine** to deploy the selected rules to the local machine and verify if the rules are working as expected. Click **Deploy** on the popup window to confirm the action.

    NOTE:

    While testing the app rules, the rules affect only the current user.

    b. Click **Clear deployed rules from local machine** to clear deployed app access control rules from the local machine.

Import FSLogix rule sets

Import FSLogix rule sets to reuse existing configurations and quickly create equivalent App Access Control rules.

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

NOTE:

Some rule types and assignment types used in FSLogix aren't supported by app access control. Review your environment and consider alternative configurations where necessary.
To import FSLogix rule sets:

1. Click **Import > FSLogix Apps Rule Set** to begin the import.
2. Click **Browse**, locate the FSLogix Rule definition file that was saved using the FSLogix Rule Editor, and then click **Open**.

   NOTE:

   Make sure the Rule definition file and its associated Assignment file are stored in the same folder. The tool migrates supported rule sets along with their assignments.

3. When the migration completes, review the details.

   Check for any unsupported rules or data, and validate the results. You can edit or add rules after migration.
4. Click **Import** to finalize the process.

The imported rules are now available for testing and can be saved along with your existing rules.

Assign app access rules to AAD users/groups and NDJ machines

To assign app access rules to AAD users or groups and NDJ machines, complete the following steps.

1. In the WEM web console, select **Configuration Sets** > Your site name > **Profiles** > **Profile Management Settings** > **App access control**.
2. Select the **Enable app access control** checkbox and click **Add rules**.
3. On the **Rules** page, click **AAD/NDJ object selector** to add the desired AAD users and NDJ machines.
4. Copy the user or machine data.
5. Go to **Citrix Environment Tool Hub** > **Rule Generator for App Access Control**, where you create an app rule.
6. Go to the **Assignments** page, and paste the data.

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

7. Click **Done** to create the app access control rules.
8. Copy the app access control rules.
9. Go to the WEM web console. Select **configure set** > Your site name > **Profile Management settings** > **App access control** and paste the data there.

Profile Cleanup Tool

Use this tool to delete or archive inactive user profiles in the user stores. This tool helps you reclaim disk space, improve security, and ensure compliance with data retention policies.

Typical use cases include:

- Offboarding employees: Remove profiles of employees who have left your organization.
- Managing inactive accounts: Delete or archive profiles of users who haven't logged on for a specified period.
- Addressing storage limitations: Free up disk space by identifying and removing unnecessary profiles.
- Enhancing security: Remove sensitive data from inactive or compromised accounts.

To clean user profiles, follow these steps:

1. Run the tool.

   Sign in to a machine where Citrix Environment Tool Hub is installed. Run the tool hub as an administrator, and click **Profile Cleanup Tool** to open its UI.
2. Specify the locations of the user stores.

   Enter the paths to the user stores where you want to clean up user profiles.

   TIP:

   If the machine is configured with the Citrix Profile Management settings, click the **Load from local registry** link to auto-fill the profile location fields.

FIELD	DESCRIPTION
Path to user store	Enter the full path to the user store. For more information, see Specify the path to the user store.

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

FIELD	DESCRIPTION
Path to replicated user stores (optional)	If replicated user stores are deployed, enter their paths, separated by line breaks (Press **Enter** after each path). For more information, see Replicate user stores.
Customized storage path for VHDX files (optional)	If VHDX files are stored in a path other than the user store, enter that path. For more information, see Specify the storage capacity and path for VHD containers.

3. Check your access to the specified user stores.

   Click **Check access** to verify that your user account has *Read and Write* permission to the specified locations. If your account lacks access, select **Use a different account**, enter a valid user name and password, and click **Check access** again.

4. Search for profiles.

   a. Click **Find profiles**. The **Find profiles** page opens.

   b. Enter search criteria such as partial user name, last logon time, last write time, and AD user status.

   c. click **Find profiles**. The search begins and can take time if the user store contains many profiles.

   NOTE:

   If more than 200 profiles are found, only the first 200 appear in the search results. For larger numbers of profiles, we recommend operating in batches.

5. Delete or archive profiles.

   a. Select one or more user profiles from the search results.

   b. Click the appropriate action button and follow the onscreen instructions to complete the action:

   - **Delete**: Delete the selected user profiles.
   - **Archive**: Move the selected user profiles from the user store to a location that you specify.

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

> **NOTE:**
>
> To archive user profiles, the account you're using must have *Write* permission to the target location.

After the operation is complete, you can:

- Click **Done** to clear the **Find profiles** results and return to the **Check access** status.
- Click **Back to search results** to return to the **Find profiles** results, with successfully processed users removed.
- If there are failed results:
  - Click **Details** next to a failed result to view errors encountered during the operation.
  - Click **Retry failed** to retry the operation on the failed results.

Scripted Task Validator

The Scripted Task Validator tool lets you:

- Validate scripted tasks by running them on a WEM Agent machine and reviewing results
- Export scripted tasks for later import into the WEM Web console

Validate and export a scripted task

Use the **Scripted Task Validator** tool to run a scripted task and review the execution results. If needed, export the task for later import into the WEM Web console.

1. Click **Open Script** to load a locally prepared PowerShell script. Alternatively, select a recently opened script from the **Recent** list.
2. Update the script within the code editor as required. See Edit a scripted task.
3. Go to the **Configuration** tab and configure the following settings. See Configure a scripted task.
   - Permissions
   - Verify signature before running the script
   - Working folder
   - Output files
   - Input parameters

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

- Timeout value

4. Click **Run** to verify script content.
5. View **Output** console.
6. Click **Export**.
7. In the **Export script** wizard, configure the following settings and then click **Save**.
   - **Include all other files in the same folder**. Optionally, choose whether to include all files in the same directory when exporting.
   - **Add signature**. Optionally, choose whether to sign the file when exporting.

     NOTE:

     Select a certificate installed in the local certificate store. The certificate must contain a private key and support code signing.
8. Click **Export**.

VHD Expansion Tool

Use this tool to increase the capacity of a VHDX file that stores user profile data or other data, such as Outlook or OneDrive content.

To expand a VHDX file, follow these steps:

1. Open the tool from the Tool Hub.
2. Specify the full path to the VHDX file. You can paste the file path directly or click **Browse** to locate the file using File Explorer.
3. Click **Check disk status**. This action retrieves the VHDX metadata, verifies that the file is accessible, and displays its current capacity.
4. Enter the new capacity for the VHDX file.
5. Click **Expand** to apply the change. The tool updates the VHDX file to reflect the new capacity.

Add local applications for quick access

Add local applications to the Citrix Environment Tool Hub for quick access. Added applications are treated as part of your personal data and are retained when you switch machines in a Profile Management environment.

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

To add local applications:

1. Under the **Local apps** tab, click **Add local app**.
2. Navigate to and select one or more applications.

To add local Citrix applications, such as Citrix Virtual Desktop Agent, Citrix Workspace, and Citrix Workspace Environment Management Console:

1. Under the **Local apps** tab, click **Scan for Citrix components**.
2. Review the names and paths of the applications detected by the scan.
3. Select the applications that you want to add.

NOTE:

To remove an added application, click the trash can icon.

Common Control Panel applets

The following Control Panel applets are common in Windows:

Applet name	Canonical name
Action Center	Microsoft.ActionCenter
Administrative Tools	Microsoft.AdministrativeTools
AutoPlay	Microsoft.AutoPlay
Biometric Devices	Microsoft.BiometricDevices
BitLocker Drive Encryption	Microsoft.BitLockerDriveEncryption
Color Management	Microsoft.ColorManagement
Credential Manager	Microsoft.CredentialManager
Date and Time	Microsoft.DateAndTime
Default Programs	Microsoft.DefaultPrograms

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

Device Manager	Microsoft.DeviceManager
Devices and Printers	Microsoft.DevicesAndPrinters
Display	Microsoft.Display
Ease of Access Center	Microsoft.EaseOfAccessCenter
Family Safety	Microsoft.ParentalControls
File History	Microsoft.FileHistory
Folder Options	Microsoft.FolderOptions
Fonts	Microsoft.Fonts
HomeGroup	Microsoft.HomeGroup
Indexing Options	Microsoft.IndexingOptions
Infrared	Microsoft.Infrared
Internet Options	Microsoft.InternetOptions
iSCSI Initiator	Microsoft.iSCSIInitiator
iSNS Server	Microsoft.iSNSServer
Keyboard	Microsoft.Keyboard
Language	Microsoft.Language
Location Settings	Microsoft.LocationSettings
Mouse	Microsoft.Mouse
MPIOConfiguration	Microsoft.MPIOConfiguration
Network and Sharing Center	Microsoft.NetworkAndSharingCenter
Notification Area Icons	Microsoft.NotificationAreaIcons
Pen and Touch	Microsoft.PenAndTouch

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

Personalization	Microsoft.Personalization
Phone and Modem	Microsoft.PhoneAndModem
Power Options	Microsoft.PowerOptions
Programs and Features	Microsoft.ProgramsAndFeatures
Recovery	Microsoft.Recovery
Region	Microsoft.RegionAndLanguage
RemoteApp and Desktop Connections	Microsoft.RemoteAppAndDesktopConnections
Sound	Microsoft.Sound
Speech Recognition	Microsoft.SpeechRecognition
Storage Spaces	Microsoft.StorageSpaces
Sync Center	Microsoft.SyncCenter
System	Microsoft.System
Tablet PC Settings	Microsoft.TabletPCSettings
Taskbar and Navigation	Microsoft.Taskbar
Troubleshooting	Microsoft.Troubleshooting
TSAppInstall	Microsoft.TSAppInstall
User Accounts	Microsoft.UserAccounts
Windows Anytime Upgrade	Microsoft.WindowsAnytimeUpgrade
Windows Defender	Microsoft.WindowsDefender
Windows Firewall	Microsoft.WindowsFirewall
Windows Mobility Center	Microsoft.MobilityCenter
Windows To Go	Microsoft.PortableWorkspaceCreator

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

Windows Update	Microsoft.WindowsUpdate
Work Folders	Microsoft.WorkFolders

Dynamic tokens

You can use dynamic tokens in any Workspace Environment Management actions to make them more powerful.

You can use dynamic tokens in the following fields:

- Group Policy settings
  - With **Action** set to **Delete** value: **Value**
  - With **Action** set to **Set value** and **Type** set to **REG_SZ: Value, Data**
  - With **Action** set to **Set value** and **Type** set to **REG_EXPAND_SZ: Value, Data**
  - With **Action** set to **Set value** and **Type** set to **REG_MULTI_SZ: Value, Data**

NOTE:

Group Policy settings come in two types: Machine settings and user settings. For machine settings, some dynamic tokens are not supported. See Dynamic token support for Group Policy settings.

Dynamic token support for Group Policy settings

Using dynamic tokens in Group Policy settings allows for more adaptable policy configuration in different environments, reduces manual configuration, and simplifies policy management.

Group Policy settings come in two types:

- **Machine settings**. Those settings apply only to machines regardless of who logs on to them.
- **User settings**. Those settings apply only to users regardless of which machine they log on to.

All dynamic tokens are supported for Group Policy settings. The following ones are not supported for machine settings.

- Hashtags

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

    - ##FullUserName##
    - ##UserInitials##
    - ##ClientName##
    - ##ClientIPAddress##
    - ##UserLDAPPath##
    - ##ClientRemoteOS##

- ADAttribute
    -
- Registries under HKCU

Applications

- With **Installation application** as the application type: **Command Line**, **Working Directory**, and **Parameters**
- With **File/Folder** as the application type: **Target**
- With **URL** as the application type: **Shortcut URL**
- **Icon File**

Printers

- **Target Path**

Network drives

- **Target Path** and **Display Name**

Virtual drives

- **Target Path**

Registries

- **Target path**, **Target name**, and **Target value**

NOTE:

The **Target value** field does not support environment variable expansion. If you use environment variables, they do not work as expected.

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

Environment variables

- **Variable value**

Ports

- **Port Target**

Ini files

- **Target path**, **Target section**, **Target value name**, and **Target value**

> **NOTE:**
>
> The **Target section**, **Target value name**, and **Target value** fields do not support environment variable expansion. If you use environment variables, they do not work as expected.

External tasks

- **Path** and **Arguments**

File system operations

- **Source Path** and **Target Path**

Certain filter conditions

- Example: With **Active Directory Attribute Match* as the condition type: **Tested Active Directory Attribute** and **Matching Result**

> **NOTE:**
>
> For a complete list of supported fields for filter conditions, see Supportability matrix for filter conditions.

String operations

Sometimes you need to manipulate strings within a script to map drives or launch applications. The following string operations are accepted by the Workspace Environment Management™ agent:

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

MODAL	DESCRIPTION	EXAMPLE
#Left(string,length)#	Returns the specified number of characters on the left.	`#Left(abcdef,2)#` returns `ab`
#Right(string,length)#	Returns the specified number of characters on the right.	`#Right(abcdef,2)#` returns `ef`
#Truncate(string,length)#	If the length of the string is less than or equal to the specified length, returns the entire string. If the length of the string is greater than the specified length, returns the specified number of characters on the left.	`#Truncate(abcdef,3)#` returns `abc`
&Trim(string)&	Removes all leading and trailing blank spaces of the string.	`&Trim( a b c )&` returns `a b c`
&RemoveSpaces(string)&	Removes all blank spaces of the string.	`&RemoveSpaces( a b c )&` returns `abc`
&Expand(string)&	If the string contains an environment variable that is enclosed with \%, expands the variable.	`&Expand(%userprofile%\destop)&` returns `C:\Users\Jill\desktop`
\$Split(string, splitter],index)\$	Splits the string into substrings based on the splitter that is enclosed with [] and returns the indexed substring.	`$Split(abc-def-hij,[-],2)$` returns `hij`
#Mid(string,startindex)#	Starts at the specified index in the string and returns all characters after it.	`#Mid(abcdef,2)#` returns `cdef`
!Mid(string,startindex,length)!	Starts at the specified index in the string and returns the specified number of characters.	`!Mid(abcdef,1,2)!` returns `bc`

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

MODAL	DESCRIPTION	EXAMPLE
!Substring(string,startindex,length)!	Starts at the specified index in the string and returns the specified number of characters.	`!Substring(abcdef,1,2)!` returns `bc`
#Mod(string,length)#	Divides the string by the length and returns the remainder. The string must be able to be converted to an integer.	`#Mod(7,3)#` returns `1`

NOTE:

- String operations are also supported with hashtags and Active Directory attributes. For example: `#Left([ADAttribute:NAME],2)#` where the name attribute of the current domain user is `Administrator` returns `Ad`, and `$Split(##ClientIPAddress##,[\.],2)$` returns `157`.
- `!Mid(string,startindex,length)!` and `!Substring(string,startindex,length)!` operations are always performed last.

Hashtags

Hash-tags are a replacement feature widely used in the processing of Workspace Environment Management items. The following example illustrates how you use hash-tags:

To write to an **.ini** file, you can use **%UserName%** in the **.ini** file's path and Workspace Environment Management processes it and expands the final directory. However, assessing the value which Workspace Environment Management writes in the **.ini** itself is more complicated: you may want to write **%UserName%** literally, or write the expanded value.

To increase flexibility, **##UserName##** exists as a hash-tag, so that using **%UserName%** for a value writes it literally and **##UserName##** writes the expanded value.

See the following table for examples:

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

MODAL	DESCRIPTION	EXAMPLE
##UserName##	Returns the expanded environment variable "%username%"	Jill
##UserProfile##	Returns the expanded environment variable "%userprofile%"	C:\Users\Jill
##FullUserName##	Returns the user's full name in Active Directory	Jill Chou
##UserInitials##	Returns the user name initials in Active Directory	JC
##UserAppData##	Returns the actual path of the special folder - RoamingAppData	C:\Users\Jill\AppData\Roaming
##UserPersonal##	Returns the actual path of the special folder - Documents	C:\Users\Jill\Documents
##UserDocuments##	Returns the actual path of the special folder - Documents	C:\Users\Jill\Documents
##UserDesktop##	Returns the actual path of the special folder - Desktop	C:\Users\Jill\Desktop
##UserFavorites##	Returns the actual path of the special folder - Favorites	C:\Users\Jill\Favorites
##UserTemplates##	Returns the actual path of the special folder - Templates	C:\Users\Jill\AppData\Roaming\Microsoft\Windows\Templates
##UserStartMenu##	Returns the actual path of the special folder - StartMenu	C:\Users\Jill\AppData\Roaming\Microsoft\Windows\Start Menu
##UserStartMenuPrograms##	Returns the actual path of the special folder - Programs	C:\Users\Jill\AppData\Roaming\

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

MODAL	DESCRIPTION	EXAMPLE
		Microsoft\Windows\Start Menu\Programs
##UserLocalAppData##	Returns the actual path of the special folder - LocalAppData	C:\Users\Jill\AppData\Local
##UserMusic##	Returns the actual path of the special folder - Music	C:\Users\Jill\Music
##UserPictures##	Returns the actual path of the special folder - Pictures	C:\Users\Jill\Pictures
##UserVideos##	Returns the actual path of the special folder - Videos	C:\Users\Jill\Videos
##UserDownloads##	Returns the actual path of the special folder - Downloads	C:\Users\Jill\Downloads
##UserLinks##	Returns the actual path of the special folder - Links	C:\Users\Jill\Links
##UserContacts##	Returns the actual path of the special folder - Contacts	C:\Users\Jill\Contacts
##UserSearches##	Returns the actual path of the special folder - SavedSearches	C:\Users\Jill\Searches
##commonprograms##	Returns the actual path of the special folder - CommonPrograms	C:\ProgramData\Microsoft\Windows\Start Menu\Programs
##ComputerName##	Returns the machine's name	WIN10EN-LR3B66L
##ClientName##	Returns the client machine's name	W2K16ST-5IS28JP
##ClientIPAddress##	Returns the client machine's IP address	10.150.153.138
##IpAddress##	Returns the machine's IP address	10.150.153.213

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

MODAL	DESCRIPTION	EXAMPLE
##ADSite##	Returns the Active Directory site that the machine is a member of	NKG
##DefaultRegValue##	-	Always string.Empty
##UserLDAPPath##	Returns the current user's distinguished name	CN=Jill Chou,OU=User Accounts,OU=APAC,DC=citrite,DC=net
##VUEMAgentFolder##	Returns the agent folder	C:\Program Files (x86)\Citrix\Workspace Environment Management Agent
##RDSSessionID##	Returns the remote desktop session ID	2
##RDSSessionName##	Returns the remote desktop session name	RDP-Tcp#72
##ClientRemoteOS##	Returns the operating system of the machine used to connect to the virtual desktop	Windows
##ClientOSInfos##	Returns the machine's OS information	Windows 10 Enterprise 64-bit

Hash-tag **##UserScreenCaptureComment##** is implemented for use in specific parts of the product. This tag can be included in the Email Template under **Advanced Settings** > **UI Agent Personalization** > **Helpdesk Options**. When included, users are presented with a comment field located below the screen capture in the agent screen capture utility. The comment is included in the support email at the location at which you placed the tag in the email template.

Active Directory attributes

To work with Active Directory attributes, WEM replaces the value with the related Active Directory attribute. is the dynamic token for any Active Directory attributes. There is a related filter that checks the value of the specified attributes.

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

For user organizational unit (OU) structures, WEM replaces the value with the related Active Directory OU name. The Active Directory path is the complete user path (LDAP) in Active Directory and is a subset of it.

For example, suppose you want to build a network drive for an OU to which the users belong. You can use the dynamic token in the network drive path to resolve the users' OU dynamically. There are two ways to use the dynamic token:

- Use the dynamic token directly in the network drive path. For example, you can use the following path: `\\Server\Share\[UserParentOU:0]\`.
- Set an environment variable called OU, and then set its value to . You can then map the drive as `\\Server\Share\%OU%\`.

NOTE:

- You can substitute the digit "0" with the number that corresponds to the level you want to reach in the OU structure.
- You can append variables to the path. To do this, ensure that you have an exact folder structure that matches your OU layout.

You can also use Active Directory attributes for filtering purposes. On the **Administration > Filters > Conditions > Filter Condition List** tab, you can open the New Filter Condition window after you click **Add**. In the New Filter Condition window, you can see the following four filter condition types associated with Active Directory attributes:

- Active Directory Attribute Match
- Active Directory Group Match
- Active Directory Path Match
- Active Directory Site Match

For Active Directory Attribute Match, the dynamic token is . There is no dynamic token available for Active Directory Group Match because that condition type is used to check a group membership. For Active Directory Path Match, the dynamic token for the full LDAP path is ##UserLDAPPath##. For Active Directory Site Match, the dynamic token is ##ADSite##.

See the following table for examples:

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

MODAL	DESCRIPTION	EXAMPLE
[ADAttribute:attrName]	Returns the specified attribute of the domain user	`[ADAttribute:name]` returns `Administrator`
[PrinterAttribute:printername|attrName]	Returns the specified attribute of the specified domain printer	[PrinterAttribute:printer1|name] returns printer1
[UserParentOU: level]	Returns the specified level of the current user's parent OU	`[UserParentOU:1]` in `CN=Jill Chou,OU=User Accounts,OU=APAC,DC=citrite,DC=net` returns `APAC`

Registries

To work with a registry, WEM replaces the `[RegistryValue:<Registry path>]` value with the related registry value. For example, you can specify the following value:

-

XML files

To work with an XML file, WEM replaces the `[GetXmlValue:<XML path>|<tag name>]` value with the specific tag value in the XML file. The XML path can be an actual path or an environment variable that resolves to a path. You must enclose the environment variable with %. For example, you can specify the following value:

- \[GetXmlValue:C:\citrix\test.xml\|summary\] or
- \[GetXmlValue:%xmlpath%\|summary\]

INI files

To work with an .ini file, WEM replaces the `[GetIniValue:<INI path>|<section name in the .ini file>|<key name in the .ini.file>]` with the key value. The INI path can be an actual path or an environment variable that resolves to a path. You must enclose the environment variable with %. For example, you can specify the following value:

- \[GetIniValue:C:\citrix\test.ini\|PLD_POOL_LIC_NODE_0_0\|LicExpTime\] or
- \[GetIniValue:%inipath%\|PLD_POOL_LIC_NODE_0_0\|LicExpTime\]

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

More information

Supportability matrix for filter conditions

The following table lists all condition types whose tested value or matching result supports dynamic tokens.

CONDITION TYPE	TESTED VALUE	MATCHING RESULT
ComputerName Match	-	Yes
ClientName Match	-	Yes
Environment Variable Match	No	Yes
Registry Value Match	Yes	Yes
WMI Query Result Match	-	Yes
XenApp® Farm Name Match	-	Yes
XenApp Zone Name Match	-	Yes
XenDesktop® Farm Name Match	-	Yes
XenDesktop Desktop Group Name Match	-	Yes
Active Directory Attribute Match	Yes	Yes
Name or Value is in List	Yes	Yes
No ComputerName Match	-	Yes
No ClientName Match	-	Yes
No Environment Variable Match	No	Yes
No Registry Value Match	Yes	Yes
No WMI Query result Match	-	Yes

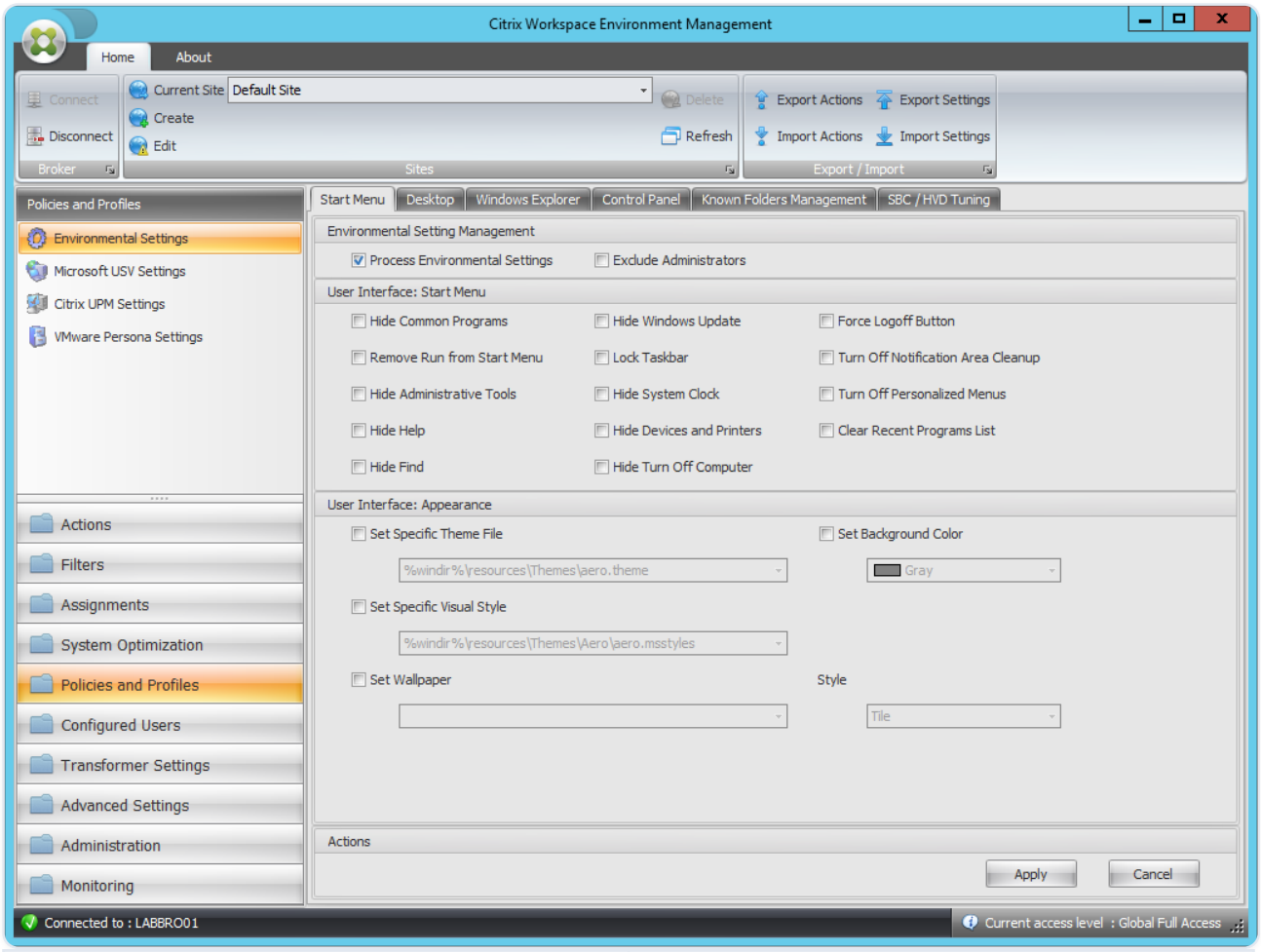
© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONDITION TYPE	TESTED VALUE	MATCHING RESULT
No XenApp Farm Name Match	-	Yes
No XenApp Zone Name Match	-	Yes
No XenDesktop Farm Name Match	-	Yes
No XenDesktop Desktop Group Name Match	-	Yes
No Active Directory Attribute Match	Yes	Yes
Name or Value is not in List	Yes	Yes
Dynamic Value Match	Yes	Yes
No Dynamic Value Match	Yes	Yes
File Version Match	Yes	Yes
No File Version Match	Yes	Yes
Published Resource Name	-	Yes
Name is in List	Yes	Yes
Name is not in List	Yes	Yes
File/Folder exists	-	Yes
File/Folder does not exist	-	Yes

Environmental Settings registry values

This article describes the registry values associated with Environmental Settings in Workspace Environment Management.

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



HIDE COMMON PROGRAMS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoCommonGroups
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

REMOVE RUN FROM START MENU	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`

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

REMOVE RUN FROM START MENU	
Value Name	NoRun
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

HIDE ADMINISTRATIVE TOOLS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`
Value Name	Start_AdminToolsRoot
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service called by agent

HIDE HELP	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoSMHelp
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

HIDE FIND	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoFind
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

HIDE WINDOWS UPDATE	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoWindowsUpdate
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

LOCK TASKBAR	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	LockTaskbar
Value Type	DWORD
Enabled Value	1
Disabled Value	0

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

LOCK TASKBAR	
Processing	Service at logon

HIDE SYSTEM CLOCK	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	HideClock
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

HIDE DEVICES AND PRINTERS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`
Value Name	Start_ShowPrinters
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service called by agent

HIDE TURN OFF COMPUTER	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoClose

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

HIDE TURN OFF COMPUTER	
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

FORCE LOGOFF BUTTON	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	ForceStartMenuLogoff
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

TURN OFF NOTIFICATION AREA CLEANUP	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoAutoTrayNotify
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

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

TURN OFF PERSONALIZED MENUS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	Intellimenus
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service at logon

CLEAR RECENT PROGRAMS LIST	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	ClearRecentProgForNewUserInStartMenu
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

SET SPECIFIC THEME FILE	
Parent Key	`HKCU\Software\Policies\Microsoft\Windows\Personalization`
Value Name	ThemeFile
Value Type	REG_SZ
Enabled Value	Path specified in console
Disabled Value	Value is absent

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

SET SPECIFIC THEME FILE	
Processing	Service at logon

SET BACKGROUND COLOR	
Parent Key	`HKCU\Control Panel\Colors`
Value Name	Background
Value Type	REG_SZ
Enabled Value	Configured color (R G B)
Disabled Value	Value does not exist or 0 0 0 if previously configured value
Processing	Service called by agent

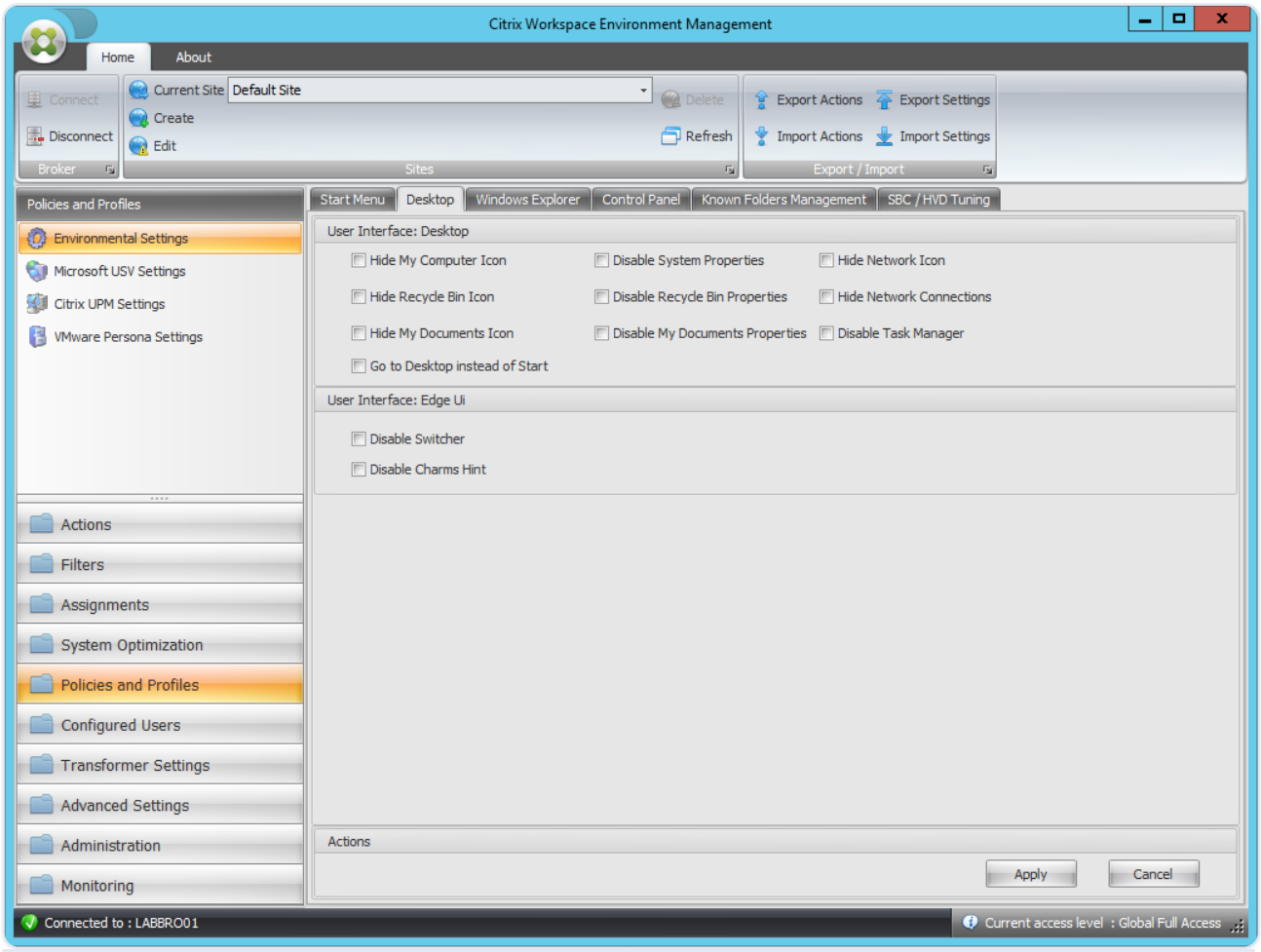
SET SPECIFIC VISUAL STYLE	
Parent Key	`HKCU\Software\Policies\Microsoft\Windows\Personalization`
Value Name	SetVisualStyle
Value Type	REG_SZ
Enabled Value	Path specified in console
Disabled Value	Value is absent
Processing	Service at logon

SET WALLPAPER	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System`
Value Name	Wallpaper
Value Type	REG_SZ

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

SET WALLPAPER	
Enabled Value	Path specified in console
Disabled Value	Value is absent
Processing	Service at logon
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System`
Value Name	WallpaperStyle
Value Type	REG_SZ
Enabled Value	Depends on Style value
Disabled Value	Value is absent
Processing	Service at logon
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System`
Value Name	TileWallpaper
Value Type	REG_SZ
Enabled Value	Depends on Style value
Disabled Value	Value is absent
Processing	Service at logon

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



HIDE MY COMPUTER ICON	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum`
Value Name	{20D04FE0-3AEA-1069-A2D8-08002B30309D}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

HIDE RECYCLE BIN ICON	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum`

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

HIDE RECYCLE BIN ICON	
Value Name	{645FF040-5081-101B-9F08-00AA002F954E}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

HIDE MY DOCUMENTS ICON	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum`
Value Name	{450D8FBA-AD25-11D0-98A8-0800361B1103}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

GO TO DESKTOP INSTEAD OF START	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage`
Value Name	OpenAtLogon
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service at logon

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

DISABLE SYSTEM PROPERTIES	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoPropertiesMyComputer
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

DISABLE RECYCLE BIN PROPERTIES	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoPropertiesRecycleBin
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

DISABLE MY DOCUMENTS PROPERTIES	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoPropertiesMyDocuments
Value Type	DWORD
Enabled Value	1
Disabled Value	0

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

DISABLE MY DOCUMENTS PROPERTIES	
Processing	Service called by agent

HIDE NETWORK ICON	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum`
Value Name	{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

HIDE NETWORK CONNECTIONS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoNetworkConnections
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

DISABLE TASK MANAGER	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System`
Value Name	DisableTaskMgr

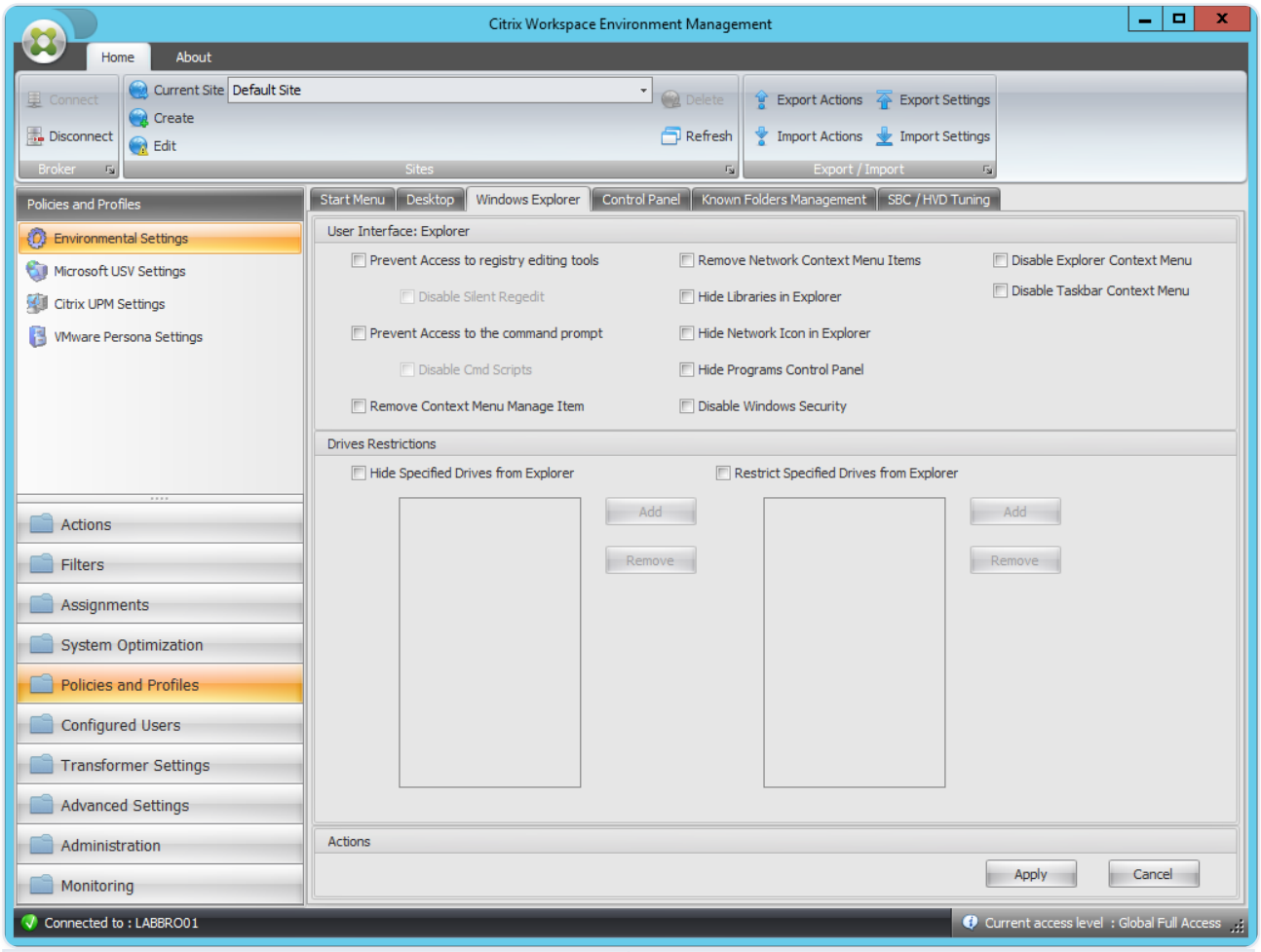
© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISABLE TASK MANAGER	
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

DISABLE SWITCHER	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\ImmersiveShell\EdgeUI`
Value Name	DisableTLcorner
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

DISABLE CHARM HINTS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\ImmersiveShell\EdgeUI`
Value Name	DisableCharmsHint
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

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



PREVENT ACCESS TO REGISTRY EDITING TOOLS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System`
Value Name	DisableRegistryTools
Value Type	DWORD
Enabled Value	Disable Silent Regedit ? 2 : 1
Disabled Value	0
Processing	Service called by agent

PREVENT ACCESS TO THE COMMAND PROMPT	
Parent Key	`HKCU\Software\Policies\System`

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

PREVENT ACCESS TO THE COMMAND PROMPT	
Value Name	DisableCMD
Value Type	DWORD
Enabled Value	Disable Silent Cmd Scripts ? 2 : 1
Disabled Value	0
Processing	Service called by agent

REMOVE CONTEXT MENU MANAGE ITEM	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoManageMyComputerVerb
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

REMOVE NETWORK CONTEXT MENU ITEMS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoNetworkConnections
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

HIDE LIBRARIES IN EXPLORER	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum`
Value Name	{031E4825-7B94-4dc3-B131-E946B44C8DD5}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

HIDE NETWORK ICON IN EXPLORER	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum`
Value Name	{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

HIDE PROGRAMS CONTROL PANEL	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Programs`
Value Name	NoProgramsCPL
Value Type	DWORD
Enabled Value	1

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

HIDE PROGRAMS CONTROL PANEL	
Disabled Value	0
Processing	Service called by agent

DISABLE WINDOWS SECURITY	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoNtSecurity
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

DISABLE EXPLORER CONTEXT MENU	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoViewContextMenu
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

DISABLE TASKBAR CONTEXT MENU	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`

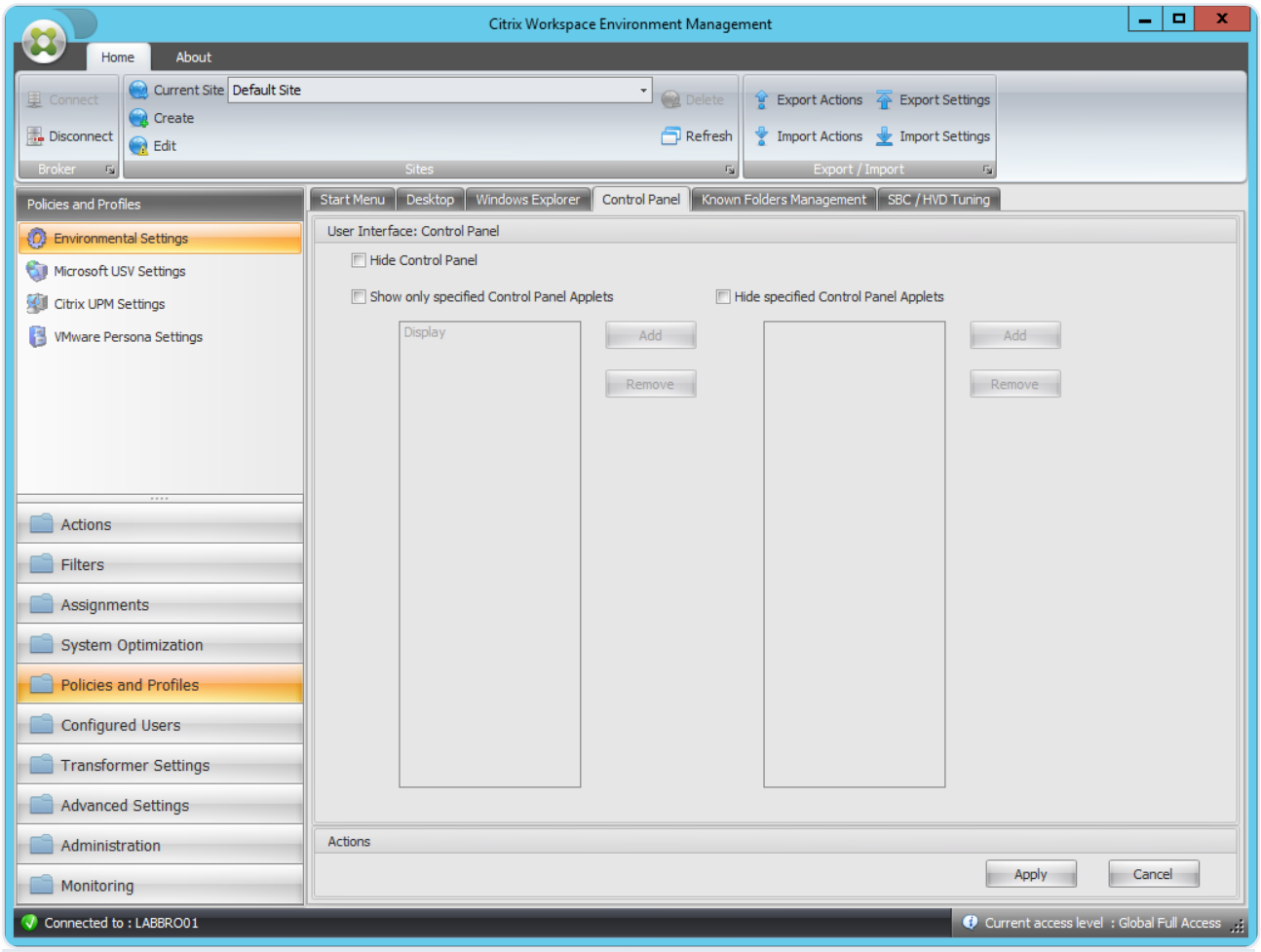
© 1997–2026 Citrix Systems, Inc. All rights reserved.

DISABLE TASKBAR CONTEXT MENU	
Value Name	NoTrayContextMenu
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

HIDE SPECIFIED DRIVES FROM EXPLORER	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoDrives
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon

RESTRICT SPECIFIED DRIVES FROM EXPLORER	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoViewOnDrive
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon

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



HIDE CONTROL PANEL	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	NoControlPanel
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

SHOW ONLY SPECIFIED CONTROL PANEL APPLETS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`

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

SHOW ONLY SPECIFIED CONTROL PANEL APPLETS	
Value Name	RestrictCpl
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

FOR EACH ALLOWED APPLET	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictCpl`
Value Name	Applet index (starting at 1 and automatically incremented)
Value Type	REG_SZ
Enabled Value	AppletName
Disabled Value	Null / Removed
Processing	Service called by agent

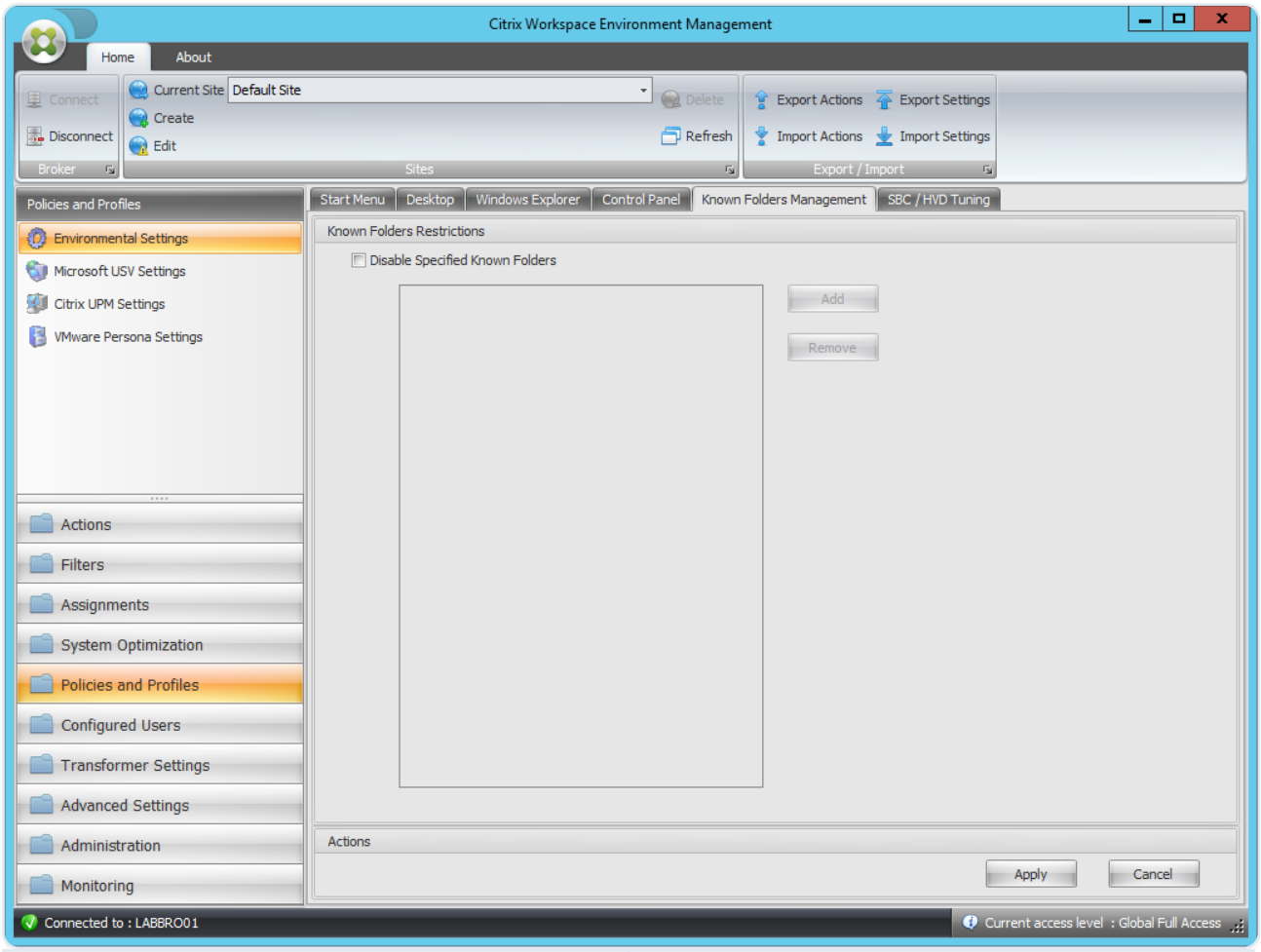
HIDE SPECIFIED CONTROL PANEL APPLETS	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Value Name	DisallowCpl
Value Type	DWORD
Enabled Value	1
Disabled Value	0

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

HIDE SPECIFIED CONTROL PANEL APPLETS	
Processing	Service called by agent

FOR EACH DISALLOWED APPLET	
Parent Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowCpl`
Value Name	Applet index (starting at 1 and automatically incremented)
Value Type	REG_SZ
Enabled Value	AppletName
Disabled Value	Null / Removed
Processing	Service called by agent

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

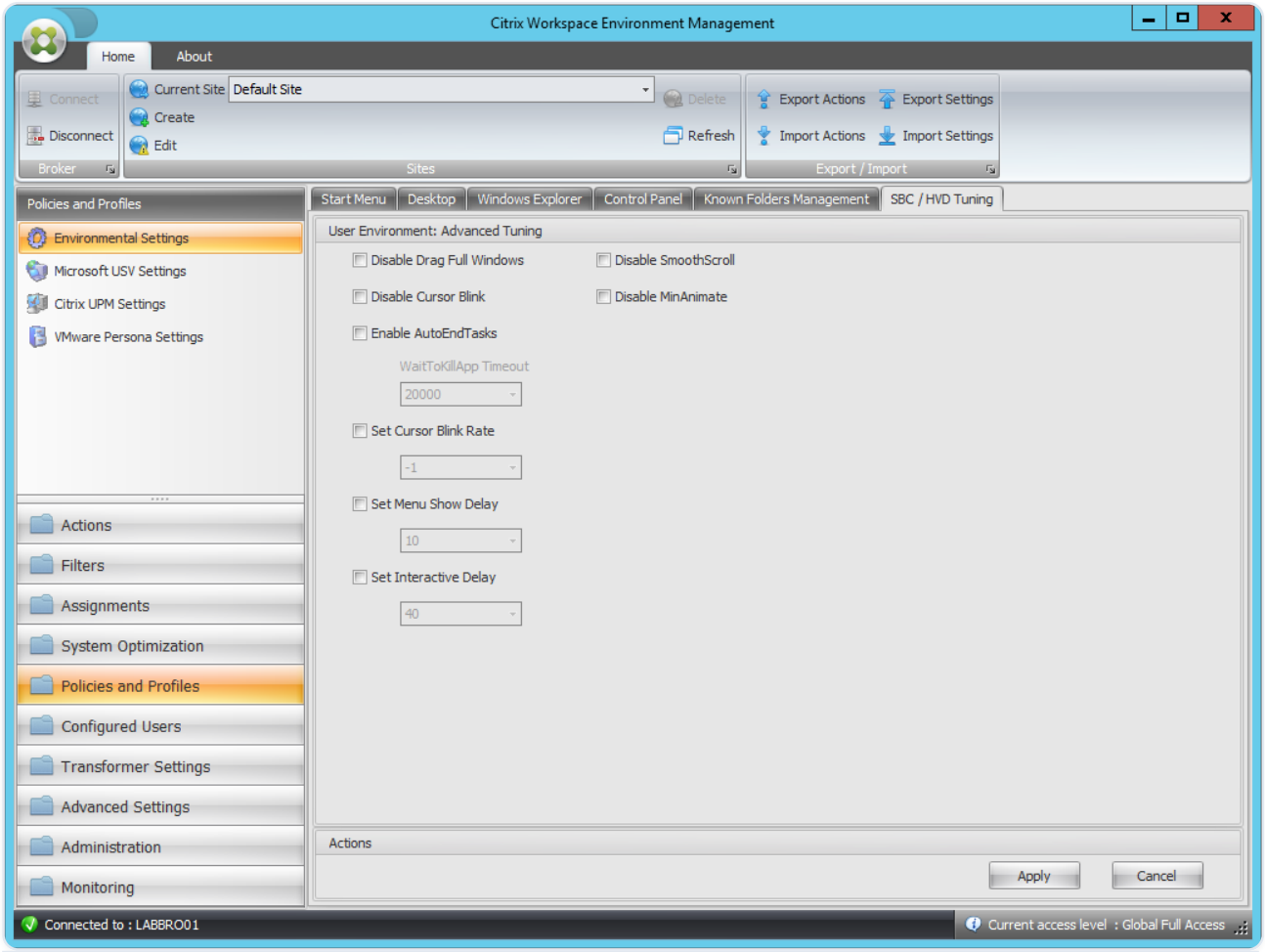


DISABLE SPECIFIED KNOWN FOLDERS	
Parent Key	`HKCU\Software\Policies\Microsoft\Windows\Explorer`
Value Name	DisableKnownFolders
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon

FOR EACH DISABLED FOLDER	
Parent Key	`HKCU\Software\Policies\Microsoft\Windows\Explorer\ DisableKnownFolders`

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

FOR EACH DISABLED FOLDER	
Value Name	Disabled folder name
Value Type	REG_SZ
Enabled Value	Disabled folder name
Disabled Value	Null / Removed
Processing	Service at logon



DISABLE DRAG FULL WINDOWS	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	DragFullWindows
Value Type	REG_SZ
Enabled Value	0

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

DISABLE DRAG FULL WINDOWS	
Disabled Value	1
Processing	Service at logon

DISABLE CURSOR BLINK	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	DisableCursorBlink
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

ENABLE AUTOENDTASKS	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	AutoEndTasks
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

WAITTOKILLAPP TIMEOUT	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	WaitToKillAppTimeout
Value Type	DWORD

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

WAITTOKILLAPP TIMEOUT	
Enabled Value	Configured value
Disabled Value	20000 (decimal)
Processing	Service at logon

SET CURSOR BLINK RATE	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	CursorBlinkRate
Value Type	DWORD
Enabled Value	Configured value
Disabled Value	500 (decimal)
Processing	Service at logon

SET MENU SHOW DELAY	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	MenuShowDelay
Value Type	DWORD
Enabled Value	Configured value
Disabled Value	400 (decimal)
Processing	Service at logon

SET INTERACTIVE DELAY	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	InteractiveDelay

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

SET INTERACTIVE DELAY	
Value Type	DWORD
Enabled Value	Configured value
Disabled Value	Null / Removed
Processing	Service at logon

DISABLE SMOOTHSCROLL	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	SmoothScroll
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service at logon

DISABLE MINANIMATE	
Parent Key	`HKCU\Control Panel\Desktop`
Value Name	MinAnimate
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service at logon

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

Filter conditions

Workspace Environment Management includes the following filter conditions that you use to configure the circumstances under which the agent assigns resources to users. For more information about using these conditions in the administration console, see Filters.

When using the following filter conditions, be aware of these two scenarios:

- If the agent is installed on a single-session or multi-session OS:
  - “Client” refers to a client device connecting to the agent host.
  - “Computer” and “Client Remote” refer to the agent host.
- If the agent is installed on a physical endpoint, conditions that contain “client” in the condition names are not applicable.

CONDITION NAME	ALWAYS TRUE
Expected value type	N/A
Expected result type	N/A
Expected syntax	N/A
Returns	True.

CONDITION NAME	COMPUTERNAME MATCH
Expected value type	N/A
Expected result type	String.
Expected syntax	Single name test: Computername Multiple tests (OR): Computername1;Computername2 Wildcard (also works with multiples): ComputerName*
Returns	True if the current computer name matches the tested value, false otherwise.

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

CONDITION NAME	CLIENTNAME MATCH
Expected value type	N/A
Expected value type	String.
Expected syntax	Single name test: Clientname Multiple tests (OR): Clientname1;Clientname2 Wildcard (also works with multiples): ClientName*
Returns	True if the current client name matches the tested value, false otherwise.

CONDITION NAME	IP ADDRESS MATCH
Expected value type	N/A
Expected result type	IP address.
Expected syntax	Single name test: IpAddress Multiple tests (OR): IpAddress1;IpAddress2 Wildcard (also works with multiples): IpAddress* Range (also works with multiples): IpAddress1-IpAddress2
Returns	True if the current computer IP address matches the tested value, false otherwise.

CONDITION NAME	CLIENT IP ADDRESS MATCH
Expected value type	N/A
Expected result type	IP address.
Expected syntax	Single name test: ClientIpAddress Multiple tests (OR): ClientIpAddress1;ClientIpAddress2 Wildcard (also works with multiples): ClientIpAddress* Range (also works with multiples): IpAddress1-IpAddress2
Returns	True if the current client IP address matches the tested value, false otherwise.

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

CONDITION NAME	ACTIVE DIRECTORY SITE MATCH
Expected value type	N/A
Expected result type	Exact name of the Active Directory site to test.
Expected syntax	Active directory site name.
Returns	True if the specified site matches the current site, false otherwise.

CONDITION NAME	SCHEDULING
Expected value type	N/A
Expected result type	Day of week (example: Monday).
Expected syntax	Single name test: DayOfWeek Multiple tests (OR): DayOfWeek1; DayOfWeek2
Returns	True if today matches the tested value, false otherwise.

CONDITION NAME	ENVIRONMENT VARIABLE MATCH
Expected value type	String. Name of the tested variable.
Expected result type	String. Expected value of the tested variable.
Expected syntax	Single name test: value Not null test: ?
Returns	True if environment variable exists and value matches, false otherwise.

CONDITION NAME	REGISTRY VALUE MATCH
Expected value type	String. Full path and name of the registry value to test. Example: Registry Key **HKCU\Software\Citrix\TestValueName**

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

CONDITION NAME	REGISTRY VALUE MATCH
Expected result type	String. Expected value of the tested registry entry.
Expected syntax	Single name test: value Not null test: ?
Returns	True if registry value exists and value matches, false otherwise.

CONDITION NAME	WMI QUERY RESULT MATCH
Expected value type	N/A
Expected result type	String.
Expected syntax	Valid WMI query. For more information, see `<https://docs.microsoft.com/en-us/windows/win32/wmisdk/querying-with-wql>`.
Returns	True if query is successful and has a result, false otherwise.

CONDITION NAME	USER COUNTRY MATCH
Expected value type	N/A
Expected result type	String.
Expected syntax	Two letter ISO language name.
Returns	True if user ISO language name matches the specified value, false otherwise.

CONDITION NAME	USER UI LANGUAGE MATCH
Expected value type	N/A
Expected result type	String. Two letter ISO language name. Example FR.

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

CONDITION NAME	USER UI LANGUAGE MATCH
Expected syntax	Two letter ISO language name. Example FR.
Returns	True if user UI ISO language name matches the specified value, false otherwise.

CONDITION NAME	USER SBC RESOURCE TYPE
Expected value type	N/A
Expected result type	Select from list.
Expected syntax	N/A
Returns	True if user context (published desktop or application) matches the selected value, false otherwise.

CONDITION NAME	OS PLATFORM TYPE
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if machine platform type (x64 or x86) matches the selected value, false otherwise.

CONDITION NAME	CONNECTION STATE
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if connection state (online or offline) matches the selected value, false otherwise.

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

CONDITION NAME	CITRIX VIRTUAL APPS™ VERSION MATCH
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Version. Example: 6.5
Expected syntax	N/A
Returns	True if version matches the selected value, false otherwise.

CONDITION NAME	CITRIX VIRTUAL APPS FARM NAME MATCH
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Farm Name (up to version 6.5). Example: Farm.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

CONDITION NAME	CITRIX VIRTUAL APPS ZONE NAME MATCH
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Zone Name (up to version 6.5). Example: Zone.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

CONDITION NAME	CITRIX VIRTUAL DESKTOPS™ FARM NAME MATCH
Expected value type	N/A

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

CONDITION NAME	CITRIX VIRTUAL DESKTOPS™ FARM NAME MATCH
Expected result type	String. Citrix Virtual Desktops Farm Name (up to version 5). Example: Farm.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

CONDITION NAME	CITRIX VIRTUAL DESKTOPS DELIVERY GROUP NAME MATCH
Expected value type	N/A
Expected result type	String. Citrix Virtual Desktops Delivery Group. Example: Group.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

CONDITION NAME	CITRIX PROVISIONING™ IMAGE MODE
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current Citrix Provisioning image mode matches the selected value, false otherwise.

CONDITION NAME	CLIENT OS
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A

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

CONDITION NAME	CLIENT OS
Returns	True if current client operating system matches the selected value, false otherwise.

CONDITION NAME	ACTIVE DIRECTORY PATH MATCH
Expected value type	N/A
Expected result type	String. Name of the tested Active Directory Path.
Expected syntax	Single name test: strict LDAP path matching Wildcard test: OU=Users* Multiple entries: separate entries with semicolon (;)
Returns	True if attribute exists and the value matches, false otherwise.

CONDITION NAME	ACTIVE DIRECTORY ATTRIBUTE MATCH
Expected value type	String. Name of the tested Active Directory attribute.
Expected result type	String. Expected value of the tested Active Directory attribute.
Expected syntax	Single value test: value Multiple value entries: separate entries with semicolon (;) Test for not null: ?
Returns	True if attribute exists and the value matches, false otherwise.

CONDITION NAME	NAME OR VALUE IS IN LIST
Expected value type	String. Full file path of the XML list generated by the Integrity List manager utility.
Expected result type	String. Expected value of the name/value to look for in the list.

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

CONDITION NAME	NAME OR VALUE IS IN LIST
Expected syntax	String
Returns	True if the input value is found in the name/value pairs in the specified list, false otherwise.

CONDITION NAME	NO COMPUTERNAME MATCH
Negative condition behavior	Runs **ComputerName Match** and returns the opposite result (true if false, false if true). See condition **ComputerName Match** for more information.

CONDITION NAME	NO CLIENTNAME MATCH
Negative condition behavior	Runs ClientName Match and returns the opposite result (true if false, false if true). See condition **ClientName Match** for more information.

CONDITION NAME	NO IP ADDRESS MATCH
Negative condition behavior	Runs IP Address Match and returns the opposite result (true if false, false if true). See condition **IP Address Match** for more information.

CONDITION NAME	NO CLIENT IP ADDRESS MATCH
Negative condition behavior	Runs Client IP Address Match and returns the opposite result (true if false, false if true). See condition **Client IP Address Match** for more information.

CONDITION NAME	NO ACTIVE DIRECTORY SITE MATCH
Negative condition behavior	Runs Active Directory Site Match and returns the opposite result (true if false, false if true).

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

CONDITION NAME	NO ACTIVE DIRECTORY SITE MATCH
	See condition **Active Directory Site Match** for more information.

CONDITION NAME	NO ENVIRONMENT VARIABLE MATCH
Negative condition behavior	Runs Environment Variable Match and returns the opposite result (true if false, false if true). See condition **Environment Variable Match** for more information.

CONDITION NAME	NO REGISTRY VALUE MATCH
Negative condition behavior	Runs Registry Value Match and returns the opposite result (true if false, false if true). See condition **Registry Value Match** for more information.

CONDITION NAME	NO WMI QUERY RESULT MATCH
Negative condition behavior	Runs WMI Query result Match and returns the opposite result (true if false, false if true). See condition **WMI Query result Match** for more information.

CONDITION NAME	NO USER COUNTRY MATCH
Negative condition behavior	Runs User Country Match and returns the opposite result (true if false, false if true). See condition **User Country Match** for more information.

CONDITION NAME	NO USER UI LANGUAGE MATCH
Negative condition behavior	Runs User UI Language Match and returns the opposite result (true if false, false if true). See condition **User UI Language Match** for more information.

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

CONDITION NAME	NO CITRIX VIRTUAL APPS VERSION MATCH
Negative condition behavior	Runs Citrix Virtual Apps Version Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Apps Version Match** for more information.

CONDITION NAME	NO CITRIX VIRTUAL APPS FARM NAME MATCH
Negative condition behavior	Runs Citrix Virtual Apps Farm Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Apps Farm Name Match** for more information.

CONDITION NAME	NO CITRIX VIRTUAL APPS ZONE NAME MATCH
Negative condition behavior	Runs Citrix Virtual Apps Zone Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Apps Zone Name Match** for more information.

CONDITION NAME	NO CITRIX VIRTUAL DESKTOPS FARM NAME MATCH
Negative condition behavior	Runs Citrix Virtual Desktops Farm Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Desktops Farm Name Match** for more information.

CONDITION NAME	NO CITRIX VIRTUAL DESKTOPS DELIVERY GROUP NAME MATCH
Negative condition behavior	Runs Citrix Virtual Desktops Delivery Group Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Desktops Delivery Group Name Match** for more information.

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

CONDITION NAME	NO ACTIVE DIRECTORY PATH MATCH
Negative condition behavior	Runs Active Directory Path Match and returns the opposite result (true if false, false if true). See condition **Active Directory Path Match** for more information.

CONDITION NAME	NO ACTIVE DIRECTORY ATTRIBUTE MATCH
Negative condition behavior	Runs Active Attribute Path Match and returns the opposite result (true if false, false if true). See condition **Active Attribute Path Match** for more information.

CONDITION NAME	NAME OR VALUE IS NOT IN LIST
Negative condition behavior	Runs Name or Value is in List and returns the opposite result (true if false, false if true). See condition **Name or Value is in List** for more information.

CONDITION NAME	CLIENT REMOTE OS MATCH
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current remote client operating system matches selected value, false otherwise.

CONDITION NAME	NO CLIENT REMOTE OS MATCH
Negative condition behavior	Runs Client Remote OS Match and returns the opposite result (true if false, false if true). See condition **Client Remote OS Match** for more information.

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

CONDITION NAME	DYNAMIC VALUE MATCH
Expected value type	String. Any dynamic expression using environment variables or Dynamic Tokens.
Expected result type	String. Expected value of the tested expression.
Expected syntax	Single name test: value Not null test: ?
Returns	True if dynamic expression result value exists and value matches, false otherwise.

CONDITION NAME	NO DYNAMIC VALUE MATCH
Negative condition behavior	Runs Dynamic Value Match and returns the opposite result (true if false, false if true). See condition **Dynamic Value Match** for more information.

CONDITION NAME	TRANSFORMER MODE STATE
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current Transformer state matches selected value, false otherwise.

CONDITION NAME	NO CLIENT OS MATCH
Negative condition behavior	Runs Client OS Match and returns the opposite result (true if false, false if true). See condition **Client OS Match** for more information.

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

CONDITION NAME	ACTIVE DIRECTORY GROUP MATCH
Expected value type	N/A
Expected result type	String.
Expected syntax	Single name test: group NetBIOS name (DOMAIN\Groupname) Multiple tests (OR): Groupname1;Groupname2
Returns	True if any of the current user groups matches the tested value, false otherwise.

CONDITION NAME	NO ACTIVE DIRECTORY GROUP MATCH
Negative condition behavior	Runs Active Directory Group Match and returns the opposite result (true if false, false if true). See condition **Active Directory Group Match** for more information.

CONDITION NAME	FILE VERSION MATCH
Expected value type	String. Full path and name of the file to test.
	Example: **C:\Test\TestFile.dll**
Expected result type	String. Expected file version value of the tested file.
Expected syntax	Single name test: value Not null test: ?
Returns	True if registry value exists and value matches, false otherwise.

CONDITION NAME	NO FILE VERSION MATCH
Negative condition behavior	Runs File Version Match and returns the opposite result (true if false, false if true). See condition **File Version Match** for more information.

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

CONDITION NAME	NETWORK CONNECTION STATE
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current network connection state matches selected value, false otherwise.

IMPORTANT:

Before you use Published Resource Name as the filter condition type, keep the following in mind: If the published resource is a published application, type the browser name of the application in the **Matching Result** field. If the published resource is a published desktop, type the published name of the desktop in the **Matching Result** field.

CONDITION NAME	PUBLISHED RESOURCE NAME
Expected value type	N/A
Expected result type	String. Name of the published resource (Citrix Virtual Apps/Citrix Virtual Desktops/RDS).
Expected syntax	Single name test: published resource name Multiple tests (OR): Name1;Name2 Wildcard test: Name*
Returns	True if the current published resource name matches the tested value, false otherwise.

CONDITION NAME	NAME IS IN LIST
Expected value type	String. Full file path of the XML list generated by the Integrity List manager utility.
Expected result type	String. Expected value of the name to look for in the list.

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

CONDITION NAME	NAME IS IN LIST
Expected syntax	String
Returns	True if there is a name match in the name/value pairs in the specified list, false otherwise.

CONDITION NAME	NAME IS NOT IN LIST
Negative condition behavior	Runs Name is in List and returns the opposite result (true if false, false if true). See condition **Name is in List** for more information.

CONDITION NAME	FILE/FOLDER EXISTS
Expected value type	N/A
Expected result type	String.
Expected syntax	Full path of the file system entry (file or folder) to test.
Returns	True if the specified file system entry exists, false otherwise.

CONDITION NAME	FILE/FOLDER DOES NOT EXIST
Negative condition behavior	Runs File/Folder exists and returns the opposite result (true if false, false if true). See condition **File/Folder exists** for more information.

CONDITION NAME	DATETIME MATCH
Expected value type	N/A
Expected result type	DateTime as String. Date/time to test.
Expected syntax	Single Date: 06/01/2016 Date Range: 06/01/2016-08/01/2016 Multiple entries:

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

CONDITION NAME	DATETIME MATCH
	entry1;entry2 Ranges and single dates can be mixed
Returns	True if execution date/time matches any of the specified entries, false otherwise.

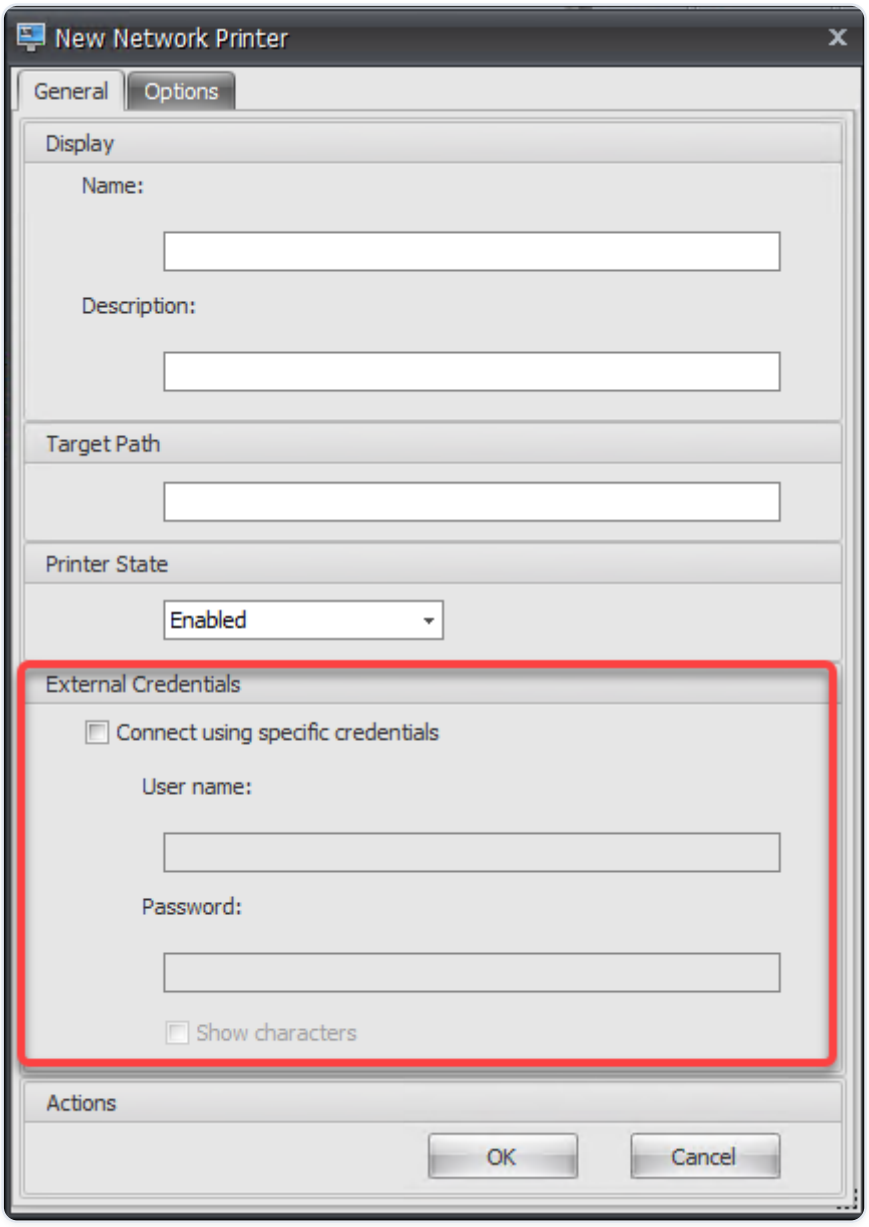
CONDITION NAME	NO DATETIME MATCH
Negative condition behavior	Runs DateTime Match and returns the opposite result (true if false, false if true). See condition **DateTime Match** for more information.

FIPS support

You can run Workspace Environment Management™ (WEM) in a FIPS environment. The following configurations in WEM relate to FIPS:

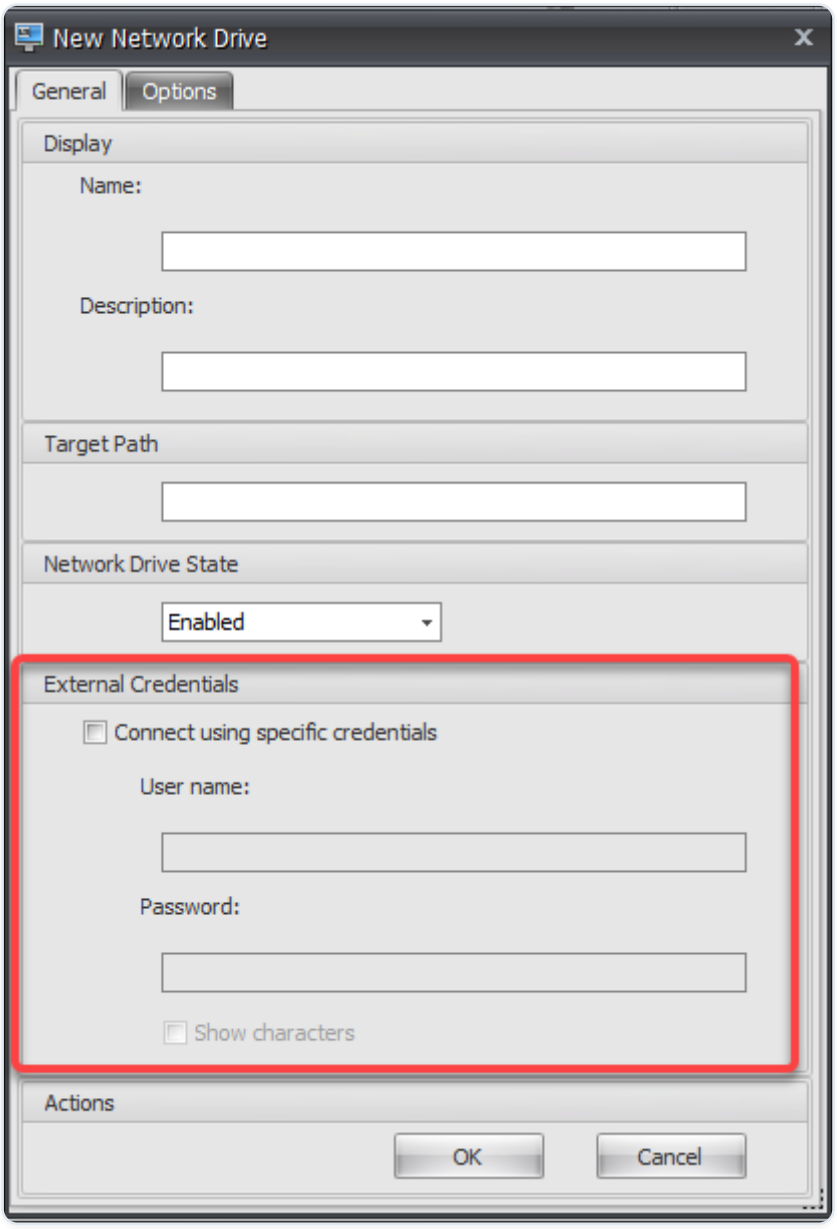
- Printer credentials in **Administration console > Actions > Printers**:

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



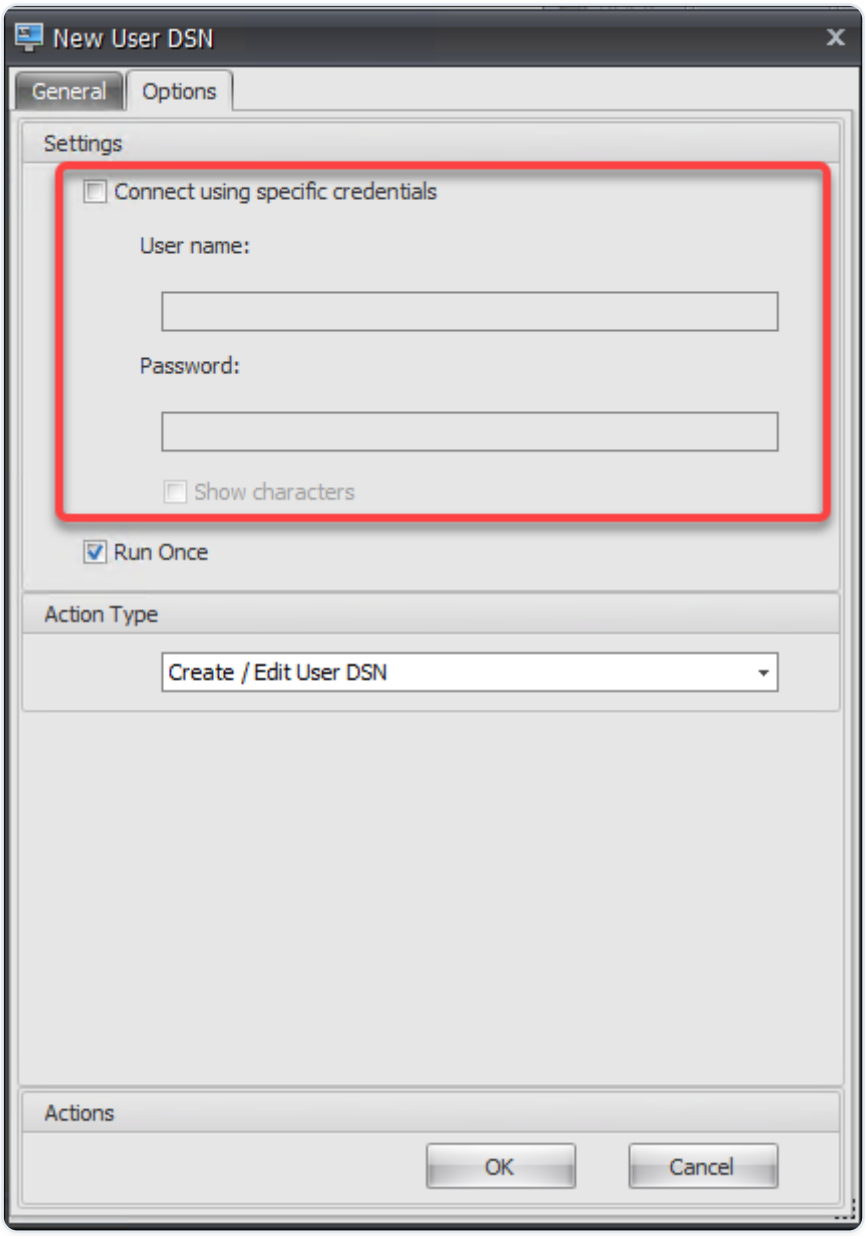
- Network drive credentials in **Administration console > Actions > Network Drives**:

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

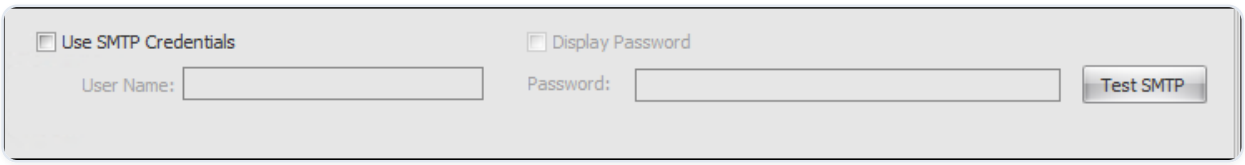


- User DSN credentials in **Administration console > Actions > User DSN**:

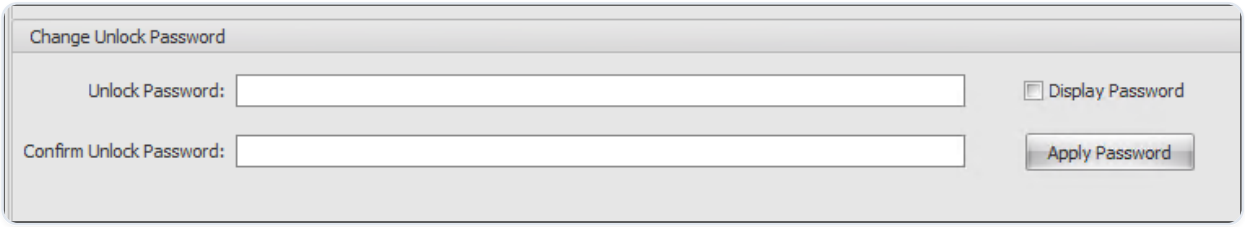
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- SMTP credentials in **Administration console > Advanced Settings > UI Agent Personalization > Helpdesk Options**:

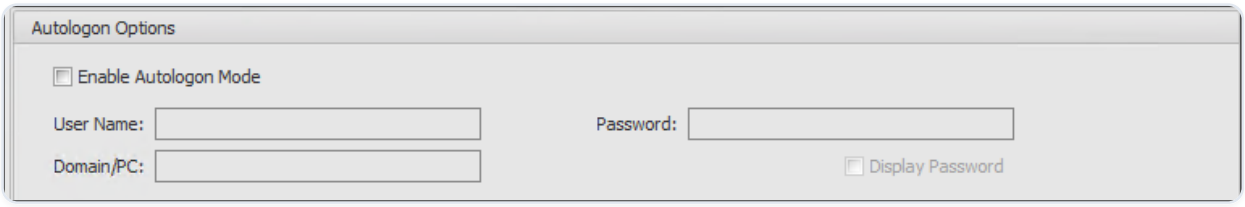


- Unlock password settings in **Administration console > Transformer Settings > General > General Settings**:



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

- Auto logon credentials in **Administration console > Transformer Settings > Advanced > Logon/Logoff & Power Settings**:



Be aware of the following consideration when running WEM in a FIPS environment.

- You cannot restore to your WEM environment the following items if they are exported from a WEM 2003 or earlier environment.
  - Actions (printers, network drives, user DSN) and action groups containing those actions
  - Settings (agent configuration settings and transformer settings)
  - Configuration sets

Upgrade considerations

If you want to run WEM in FIPS mode, be aware of the following considerations before upgrading the WEM infrastructure services and administration console:

- If you have *WEM 2006 or later* running in your environment, you can first upgrade to 2109 and then switch to FIPS mode or *the opposite way*.
- If you have *WEM 2003 or earlier* running in your environment, you must first upgrade to 2109 and then switch to FIPS mode.

Agent considerations

To run the WEM agent in a FIPS environment, make sure that the version of the agent is *2006 or later*.

Load balancing with Citrix ADC

This article guides you through the deployment of a Workspace Environment Management™ (WEM) server group containing two or more infrastructure servers in all active load balanced configurations. The article provides details of how to configure a Citrix ADC appliance to load balance incoming requests from the WEM administration console and the WEM agent.

You can listen on these WEM ports with Citrix ADC:

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

- Administration port (by default, 8284)
- Agent service port (by default, 8286)
- Cached data synchronization port (by default, 8288)

Suppose you want to deploy a WEM server group containing two infrastructure servers (infrastructure server 1 and infrastructure server 2). Perform the following steps:

1. Log on to the Citrix ADC management GUI and then click **Configuration**.
2. Navigate to **Traffic Management > Load Balancing > Servers > Add** and then click **Add** to add infrastructure server 1. Repeat to add infrastructure server 2.
3. Navigate to **Traffic Management > Load Balancing > Service Groups** and then click **Add** to create a service group for the *administration console service*.
    - **Protocol**. Select **TCP**.
    - **Cache Type**. Select **SERVER**.
4. On the Load Balancing Service Group page, click **No Service Group Member**.
5. On the Create Service Group Member page, select **Server Based**, click the right arrow, and then select infrastructure server 1. Repeat steps 3 through 5 for infrastructure server 2.
    - **Port**. For example, type 8284 for the administration console.
6. Follow steps 3 through 5 to create service groups for the *agent service* and *cache synchronization service*.
    - **Port**. For the agent service port, type 8286. For the cached data synchronization port, type 8288.
7. Navigate to **Traffic Management > Load Balancing > Virtual Servers** and then click **Add** to add a virtual server for the *administration console service*.
    - **Protocol**. Select **TCP**.
    - **IP Address Type**. Select **IP Address**.
    - **IP Address**. Type the Virtual IP. For details, see Configuring Citrix ADC-owned IP addresses.
    - **Port**. For example, type 8284 for the administration console.
8. Click **No Load Balancing Virtual Server Service Group Binding**.

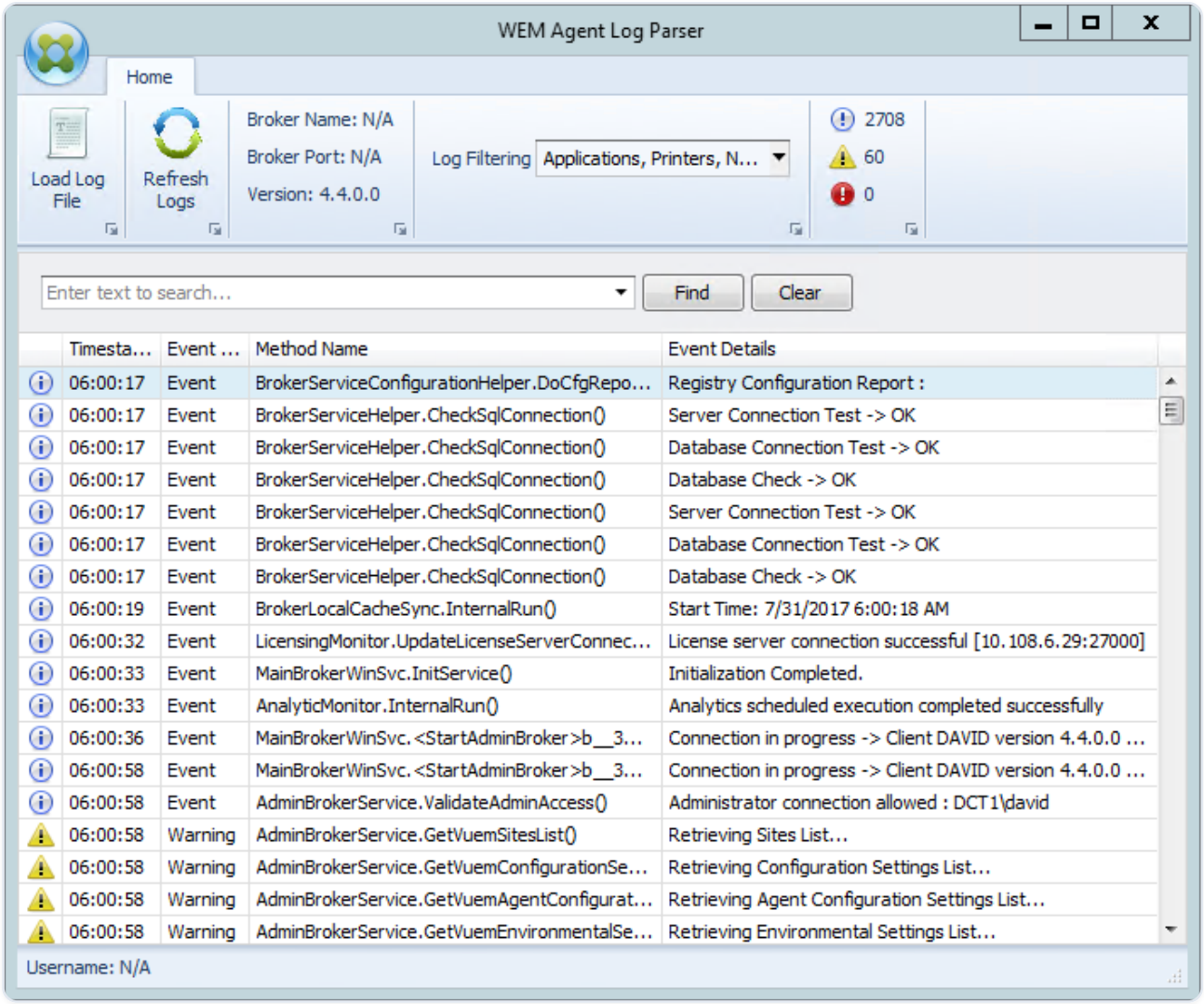
© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. On the Service Group Binding page, click the right arrow, select the corresponding service group, and then click **Bind**.
10. Follow steps 7 through 9 to create virtual servers that listen on the agent service port and the cached data synchronization port.

    - **Port**. For the agent service port, type 8286. For the cached data synchronization port, type 8288.

Log parser

Workspace Environment Management includes a log parser application, which is located in the agent installation directory. The default location is - `c:\Program Files (x86)\Citrix\Workspace Environment Management Agent\Agent Log Parser.exe`.



The **WEM Agent Log Parser** allows you to open any Workspace Environment Management™ agent log file, making them searchable and filterable. The parser summarizes the total number of events, warnings, and exceptions (in the top right of the ribbon). It also includes details about the

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

log file (the name and port of the infrastructure service it first connected to and the agent version and user name).

Port information

Workspace Environment Management™ uses the following ports.

SOURCE	DESTINATION	TYPE	PORT	DETAILS
Infrastructure service	Agent host	TCP	49752	"Agent port". Listening port on the agent host that receives instructions from the infrastructure service.
Administration console	Infrastructure service	TCP	8284	"Administration port". Port on which the administration console connects to the infrastructure service.
Agent	Infrastructure service	TCP	8286	"Agent service port". Port on which the agent connects to the infrastructure server.
Agent cache synchronization process	Infrastructure service	TCP	8288	"Cached data synchronization port". Applicable to Workspace Environment Management 1912 and later;

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

SOURCE	DESTINATION	TYPE	PORT	DETAILS
				replaces *Cache synchronization port* of Workspace Environment Management 1909 and earlier. Port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server.
Infrastructure service	Citrix License Server	TCP	27000	"Citrix License Server port". The port on which the Citrix License Server is listening and to which the infrastructure service then connects to validate licensing.
Infrastructure service	Citrix License Server	TCP	7279	The port used by the dedicated Citrix component (daemon) in the Citrix License Server to

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

SOURCE	DESTINATION	TYPE	PORT	DETAILS
				validate licensing.
Monitoring service	Infrastructure service	TCP	8287	"WEM monitoring port". Listening port on the infrastructure server used by the monitoring service.

View log files

You can collect and view logs related to Workspace Environment Management™ (WEM). You use the logs to troubleshoot issues on your own or provide the logs when you contact Citrix Technical Support for assistance. You can collect logs related to:

- WEM agent
- WEM infrastructure service
- WEM administration console
- WEM database
- WEM web console

Logs related to the agent

You can collect logs related to the WEM agent. Logs that you can collect on machines where the WEM agent is installed include:

- **WEM agent logs**
  - **Citrix WEM Agent Init.log**. The initialization log that lets you troubleshoot issues with the agent in CMD or UI mode. The log is created on logon or on refresh. If the agent fails to start, view this log file for error details. Errors appear as *exceptions*. By default, this log file is created in the user's profile folder (%userprofile%).
  - **Citrix WEM Agent.log**. The primary log that lets you troubleshoot issues with the agent in CMD or UI mode. The log lists what instructions the agent processed. If an action fails to be assigned to the current user, view this log file for error details. Errors appear as *exceptions*.

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

By default, this log file is created in the user's profile folder (%userprofile%). To change the default, go to **Administration Console > Advanced Settings > Configuration > Agent Options** and then configure the **Enable Agent Logging** setting. To view more details, enable **Debug Mode** on the **Agent Options** tab. Alternatively, you can enable logging by configuring the following registry key:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Agent Host

Name: AgentDebugModeLocalOverride

Type: DWORD

Value: 0

Set the value to 1 to enable the log file and 0 to disable it. For the changes to take effect, restart the Citrix WEM Agent Host Service. By default, logging is disabled.

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.

- **Citrix WEM Agent Host Service Debug.log**. The log that lets you troubleshoot issues with the Citrix WEM Agent Host Service. By default, this log file is located in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Agent`. To enable logging, be sure to enable **Debug Mode** for the relevant configuration set on the **Administration Console > Advanced Settings > Configuration > Service Options** tab. Alternatively, you can enable logging by configuring the following registry key:

  Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Agent Host

  Name: AgentServiceDebugModeLocalOverride

  Type: DWORD

  Value: 0

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

Set the value to 1 to enable the log file and 0 to disable it. For the changes to take effect, restart the Citrix WEM Agent Host Service. By default, logging is disabled.

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.

- **Windows event logs**. Information written to the Windows Event Log. View logs in the **Event Viewer > Applications and Services Logs > WEM Agent Service** pane.
- **Windows Communication Foundation (WCF) traces**. Logs that are helpful when you encounter issues related to communications between the WEM agent and the WEM infrastructure service. To enable logging, you must enable WCF tracing. For more information, see Windows Communication Foundation traces.

Logs related to the infrastructure service

You can collect logs related to the WEM infrastructure service. Logs that you can collect on machines where the WEM infrastructure service is installed include:

- **Windows event logs**. Information written to the Windows Event Log. View logs in the **Event Viewer > Applications and Services Logs > WEM Infrastructure Service** pane.
- **Citrix WEM Infrastructure Service Debug.log**. The log that lets you troubleshoot issues with the Citrix WEM infrastructure service (Norskale Broker Service.exe). By default, this log file is located in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Infrastructure Services\Logs`. To enable this log file, follow these steps to enable debug mode:

  a. Open the **WEM Infrastructure Service Configuration Utility** from the Start menu.

  b. On the **Advanced Settings** tab, select **Enable debug mode**.

  c. Click **Save Configuration** and click **Yes** to start the service to apply the change.

  d. Close the **WEM Infrastructure Service Configuration Utility** window.

- **WCF traces**. Logs that are helpful when you encounter communication issues related to the WEM infrastructure service. To enable logging, you must enable WCF tracing. For more information, see Windows Communication Foundation traces.

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

Logs related to the administration console

You can collect logs related to the WEM administration console. Logs that you can collect on machines where the administration console is installed include:

- **Citrix WEM Console Trace.log**. The log that lets you troubleshoot issues with the WEM administration console. By default, this log file is created in the user's profile folder (%userprofile%). To enable logging, follow these steps to enable debug mode:

  a. Open the **WEM Administration Console** from the Start menu and click **Connect**.

  b. In the **New Infrastructure Server Connection** window, check the information and then click **Connect**.

  c. On the **About** tab, click **Options** and select **Enable Debug Mode**.

  d. Click **Apply** to apply the change.

- **WCF traces**. Logs that are helpful when you encounter issues related to communications between the WEM administration console and the WEM database. To enable logging, you must enable WCF tracing. For more information, see Windows Communication Foundation traces.

Logs related to the WEM database

You can collect logs related to the WEM database. Logs are created when you use the WEM database management utility to create or upgrade a database. View the following log file for details:

- **Citrix WEM Database Management Utility Debug Log.log**. The log that lets you troubleshoot issues with the WEM database. This log file is created by default and is located in `C:\Program Files (x86)\Citrix\Workspace Environment Management Infrastructure Services\Logs`.

Logs related to the WEM web console

You can collect logs related to the WEM web console. Logs are created when you use the WEM web console configuration utility to configure the web console. Additionally, logs are created when the web console service is running. For more details, see the following log files:

- **Web Console Configuration Utility.log**. The log that lets you troubleshoot issues with the WEM web console configuration utility. This log file is created by default and is located in `C:\ProgramData`.
- **Citrix WEM Public API.log**. The log that lets you troubleshoot issues with the WEM web console service. When you configure the web console service using the **Web console**

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

configuration utility to enable logging, ensure to enable the **Enable console logging** option. This log file is located in `C:\ProgramData`.

Windows Communication Foundation traces

You can view Windows Communication Foundation (WCF) traces to help you troubleshoot the following issues:

- Communications between the agent and the infrastructure service
- Communications related to the WEM infrastructure service
- Communications related to the WEM administration console

Troubleshoot communications between the agent and the infrastructure service

If the WEM agent does not communicate properly with the WEM infrastructure service, you can view WCF traces of the VUEMUIAgent.exe service. Follow these steps to enable WCF tracing:

1. Log on to the WEM agent machine.
2. Right-click the agent icon in the taskbar and then select **Exit** to close the agent.
3. Locate the VUEMUIAgent.exe.config file in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Agent` and then create a backup copy of the file.
4. Open the file in Notepad or WordPad and insert the following snippet into the section between the `<configuration>` and the `</configSections>` marker.
5. Save the file.

```
<system.diagnostics>

    <sources>

            <source name="System.ServiceModel"

                    switchValue="Information, ActivityTracing"

                    propagateActivity="true">

            <listeners>

            <add name="traceListener"

                type="System.Diagnostics.XmlWriterTraceListener"
```

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

```
                initializeData= "c:\trace\vuemUIAgent-Traces.svclog" />
            </listeners>
        </source>
    </sources>
</system.diagnostics>
```

6. On the agent machine, create a root folder called “Trace” on the C drive (C:\Trace). Skip this step if the folder already exists.
7. Reproduce the issue you encountered and then end the VUEMUIAgent.exe process.
8. View the log file named `vuemUIAgent-Traces.svclog` in `C:\Trace`.

You can also view WCF traces of the Citrix.Wem.Agent.Service.exe service. Follow these steps:

1. Log on to the WEM agent machine.
2. Right-click the agent icon in the taskbar and then select **Exit** to close the agent.
3. End the Citrix WEM Agent Host Service.
4. Locate the Citrix.Wem.Agent.Service.exe.config file in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Agent` and then create a backup copy of the file.
5. Open the file in Notepad or WordPad and insert the following snippet into the file, starting on the fourth line right after the `</configSections>` marker.
6. Save the file.

```
<system.diagnostics>
    <sources>
            <source name="System.ServiceModel"
                    switchValue="Information, ActivityTracing"
                    propagateActivity="true">
            <listeners>
```

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

```
            <add name="traceListener"

                type="System.Diagnostics.XmlWriterTraceListener"

                initializeData= "c:\trace\NorskaleAgentHostService-
Traces.svclog" />

            </listeners>

        </source>

    </sources>

</system.diagnostics>
```

7. On the agent machine, create a root folder called “Trace” on the C drive (C:\Trace). Skip this step if the folder already exists.
8. Start the Windows service called Citrix WEM Agent Host Service and then reproduce the issue you encountered.
9. View the log file named `NorskaleAgentHostService-Traces.svclog` in `C:\Trace`.

Troubleshoot communications related to the WEM infrastructure service

If you encounter communication issues related to the WEM infrastructure service, you can view WCF traces of the Norskale Broker Service. Follow these steps to enable WCF tracing:

1. Log on to the machine where the WEM infrastructure service is installed.
2. End the Citrix WEM Infrastructure Service.
3. Locate the Norskale Broker Service.exe.config file in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Infrastructure Services` and then create a backup copy of the file.
4. Open the file in Notepad or WordPad and insert the following snippet into the file, starting on the third line right after the `<configuration>` marker.

```
<system.diagnostics>

    <sources>

            <source name="System.ServiceModel"
```

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

```
                    switchValue="Information, ActivityTracing"

                    propagateActivity="true">

            <listeners>

            <add name="traceListener"

                type="System.Diagnostics.XmlWriterTraceListener"

                initializeData= "c:
\trace\NorskaleInfrastructureBrokerService-Traces.svclog" />

            </listeners>

        </source>

    </sources>

</system.diagnostics>
```

5. Save the file.
6. On the WEM infrastructure service machine, create a root folder called “Trace” on the C drive (C:\Trace). Skip this step if the folder already exists.
7. Start the Citrix WEM Infrastructure Service and then reproduce the issue you encountered.
8. View the log file named `NorskaleInfrastructureBrokerService-Traces.svclog` in `C:\Trace`.

Troubleshoot communications between the WEM administration console and the WEM database

If you encounter issues related to communications between WEM administration console and the WEM database, you can view WCF traces of Norskale Administration Console.exe service. Follow these steps to enable WCF tracing:

1. Log on to the WEM administration console machine.
2. Close the WEM administration console.

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

3. Locate the Norskale Administration Console.exe.config file in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Administration Console` and then create a backup copy of the file.
4. Open the file in Notepad or WordPad and add the following snippet into the file, starting on the third line right after the `<configuration>` marker.

```
<system.diagnostics>

    <sources>

            <source name="System.ServiceModel"

                    switchValue="Information, ActivityTracing"

                    propagateActivity="true">

            <listeners>

            <add name="traceListener"

                type="System.Diagnostics.XmlWriterTraceListener"

                initializeData= "c:\trace\WEMConsole-Traces.svclog" />

            </listeners>

        </source>

    </sources>

</system.diagnostics>
```

5. Save the file.
6. On the administration console machine, create a root folder called “Trace” on the C drive (C:\Trace). Skip this step if the folder already exists.
7. Open the WEM administration console and then reproduce the issue you encountered.
8. View the log file named `WEMConsole-Traces.svclog` in `C:\Trace`.

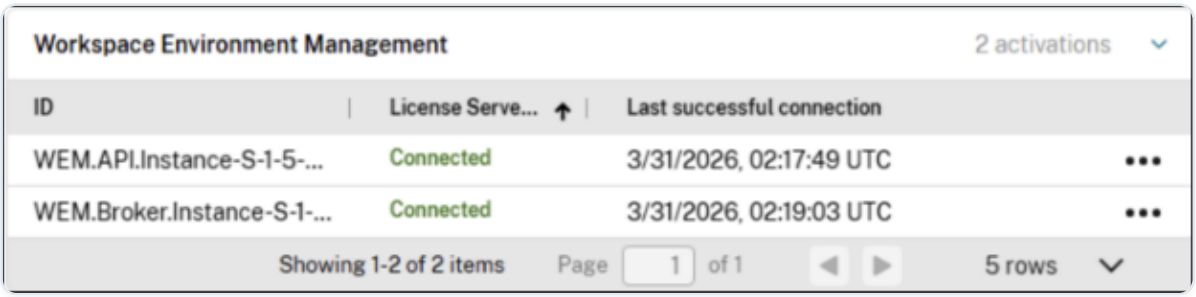
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot WEM LAS issues

This article helps you diagnose and resolve issues with the Citrix® Licensing Activation Service (LAS) in Workspace Environment Management™ (WEM). For more information about setting up licensing, see Set up licensing.

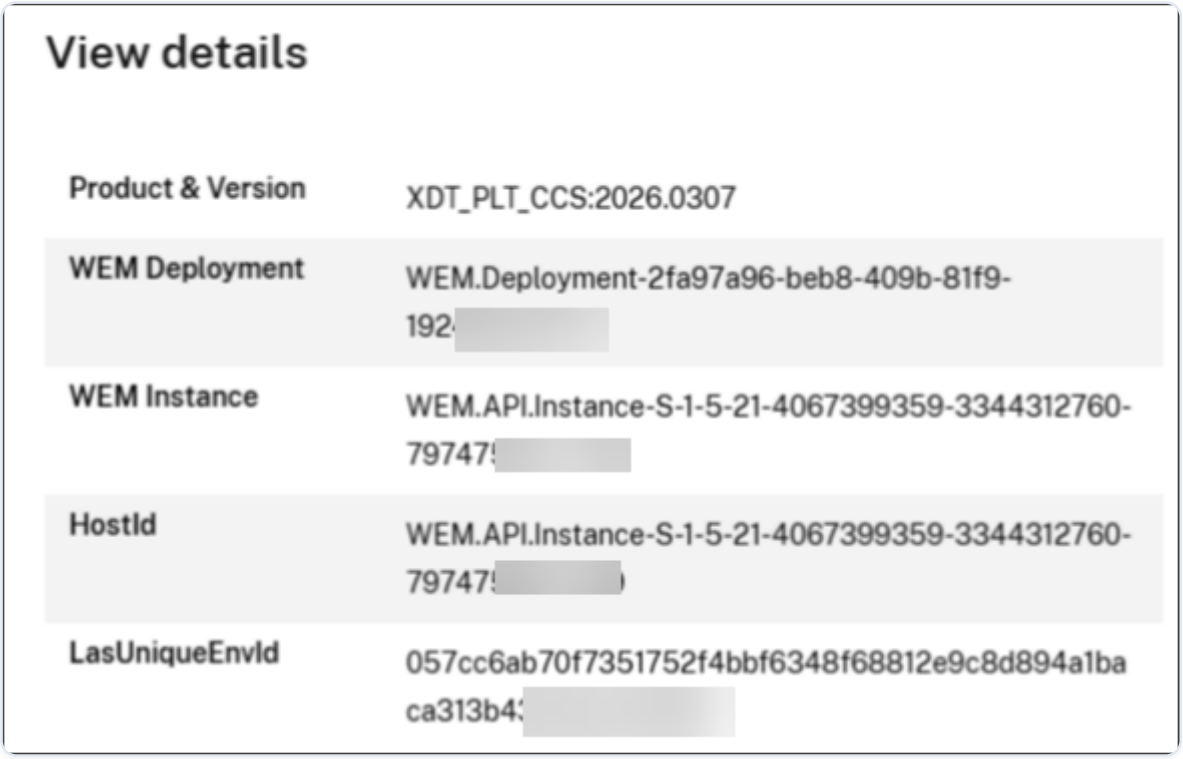
If you encounter LAS licensing issues, first check the license server status in Citrix Cloud™. If the status is not green, review activation details to help identify the cause.

1. Sign in to Citrix Cloud with your account.
2. Go to **Licensing > Licensed Deployments > License Servers**.
3. Expand **Workspace Environment Management** to view the list of activations:
    - **ID**: Machine SID
    - **License Server connectivity**: **Connected** or **Lost connection**
    - **Last successful connection**: Time of the most recent successful connection



4. Click **... > View Details** for an activation to review detailed information:
    - **Product & Version**: **Product_Edition_Model** and **BurnInDate** used when activating with LAS. **BurnInDate** is usually the product release date.
    - **WEM Deployment**: Deployment ID
    - **WEM Instance**: Machine SID
    - **HostID**: Machine SID
    - **LasUniqueEnvID**: Unique ID of the instance for which LAS provides activation

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



Check connectivity to the license server

Before WEM calls the LAS SDK, the WEM infrastructure service sends a **POST** request to the following endpoints:

```
https://{licenseServerAddress}:{lasLicenseServerPort}/lic_admin/
lasentitlements

https://{licenseServerAddress}:{lasLicenseServerPort}/ls_server/serverinfo
```

Where:

- **licenseServerAddress** is the address of the Citrix License Server.
- **lasLicenseServerPort** is the port used by the LAS service (default: **8083**).

If either URL is blocked or unreachable, the following error appears in the **Citrix WEM Infrastructure Service Debug.log**:

```
<CheckLasEnabled>d__27.MoveNext() : Error sending POST request: A task was
canceled.
```

Ensure the WEM infrastructure server can reach both URLs without network or firewall restrictions.

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

Test connectivity

Run the following commands from the WEM infrastructure server to verify that it can reach the license server. Replace `<licenseServer>` with your license server address.

1. Check that the LAS port is reachable:

   ```
   Test-NetConnection <licenseServer> -Port 8083
   ```

   `TcpTestSucceeded : True` confirms the port is open.

2. Check that the LAS endpoints respond:

   ```
   curl.exe -k -X POST "https://<licenseServer>:8083/lic_admin/
   lasentitlements" -H "Content-Type: application/json" -d "{\"ver\":
   \"1.0\"}"

   curl.exe -k -X POST "https://<licenseServer>:8083/ls_server/serverinfo"
   -H "Content-Type: application/json" -d "{\"ver\":\"1.0\"}"
   ```

   NOTE:

   The `-k` option bypasses TLS certificate validation and is intended for connectivity diagnostics only. Do not use it in production configuration.

If a command fails or times out, the WEM infrastructure server cannot reach the endpoint. Check the network path, firewall rules, and the license server address.

Troubleshoot license server certificate issues

Certificate validation can fail if the certificate is expired, not yet valid, or does not match the license server name.

Certificate expired or not yet valid

If the license server certificate has expired or is not yet valid, one of the following errors appears in the **Citrix WEM Infrastructure Service Debug.log**:

```
LICENSING: license server certificate NOT valid, is expired, subject
'{subject}', issuer '{issuer}'
```

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

```
LICENSING: license server certificate NOT valid, used too soon, subject
'{subject}', issuer '{issuer}'
```

Resolution:

- If the certificate has expired, renew it.
- If the certificate is newly issued and not yet valid, wait until its validity period begins, and then retry.

License server hostname mismatch

If the license server hostname does not match the certificate, the following error appears in the **Citrix WEM Infrastructure Service Debug.log**:

```
LICENSING: license server certificate NOT valid, hostname mismatch,
subject '{subject}', issuer '{issuer}'
```

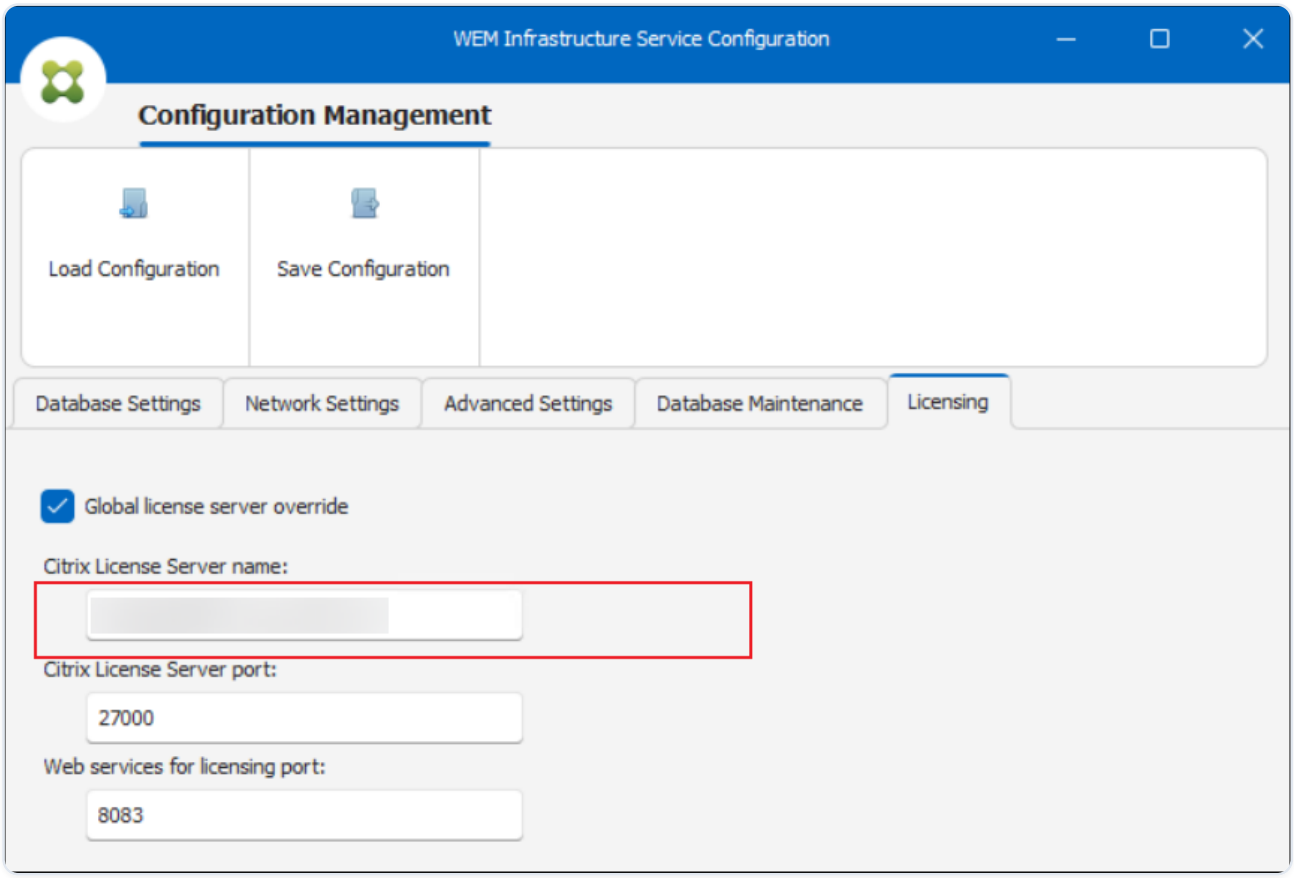
Resolution:

Verify that the **Citrix License Server name** you specified matches one of the names defined in the certificate. The hostname must match **either** of the following:

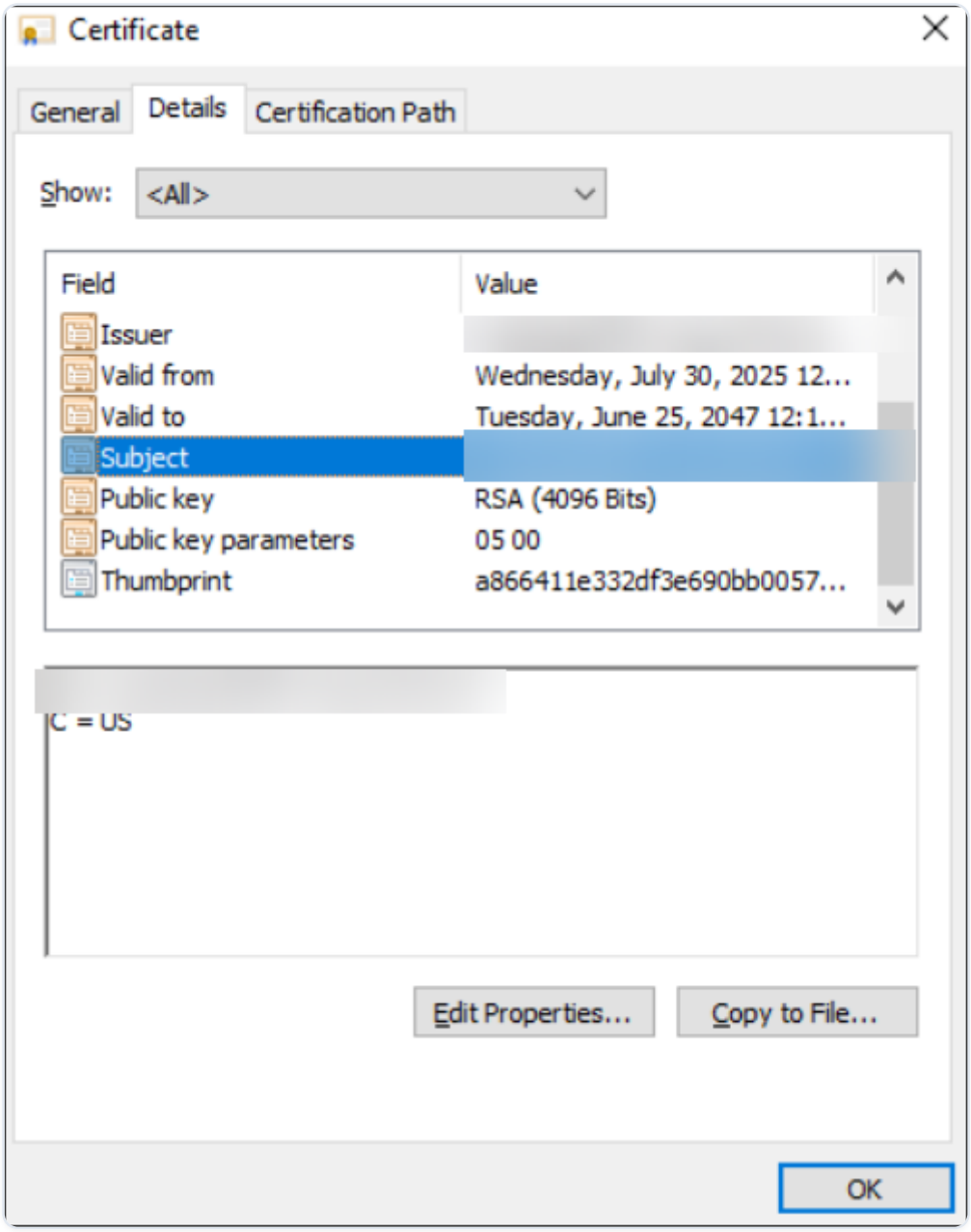
- The **Subject** field of the certificate.
- A **DNS name** listed in the **Subject Alternative Name (SAN)** extension of the certificate.

If the hostname does not match any of these entries, update the license server name, or reissue the certificate with the correct DNS names.

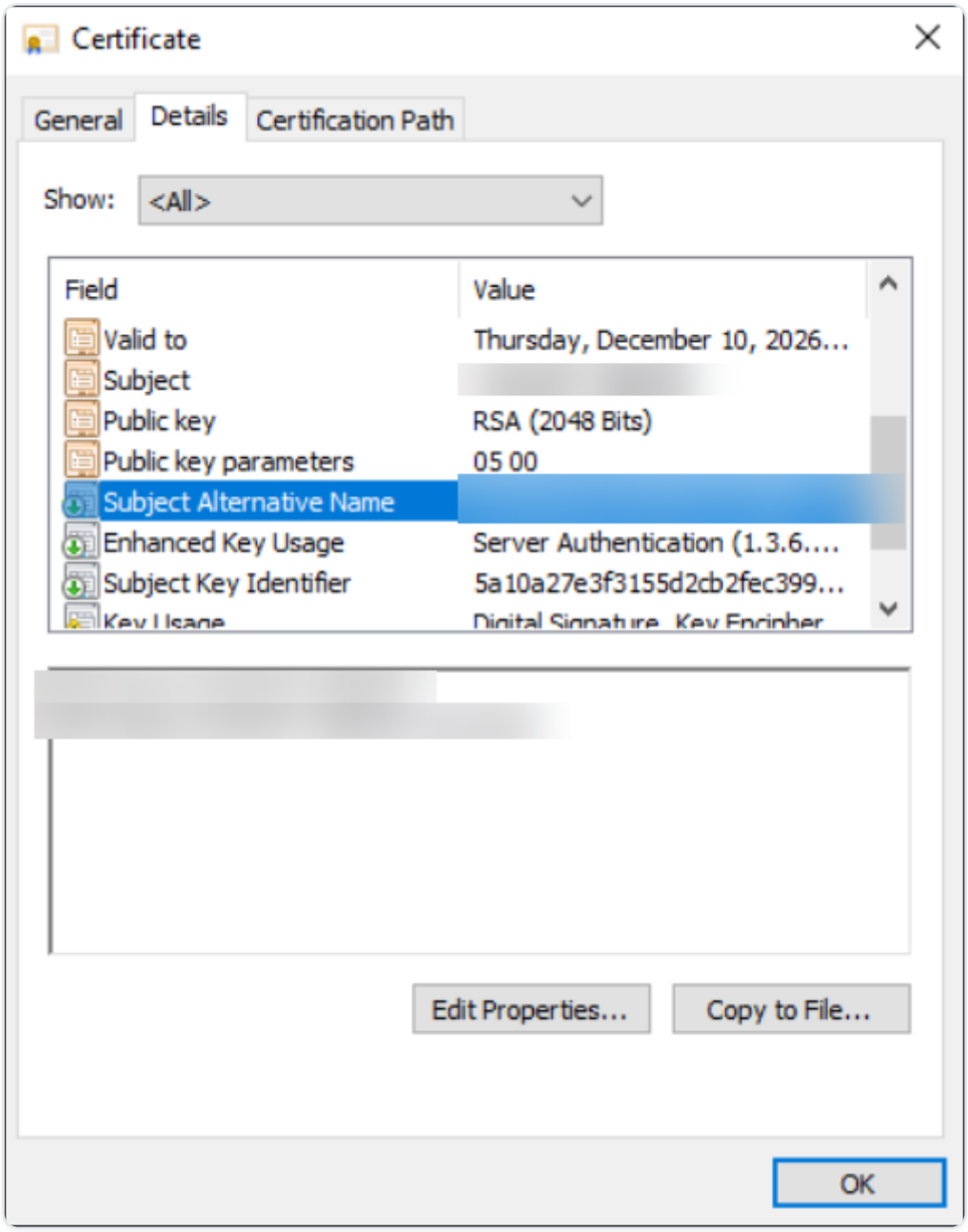
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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



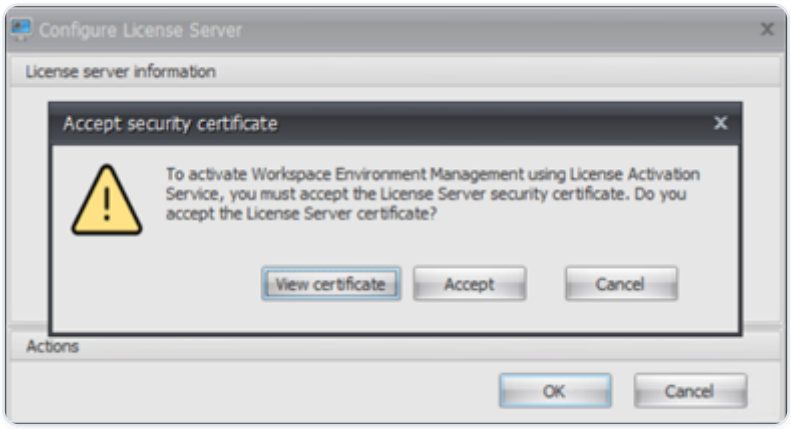
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The certificate acceptance dialog box does not appear

If the license server certificate is not trusted, the **Accept Security Certificate** dialog box should appear, and you must manually accept the certificate to proceed.

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



WEM retrieves license and certificate information from the following URL:

```
https://{licenseServerAddress}:{lasLicenseServerPort}/ls_server/serverinfo
```

If this URL is blocked or unreachable, WEM cannot retrieve the license server information, and the certificate acceptance dialog box does not appear.

Resolution:

Ensure the WEM infrastructure server can reach the URL above without any network or firewall restrictions.

Force the certificate acceptance dialog box to appear

If you need to force the certificate acceptance dialog box to appear, follow the steps for your configuration method.

If you configured the license server for **a specific WEM infrastructure server** using the **WEM Infrastructure Service Configuration utility**:

1. Delete the registry value **SpecificLasLicenseServerCertificateThumbprint** under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Infrastructure Services**.
2. Reopen the **WEM Infrastructure Service Configuration utility**.
3. Click **Save Configuration** again.

   This action triggers the **Accept Security Certificate** dialog box, allowing you to manually accept the license server certificate.

If you configured the license server **globally** in the **WEM console**:

1. Clear the value of **GlobalLasLicenseServerCertificateThumbprint** in the **VUEMParameters** table in the database.

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

2. Reconfigure the license server in the WEM console. This action triggers the certificate acceptance process.

CAUTION:

Editing the registry incorrectly can cause serious problems that might require you to reinstall the operating system. Back up the registry before you modify it.

Collect verbose LAS logs

If the preceding steps do not resolve the issue, enable trace-level logging and collect the LAS client log for Citrix Support. Enable logging on the component that reports the problem:

- The WEM infrastructure server for issues with the infrastructure services or the legacy console.
- The web console server for issues with the web console.

To enable logging, follow these steps:

1. On the affected server, open **Registry Editor** (`regedit.exe`).
2. Navigate to the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\WEM\Licensing
   ```

3. Create a **String Value (REG_SZ)** with the following settings:
   - **Name**: `LasLicenseServerLogLevel`
   - **Value**: `Trace`
4. Restart the service for the change to take effect:
   - On the WEM infrastructure server, restart the **Citrix WEM Infrastructure Service**.
   - On the web console server, restart the **Citrix WEM Public API Service**.
5. Reproduce the issue, and then collect the **Citrix WEM LAS Client Log.log** file and provide it to Citrix Support. The log file is located in the `Licensing\Las` subfolder of the component's installation folder:
   - **WEM infrastructure server**: `<Infrastructure Service installation folder>\Licensing\Las`. By default, the installation folder is `C:\Program Files (x86)\Citrix\Workspace Environment Management Infrastructure Services`.

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

- **On-premises web console** server: `<Web Console installation folder>\Licensing\Las`. By default, the installation folder is `C:\Program Files (x86)\Citrix\Workspace Environment Management Web Console`.

CAUTION:

Editing the registry incorrectly can cause serious problems that might require you to reinstall the operating system. Back up the registry before you change it.

WEM health check tool

The WEM health check tool is a standalone tool that checks the status of the WEM components and helps you to identify and resolve configuration issues with your WEM deployment. This tool is installed with the WEM agent and the WEM infrastructure service.

Launch the tool

The tool requires the **Local administrator** privilege to run. Launch `Citrix.WEM.Health.Check.Tool.exe` using one of the following methods:

- On the WEM Infrastructure server, go to `<Installation folder of WEM Infrastructure Services>\Health Check Tool` (for example, `C:\Program Files (x86)\Citrix\Workspace Environment Management Infrastructure Services\Health Check Tool`)
- On a machine with WEM agent installed, go to `<Installation folder of WEM agent>\Health Check Tool` (for example, `C:\Program Files (x86)\Citrix\Workspace Environment Management Agent\Health Check Tool`)

To collect the logs for troubleshooting purposes, enable **Debug mode**. After the problem occurs, retrieve the logs for analysis.

Home page

The **Home page** includes the following configurations:

- Configurations for both the WEM agent and the WEM infrastructure server. Select the **Name**, the **Agent Type**, the **Agent version**, and the **Join type**.
- The pre-requisite for the **Join** type can be either an AD joined or a Non-domain joined type.

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

- You can enable the **Force debug mode** or the **Debug mode** for WEM agent and WEM infrastructure server respectively.
- When you enable the **Force debug mode**, the debug mode is turned on for the agent regardless of the settings specified in the **Administration** console.
- For the changes to take effect on the WEM agent or the WEM infrastructure server immediately, you can restart the `Citrix WEM agent Host Service` and `VUEMUIAgent.exe` or the `Citrix WEM Infrastructure Service` respectively.
- **Retrieve logs** lets you retrieve and save the logs in a zipped folder as a package. You can then check the package saved on your local machine.

Infrastructure server

To check the configuration of the WEM infrastructure server, open the tool and check the basic information of the infrastructure server.

- Enable the **Debug mode** of the infrastructure server.
- Click the **Start check** button to check the configurations of the infrastructure server.
- Click **Retrieve logs** to retrieve logs, **Open report file** to view the detailed report, and **Check again** to re-check the configurations.

The following components are considered to generate the health check report.

- Windows Firewall configuration
- Agent Broker service
- Cache sync service
- Admin service
- License server

NOTE:

- Make sure that the agent cache resides in a persistent location. Using a non-persistent cache location can cause potential cache synchronization issues, excessive network data usage, performance issues, and so on.
- We recommend that you set the directory service timeout based on your connection time.

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

The following services are required for the WEM agent to function as expected. Make sure that the services are running and the startup type for each service is set to automatic.

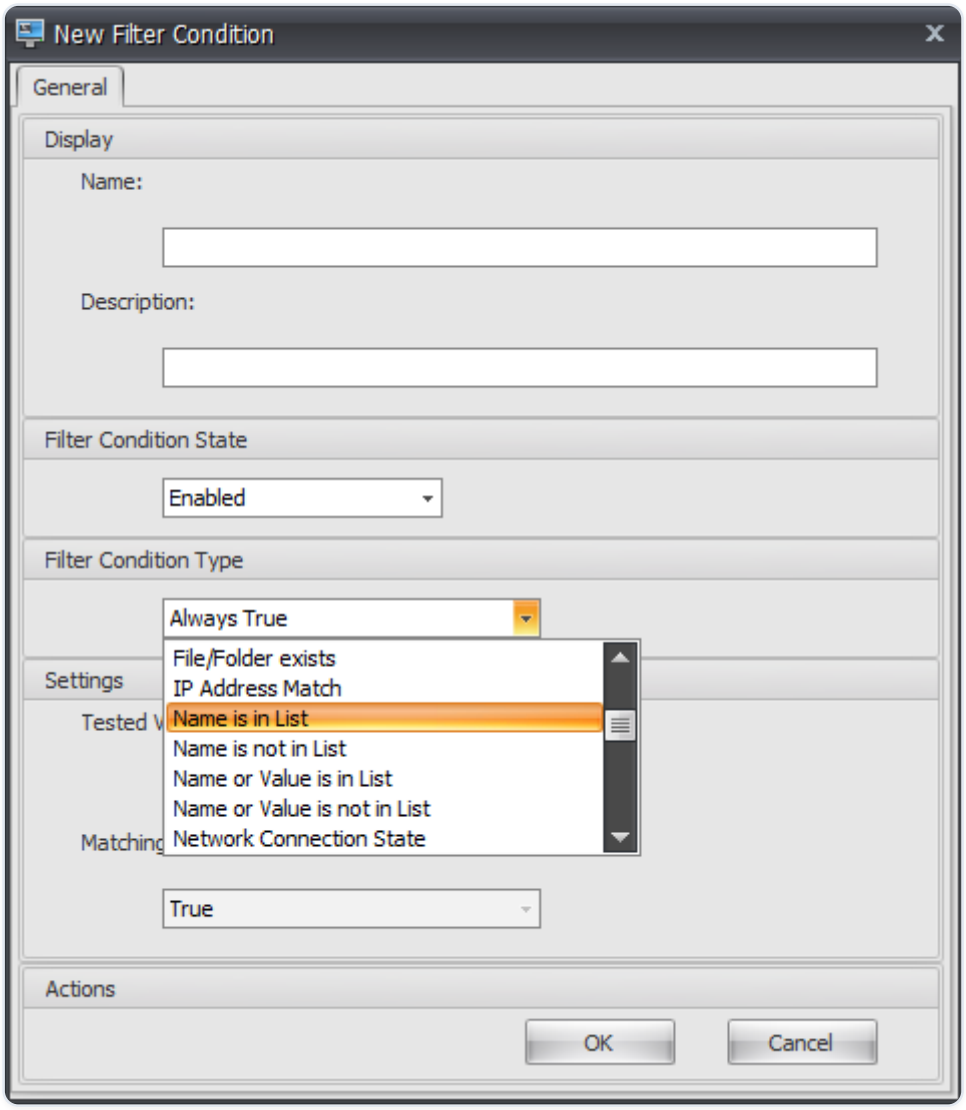
- System event notification service
- Citrix WEM agent host service
- Citrix WEM user logon service

WEM Integrity Condition List Manager

WEM Integrity Condition List Manager is a powerful tool that helps you create the XML file for filtering purposes. The tool is used with the following filter condition types: **Name is in List**, **Name is not in List**, **Name or Value is in List**, and **Name or Value is not in List**. For more information about using these conditions in the administration console, see Filters.

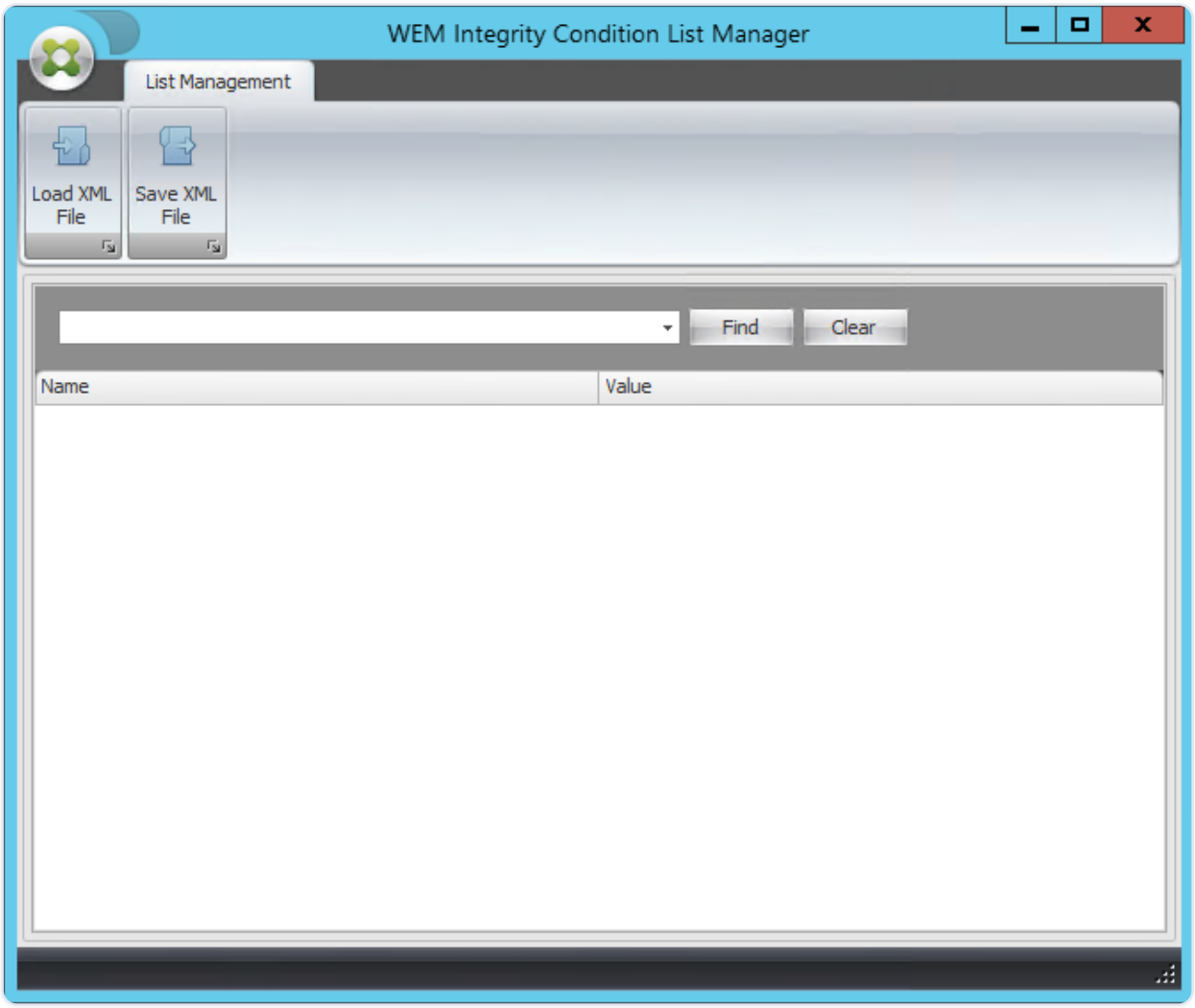
This article describes how to use the WEM Integrity Condition List Manager to create the XML file for filtering purposes. For example, suppose you want to filter the actions by using the WEM Integrity Condition List Manager in conjunction with **Name is in List**.

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



1. Open WEM Integrity Condition List Manager.

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

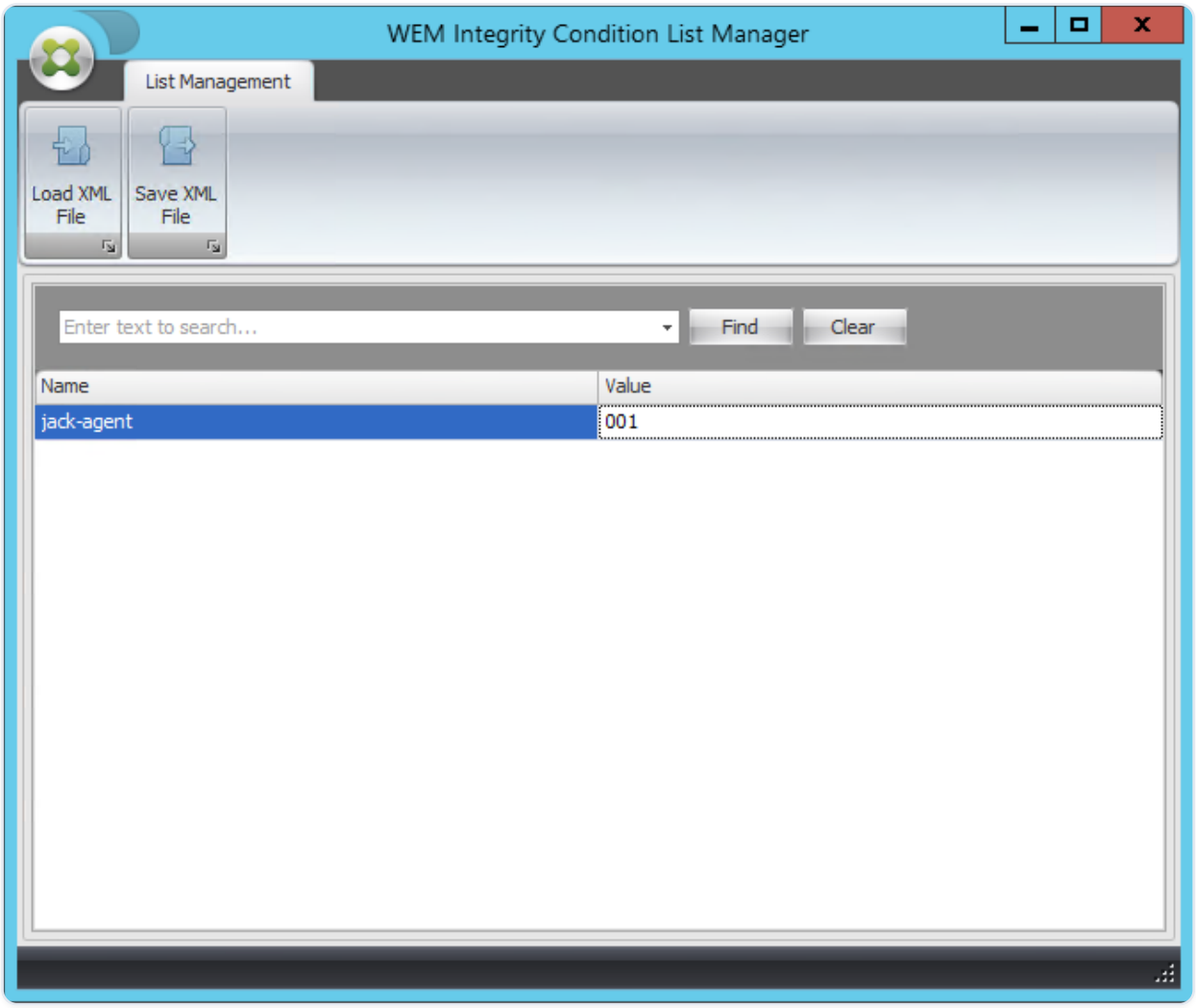


2. Right-click the blank area and then select **Add** in the context menu.
3. Type the name in the **Name** field.

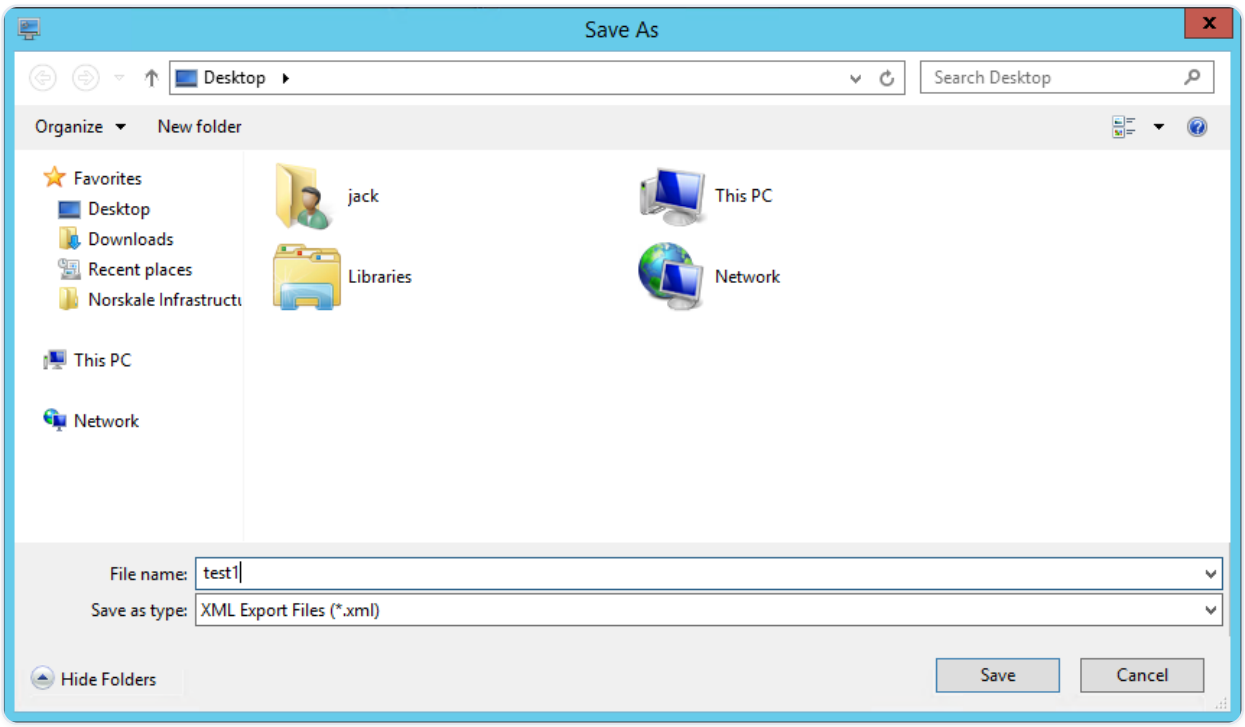
NOTE:

Type the name of the machine on which the WEM agent is running (agent host).

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

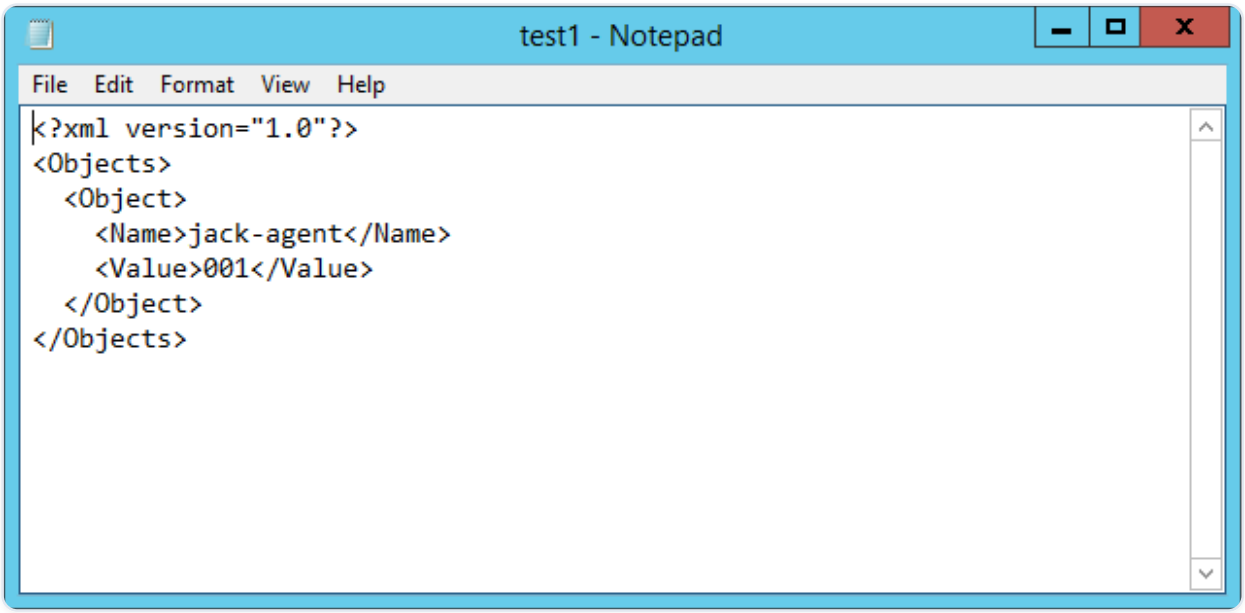


4. Click **Save XML File**, browse to the desired folder, and then click **Save**.



5. Open the saved XML file to verify that the information you provided was saved correctly.

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

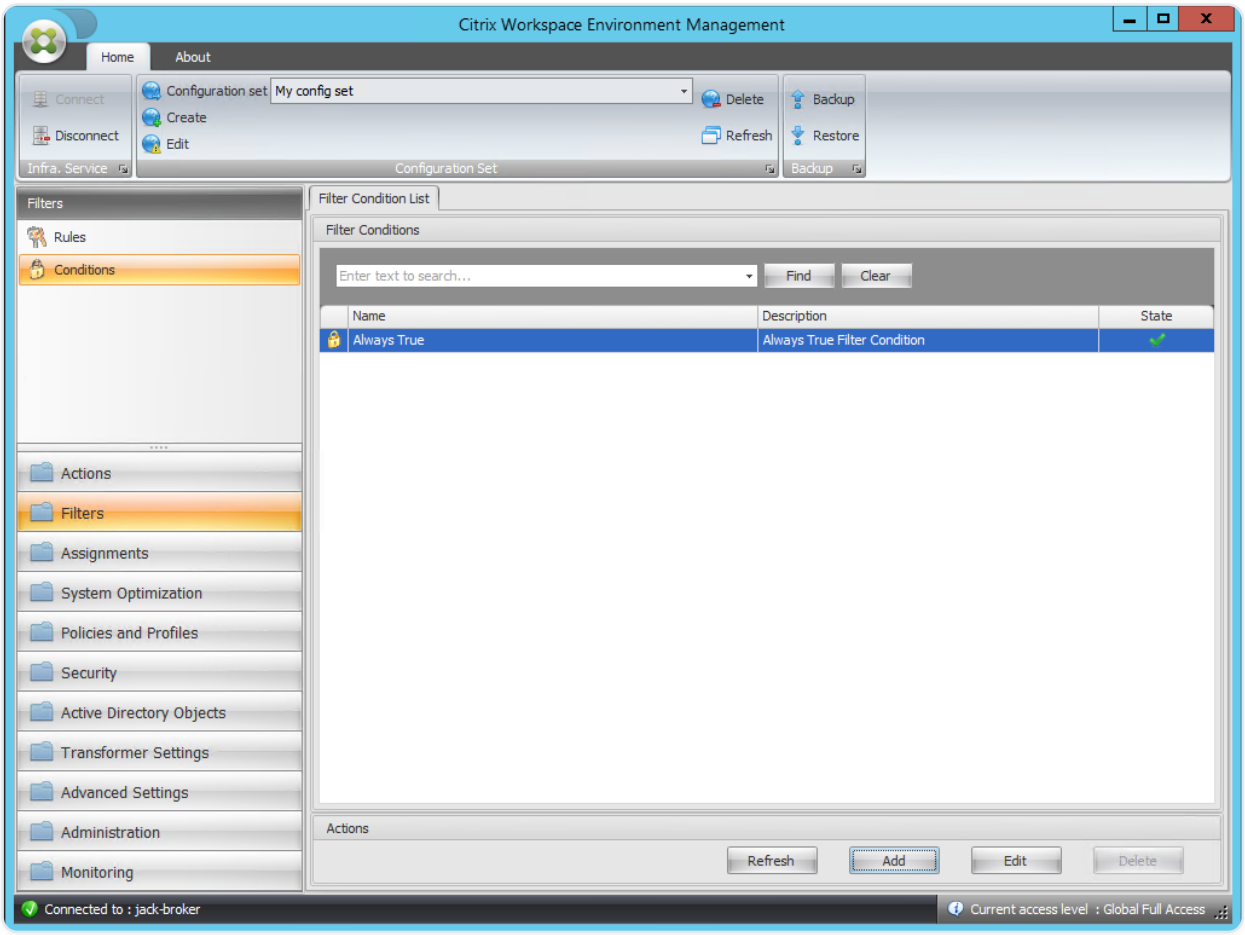


6. Copy the saved XML file to a folder on the agent host.

> **NOTE:**
>
> This feature does not work if you save the XML file on an administration console machine.

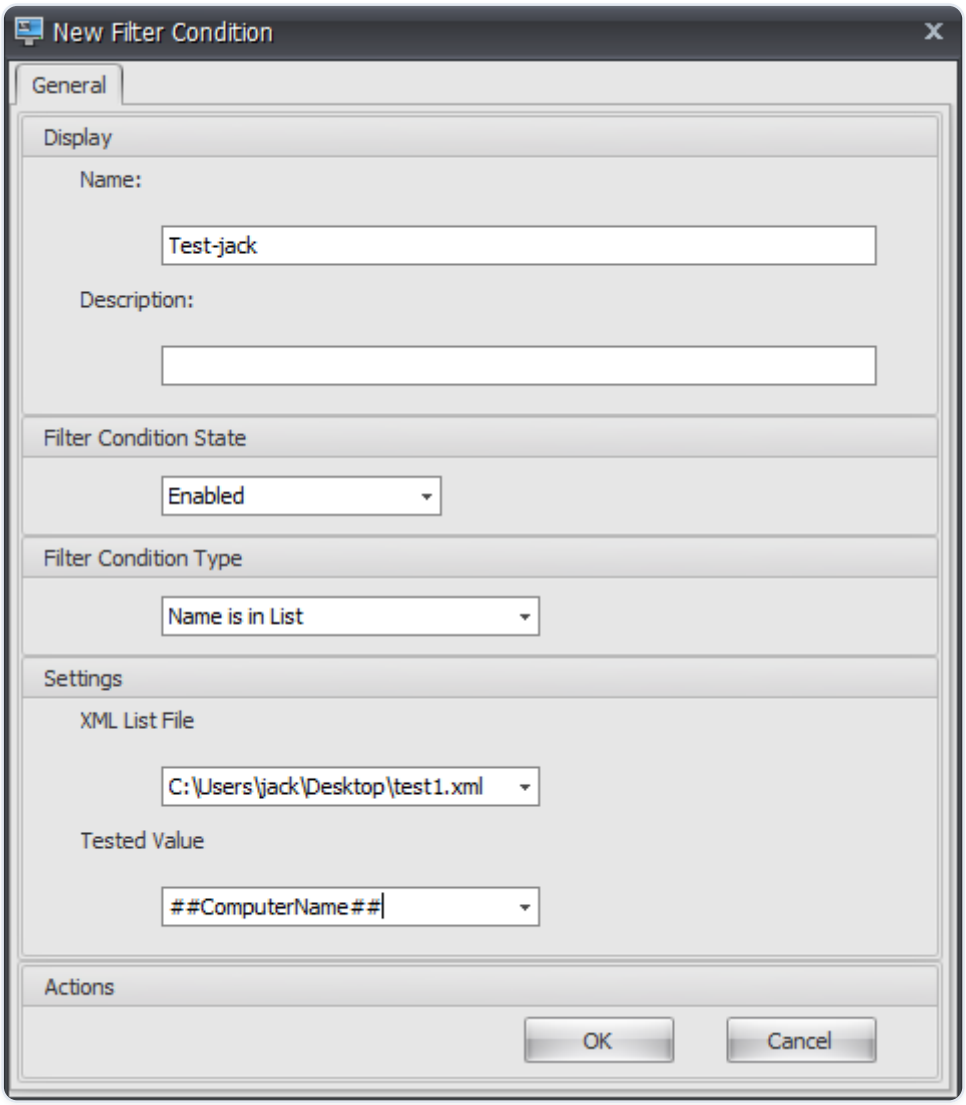
7. Go to the **Administration Console \> Filters \> Conditions \> Filter Condition List** tab and then click **Add**.

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



8. Type the information and then click **OK**.

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

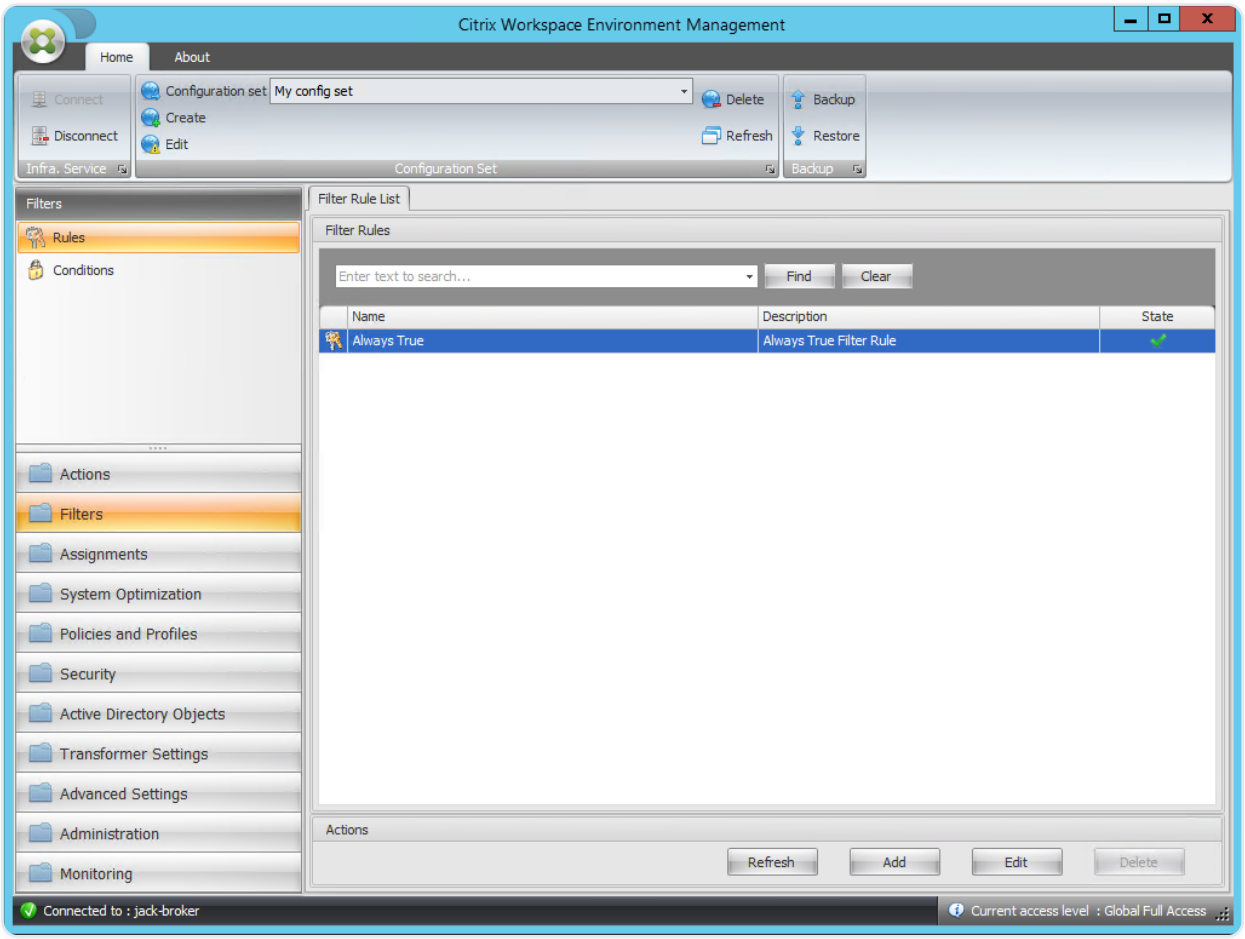


NOTE:

- **Filter Condition Type**. Select **Name is in List**.
- **XML List File**: `C:\Users\<user1>\Desktop\test1.xml` (file address on the agent host)
- **Tested Value**. Type the dynamic token that corresponds to the name you typed in the **Name** field in the WEM Integrity Condition List Manager. In this example, you typed the name of the machine on which the agent is running (agent host). Therefore, you must use the dynamic token "##ComputerName##." For more information about using dynamic tokens, see Dynamic tokens.

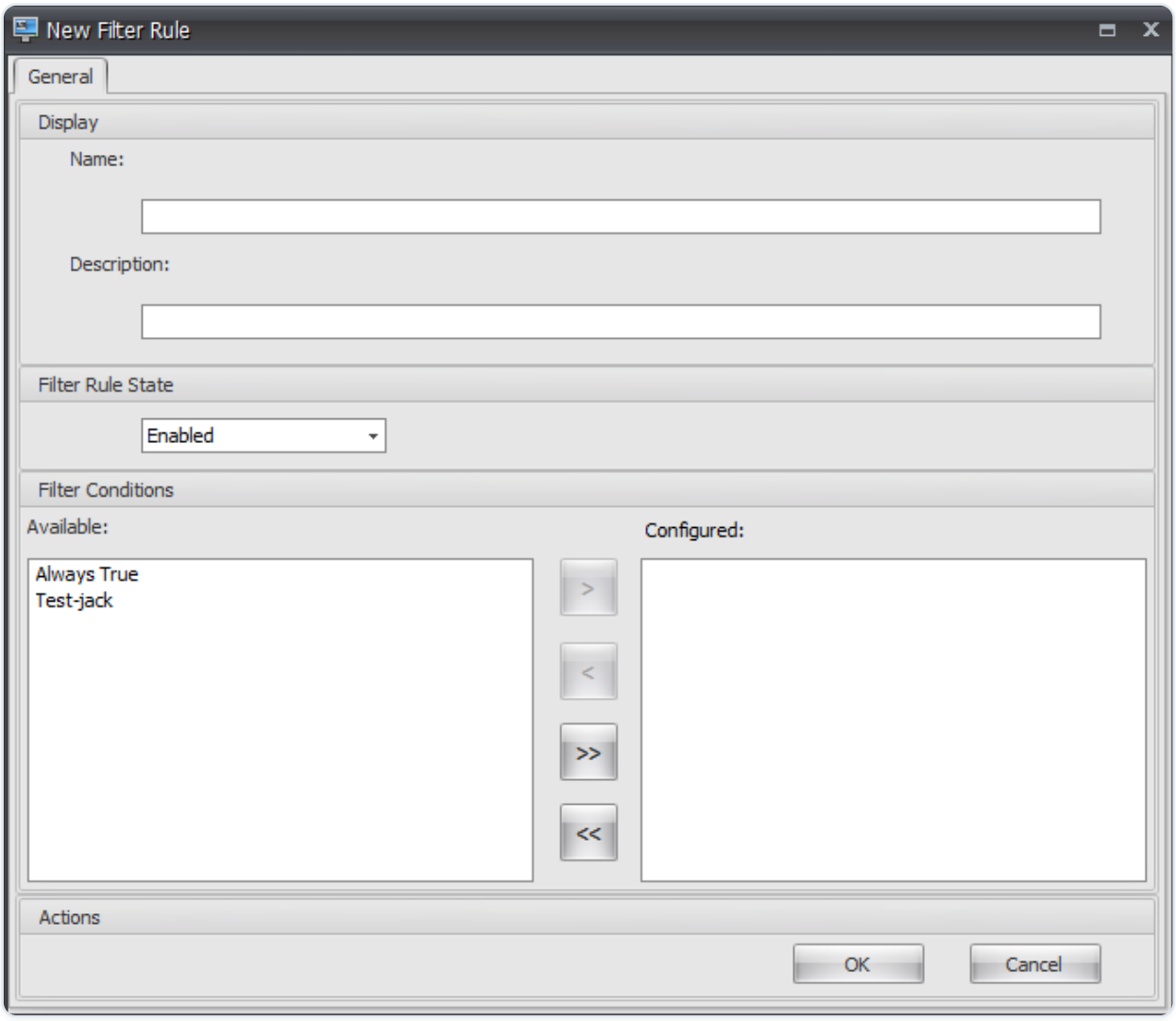
9. Go to the **Administration Console \> Filters \> Rules \> Filter Rule List** tab and then click **Add**.

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



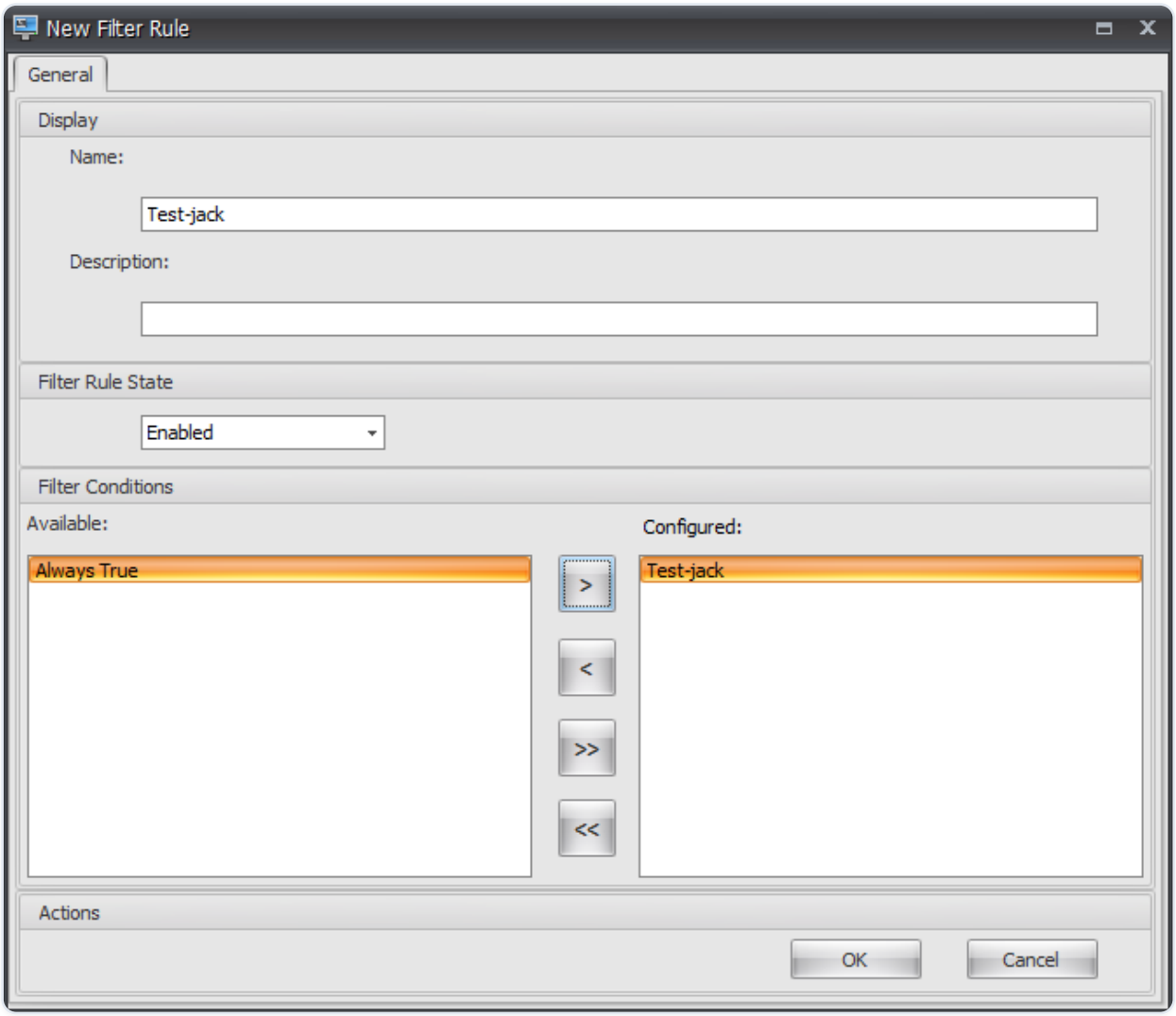
10. Type the filter name in the **Name** field.

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



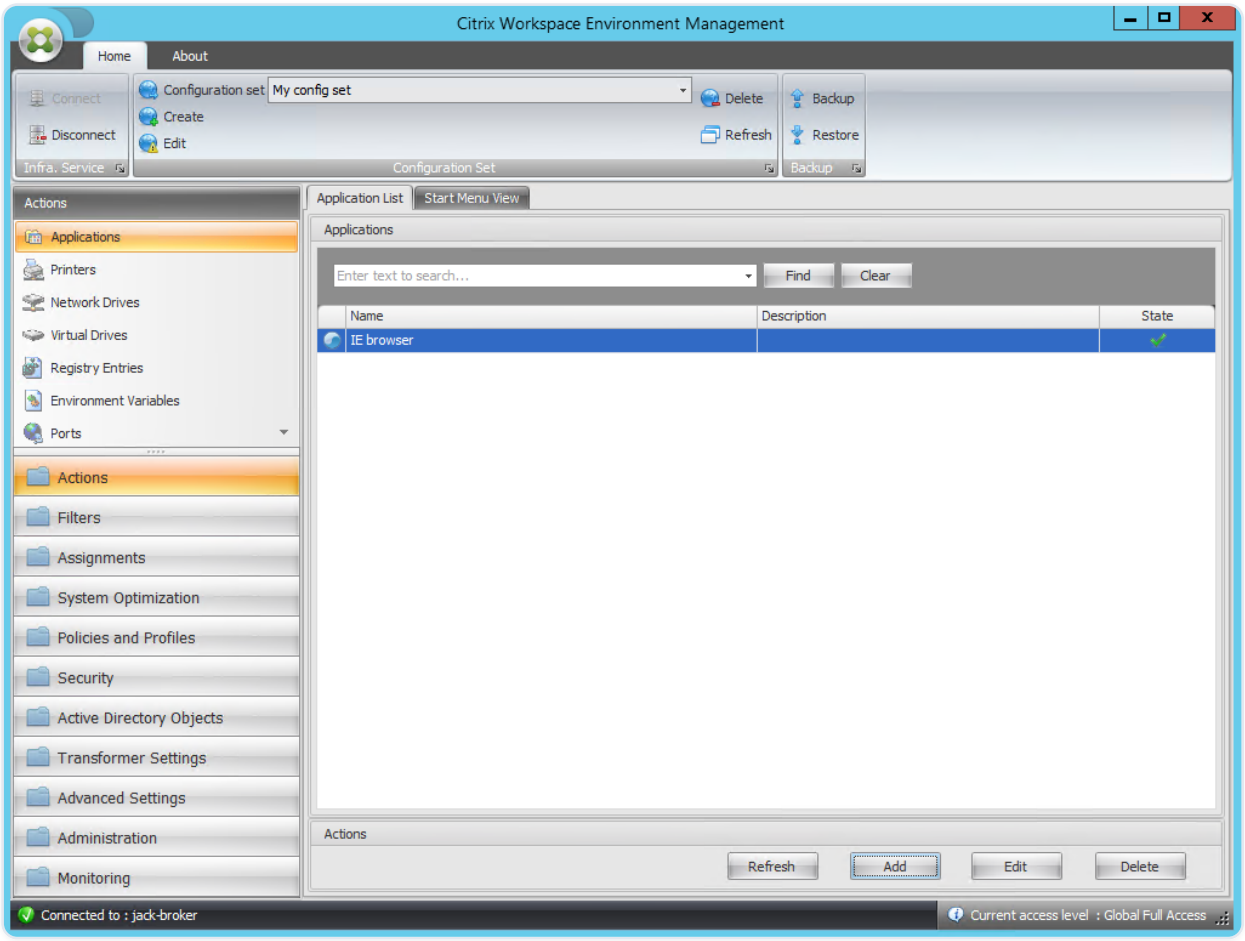
11. Move the configured condition from the **Available** pane to the **Configured** pane and then click **OK**.

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



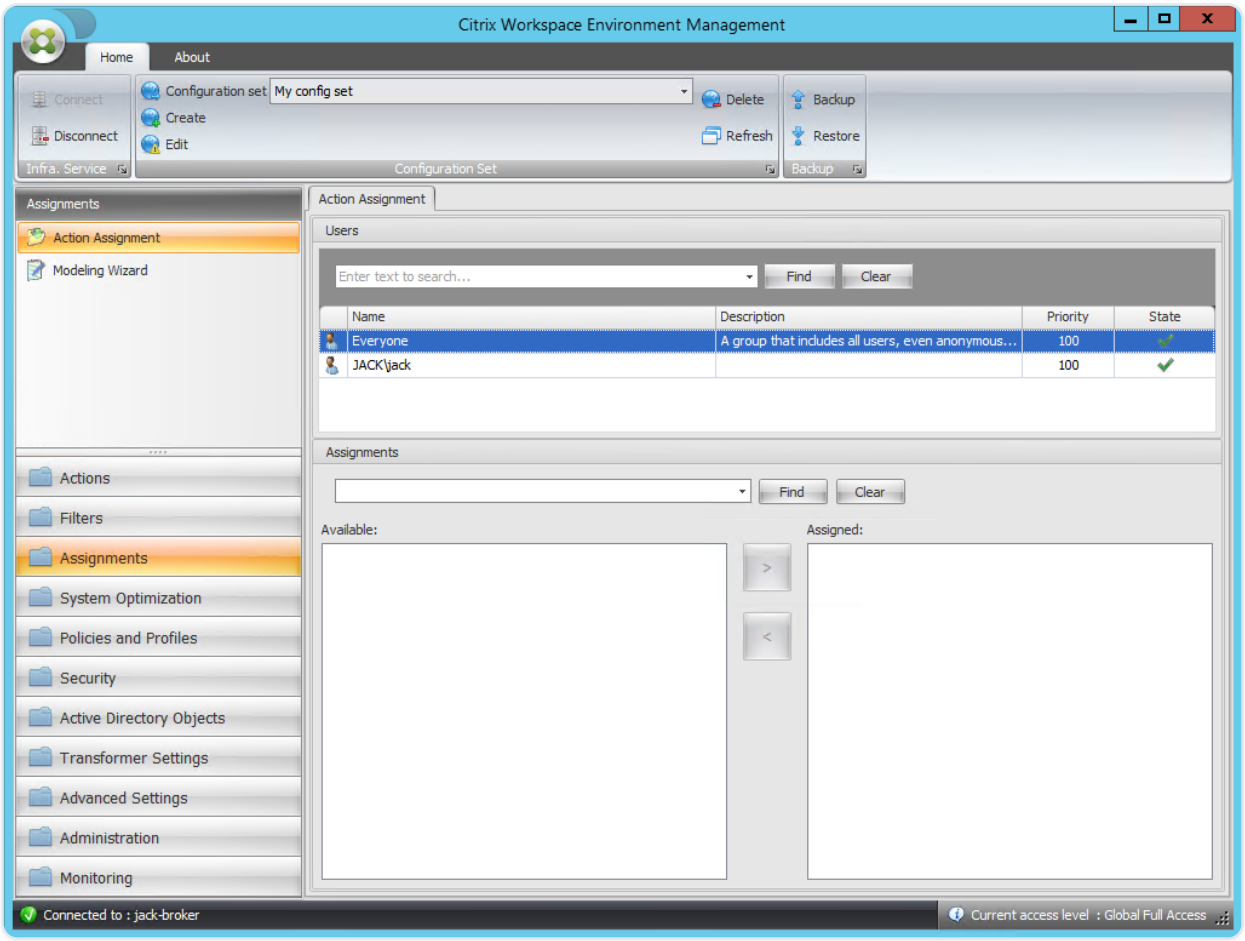
12. Go to the **Administration Console \> Actions \> Applications \> Application List** tab and then add an application.

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



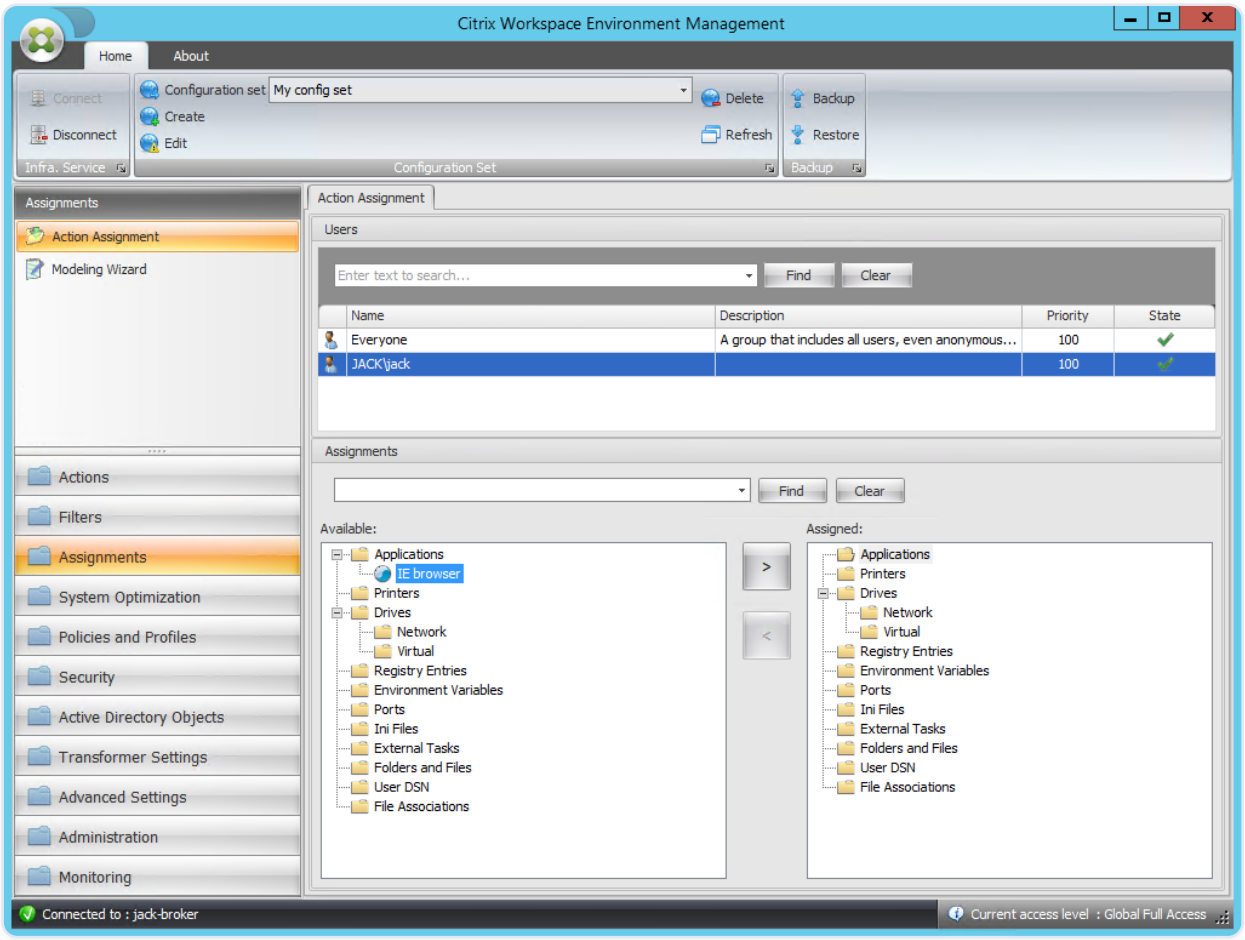
13. Go to the **Administration Console \> Assignments \> Action Assignment** tab.

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

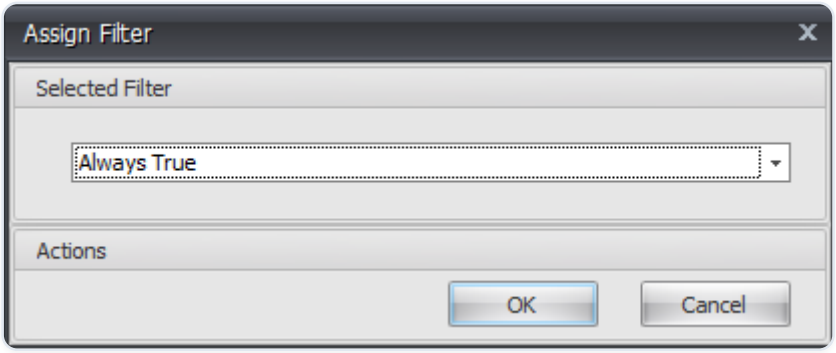


14. Double-click the desired user or user group (in this example, select the agent host).

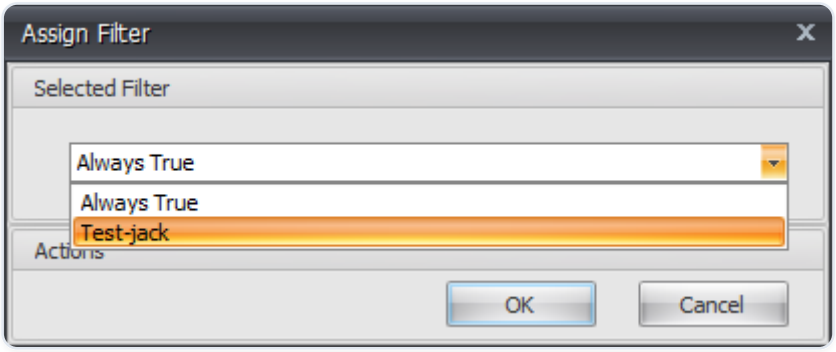
© 1997–2026 Citrix Systems, Inc. All rights reserved.



15. Move the application from the **Available** pane to the **Assigned** pane.

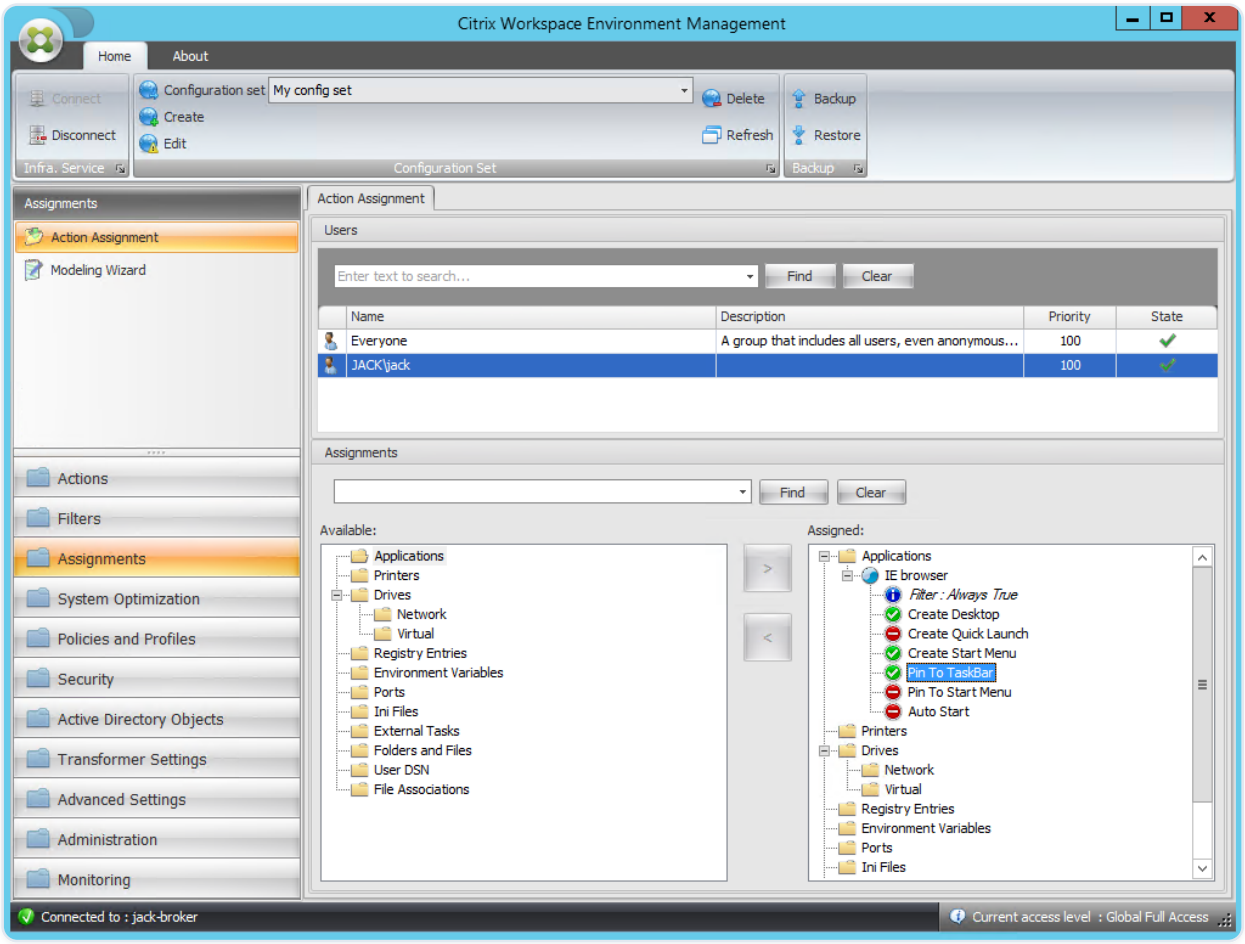


16. Select the filter and then click **OK**.



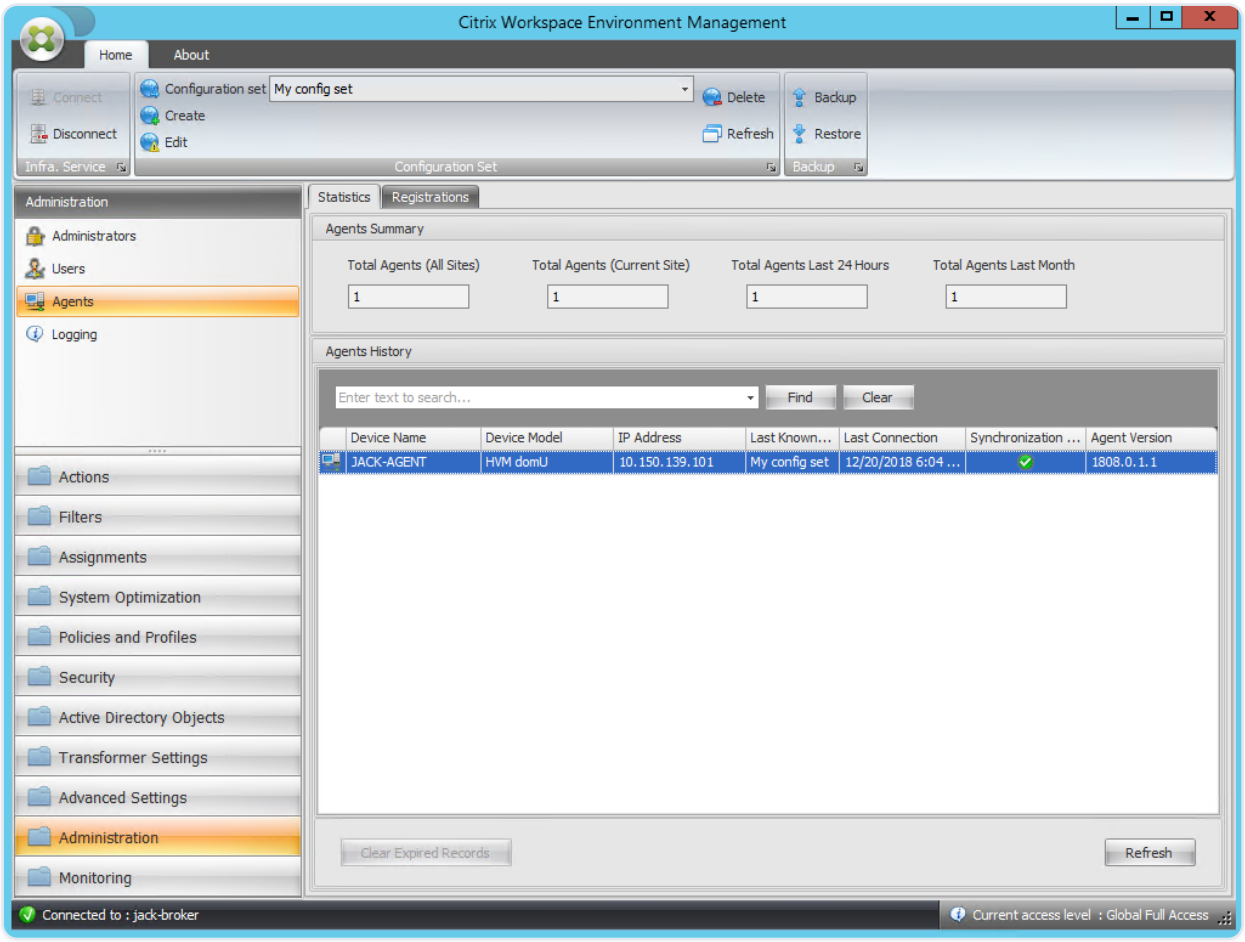
17. Enable the options for the assigned application (in this example, enable **Create Desktop** and **Pin To TaskBar**).

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



18. Go to the **Administration Console \> Administration \> Agents \> Statistics** tab and then click **Refresh**.

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

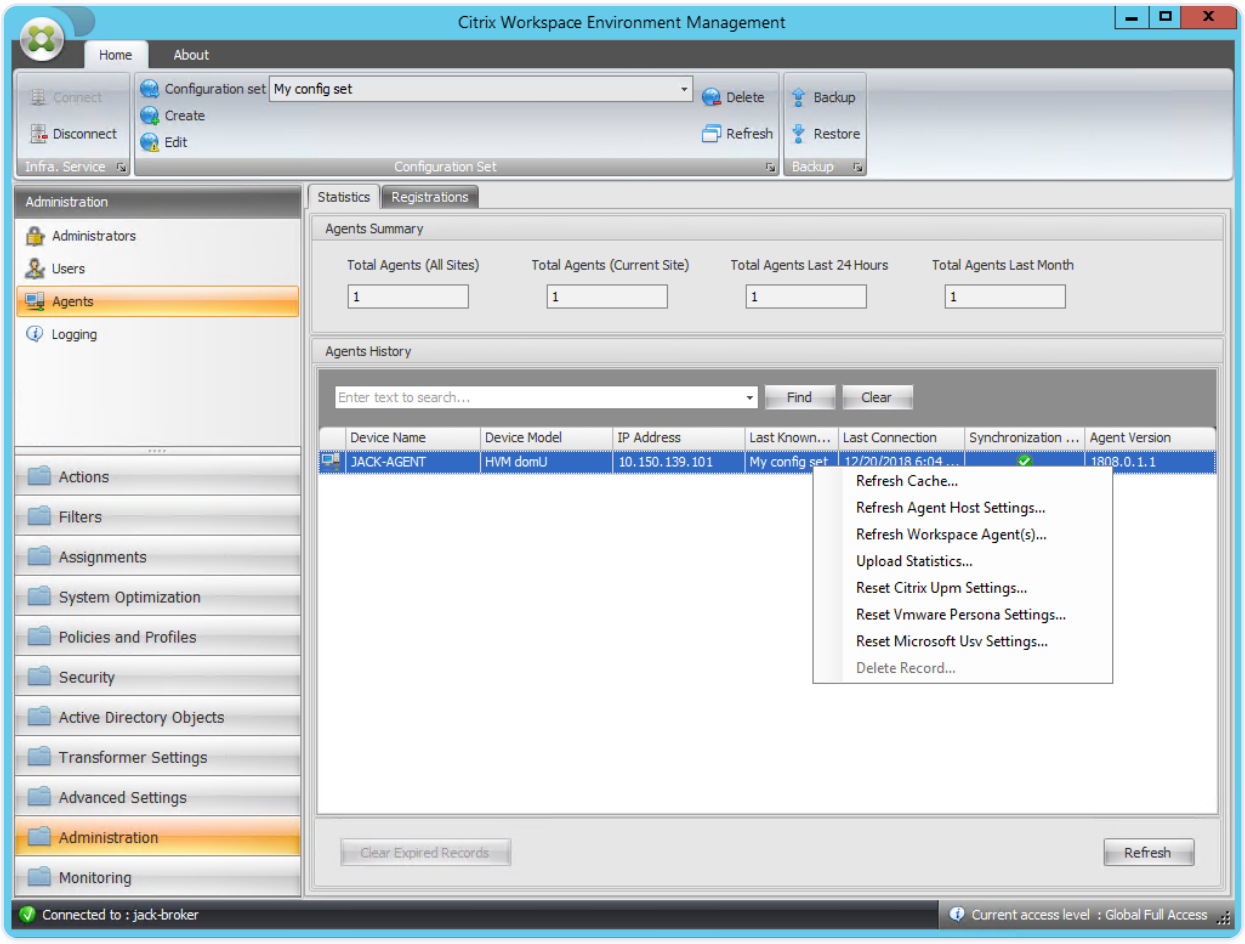


19. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.

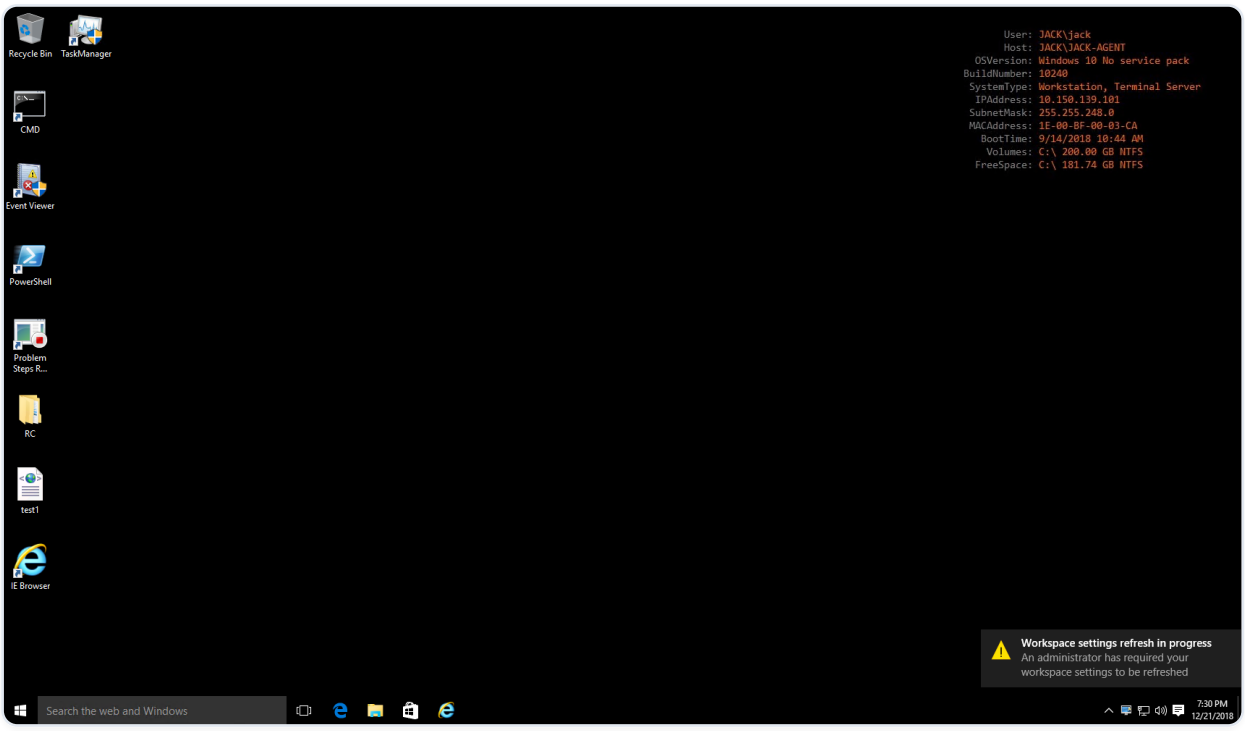
NOTE:

For the settings to take effect, you can also go to the machine on which the agent is running and then refresh Citrix WEM Agent.

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



20. Go to the machine on which the agent is running (agent host) to verify that the configured condition works.



In this example, the application was assigned to the agent machine successfully. It was created on the desktop and pinned to the taskbar.

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

XML printer list configuration

Workspace Environment Management™ includes the ability to configure user printers via an XML printer list file.

After you have created an XML printer list file, create a printer action in the administration console with an **Action Type** option set to **Use Device Mapping Printers File**.

NOTE:

Only printers that do not require specific Windows credentials are supported.

XML printer list file structure

The XML file is encoded in UTF-8, and has the following basic XML structure:

```
<?xml version="1.0" encoding="UTF-8"?>



    <ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">

    ...

    </
ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

Every client and associated device is represented by an object of the following type:

```
SerializableKeyValuePair&lt;string, List&lt;VUEMUserAssignedPrinter>>>
```

Each device is represented like this:

```
    <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

        <Key>DEVICE1</Key>

        <Value>
```

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

```
            <VUEMUserAssignedPrinter>

               ...

            </VUEMUserAssignedPrinter>

        </Value>

    </SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

Each block of devices must be matched to a specific client or computer name. The **\<Key>** tag contains the relevant name. The **\<Value>** tag contains a list of **VUEMUserAssignedPrinter** objects matching the printers assigned to the specified client.

```
    <?xml version="1.0" encoding="utf-8"?>



 <ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema">

        <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

            <Key>DEVICE1</Key>

            <Value>

                <VUEMUserAssignedPrinter>

             ...

                </VUEMUserAssignedPrinter>

            </Value>

        </SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

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

```
        </
ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

VUEMUserAssignedPrinter tag syntax

Each configured printer must be defined in a **\<VUEMUserAssignedPrinter>** tag, using the following attributes:

\<IdPrinter>. This is the Workspace Environment Management printer ID for the configured printer. Each printer must have a different ID. **Note** The XML Printer List action configured in the Workspace Environment Management Administration Console is also a printer action with its own ID which must be different from the ID of printers individually configured in the XML list.

\<IdSite>. Contains the site ID for the relevant Workspace Environment Management site, which must match the ID of an existing site.

\<State>. Specifies the state of the printer where 1 is active and 0 is disabled.

\<ActionType>. Must always be 0.

\<UseExtCredentials>. Must be 0. The use of specific Windows credentials is not currently supported.

\<isDefault>. If 1, printer is the default Windows printer. If 0, it is not configured as default.

\<IdFilterRule>. Must always be 1.

\<RevisionId>. Must always be 1. If printer properties are later modified, increment this value by 1 to notify the Agent Host and ensure the printer action is reprocessed.

\<Name>. This is the printer name as perceived by the Workspace Environment Management Agent Host. This field **cannot** be left blank.

\<Description>. This is the printer description as perceived by the Workspace Environment Management Agent Host. This field can be blank.

\<DisplayName>. This is unused and should be left blank.

\<TargetPath>. This is the UNC path to the printer.

\<ExtLogin>. Contains the name of the Windows account used when specifying Windows credentials for connection. .

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

\<ExtPassword>. Contains the password for the Windows account used when specifying Windows credentials for connection. .

\<Reserved01>. This contains advanced settings. **Do not** alter it in any way.

```
&gt;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;SelfHealingEnabled&lt;/
Name&gt;&lt;Value&gt;0&lt;/Value&gt;&lt;/VUEMActionAdvancedOption
```

To activate self-healing for a given printer object, simply copy and paste the above contents, changing the highlight **0** value to **1**.

Example printer object

The following example assigns two active printers on the client or computer **DEVICE1**:

- **HP LaserJet 2200 Series** on UNC path `\\server.example.net\HP LaserJet 2200 Series` (default printer)
- **Canon C5531i Series** printer on UNC path `\\server.example.net\Canon C5531i Series`

It also assigns one active printer on the client or computer DEVICE2:

- **HP LaserJet 2200 Series** on UNC path `\\server.example.net\HP LaserJet 2200 Series`

```
<?xml version="1.0" encoding="utf-8"?>

  <ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema">

    <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

        <Key>DEVICE1</Key>

        <Value>

            <VUEMUserAssignedPrinter>

                <IdPrinter>1</IdPrinter>

                <IdSite>1</IdSite>
```

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

```
                <State>1</State>

                <ActionType>0</ActionType>

                <UseExtCredentials>0</UseExtCredentials>

                <isDefault>1</isDefault>

                <IdFilterRule>1</IdFilterRule>

                <RevisionId>1</RevisionId>

                <Name>HP LaserJet 2200 Series</Name>

                <Description />

                <DisplayName />

                <TargetPath>\\server.example.net\HP LaserJet 2200 Series</
TargetPath>

                <ExtLogin />

                <ExtPassword />

                <Reserved01>&lt;?xml version="1.0" encoding="utf-8"?
&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/
XMLSchema"&gt;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;SelfHealingEnabl
ed&lt;/Name&gt;&lt;Value&gt;0&lt;/Value&gt;&lt;/
VUEMActionAdvancedOption&gt;&lt;/ArrayOfVUEMActionAdvancedOption&gt;</
Reserved01>

            </VUEMUserAssignedPrinter>

        </Value>

      <Value>

            <VUEMUserAssignedPrinter>

                <IdPrinter>2</IdPrinter>
```

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

```
                <IdSite>1</IdSite>

                <State>1</State>

                <ActionType>0</ActionType>

                <UseExtCredentials>0</UseExtCredentials>

                <isDefault>0</isDefault>

                <IdFilterRule>1</IdFilterRule>

                <RevisionId>1</RevisionId>

                <Name>Canon C5531i Series</Name>

                <Description />

                <DisplayName />

                <TargetPath>\\server.example.net\Canon C5531i Series</
TargetPath>

                <ExtLogin />

                <ExtPassword />

                <Reserved01>&lt;?xml version="1.0" encoding="utf-8"?
&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/
XMLSchema"&gt;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;SelfHealingEnabl
ed&lt;/Name&gt;&lt;Value&gt;0&lt;/Value&gt;&lt;/
VUEMActionAdvancedOption&gt;&lt;/ArrayOfVUEMActionAdvancedOption&gt;</
Reserved01>

            </VUEMUserAssignedPrinter>

        </Value></
SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

      <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

        <Key>DEVICE2</Key>
```

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

```
        <Value>
            <VUEMUserAssignedPrinter>
                <IdPrinter>1</IdPrinter>
                <IdSite>1</IdSite>
                <State>1</State>
                <ActionType>0</ActionType>
                <UseExtCredentials>0</UseExtCredentials>
                <isDefault>0</isDefault>
                <IdFilterRule>1</IdFilterRule>
                <RevisionId>1</RevisionId>
                <Name>HP LaserJet 2200 Series</Name>
                <Description />
                <DisplayName />
                <TargetPath>\\server.example.net\HP LaserJet 2200 Series</
TargetPath>
                <ExtLogin />
                <ExtPassword />
                <Reserved01>&lt;?xml version="1.0" encoding="utf-8"?
&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/
XMLSchema"&gt;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;SelfHealingEnabl
ed&lt;/Name&gt;&lt;Value&gt;0&lt;/Value&gt;&lt;/
VUEMActionAdvancedOption&gt;&lt;/ArrayOfVUEMActionAdvancedOption&gt;</
Reserved01>
            </VUEMUserAssignedPrinter>
```

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

```
        </Value></
SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

   </ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

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

Glossary

This article contains terms and definitions used in the Workspace Environment Management™ (WEM) software and documentation.

on-premises term only

Citrix Cloud™ service term only

Admin Broker Port. Legacy term for "administration port".

administration console. An interface that connects to the infrastructure services. You use the administration console to create and assign resources, manage policies, authorize users, and so on.

In Citrix Cloud, the Workspace Environment Management service administration console is hosted on a Citrix Cloud-based Citrix virtual apps™ server. You use the administration console to manage your WEM installation from the service's **Manage** tab using your web browser.

administration port . Port on which the administration console connects to the infrastructure service. The port defaults to 8284 and corresponds to the AdminPort command-line argument.

agent. The Workspace Environment Management agent consists of two components: the agent service and the session agent. These components are installed on the agent host.

Agent Host executable. Legacy term for "session agent".

Agent Host machine. Legacy term for "agent host".

Agent Host service. Legacy term for "agent service".

Agent Broker Port. Legacy term for "agent service port".

Agent Cache Synchronization Port. Legacy term for"cache synchronization port".

agent host. The machine on which the agent is installed.

agent host configuration GPO. The Group Policy Object (GPO) administrative template provided with the agent installation as ADM or ADMX files. Administrators import these files into Active Directory and then apply the settings to a suitable organizational unit.

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

agent port . Listening port on the agent host which receives instructions from the infrastructure service. Used, for example, to force agents to refresh from the administration console. The port default is 49752.

agent service. The service deployed on VDAs or on physical Windows devices in Transformer use cases. It is responsible for enforcing the settings you configure using the administration console.

agent service port . A port on which the agent connects to the infrastructure server. The port defaults to 8286 and corresponds to the AgentPort command-line argument.

Agent Sync Broker Port. Legacy term for "cache synchronization port".

broker. Legacy term for "infrastructure service".

Broker account. Legacy term for "infrastructure service account".

Broker server. Legacy term for "infrastructure server".

Broker Service Account. Legacy term for "infrastructure service account".

cache synchronization port . A port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server. The port defaults to 8285 and corresponds to the AgentSyncPort command-line argument.

Citrix License Server port . The port on which the Citrix License Server is listening and to which the infrastructure service then connects to validate licensing. The port default is 27000.

Citrix Cloud Connector™ . Software which allows machines in resource locations to communicate with Citrix Cloud. Installed on at least one machine (cloud connector) in each resource location.

configuration set. A set of Workspace Environment Management configuration settings.

Connection Broker. Legacy term for "infrastructure server".

database. A database containing the Workspace Environment Management configuration settings.

In the on-premises version of Workspace Environment Management, the database is created in an SQL Server instance. On Citrix Cloud, the Workspace Environment Management service settings are stored in a Microsoft Azure SQL Database service.

database server account . The account used by the database creation wizard to connect to the SQL instance to create the Workspace Environment Management database.

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

DSN. A data source name (DSN) contains database name, directory, database driver, UserID, password, and other information. Once you create a DSN for a particular database, you can use the DSN in an application to call information from the database.

infrastructure server . The computer on which the Workspace Environment Management infrastructure services are installed.

Infrastructure Server Administration Port. Legacy term for "administration port".

infrastructure service. The service installed on the infrastructure server which synchronizes the various back-end components (SQL Server, Active Directory) with the front-end components (administration console, agent host). This service was previously called the "broker."

On Citrix Cloud, the infrastructure services are hosted on Citrix Cloud and managed by Citrix. They synchronize the various back-end components (Azure SQL Database service, administration console) with the front-end components (agent, Active Directory).

infrastructure service account . The account which the infrastructure service uses to connect to the database. By default this account is the vuemUser SQL account, but during database creation you can optionally specify other Windows credentials for the infrastructure service to use.

Infrastructure service server. Legacy term for "infrastructure server".

infrastructure services. Services installed on the infrastructure server by the infrastructure services installation process.

On Citrix Cloud, the infrastructure services are hosted on Citrix Cloud and managed by Citrix. They synchronize the various back-end components (Azure SQL Database service, administration console) with the front-end components (agent, Active Directory).

initial administrators group . A user group which is selected during database creation. Only members of this group have Full Access to all Workspace Environment Management sites in the administration console. By default this group is the only group with this access.

integrated connection . Connection of the database creation wizard to the SQL instance using the current Windows account instead of an SQL account.

kiosk mode. A mode in which the agent becomes a web or application launcher redirecting users to a single app or desktop experience. This allows administrators to lock down the user environment to a single app or desktop.

Monitoring Broker Port. Legacy term for"WEM monitoring port".

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

mixed-mode authentication . In SQL Server, an authentication mode that enables both Windows Authentication and SQL Server Authentication. This is the default mechanism by which the infrastructure service connects to the database.

License server port. Legacy term for "Citrix License Server port".

network drive. A physical storage device on a LAN, a server, or a NAS device.

resource location . A location (such as a public or private cloud, a branch office, or a data center) containing the resources required to deliver services to your subscribers.

SaaS . *Software as a service* is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.

self-service window. An interface in which end users can select functionality configured in Workspace Environment Management (for example icons, default printer). This interface is provided by the session agent in "UI mode."

service principal name (SPN). The unique identifier of a service instance. SPNs are used by Kerberos authentication to associate a service instance with a service logon account.

session agent. An agent that configures app shortcuts for user sessions. The agent operates in "UI mode" and "command line" mode. UI mode provides a self-service interface accessible from a status bar icon, from which end users can select certain functions (for example icons, default printer).

Site. Legacy term for "Configuration set".

SQL user account . An SQL user account with name of "vuemUser" created during installation. This is the default account that the infrastructure service uses to connect to the database.

transformer. A feature in which Workspace Environment Management agents connect in a restricted kiosk mode.

virtual drive. A Windows virtual drive (also called an MS-DOS device name) created using the **subst** command or the **DefineDosDevice** function. A virtual drive maps a local file path to a drive letter.

virtual IP address (VIP). An IP address that does not correspond to an actual physical network interface (port).

VUEM. Virtual User Environment Management. This is a legacy Norskale term that appears in some places in the product.

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

vuemUser . An SQL account created during Workspace Environment Management database creation. This is the default account that the Workspace Environment Management infrastructure service uses to connect to the database.

WEM Broker. Legacy term for "infrastructure service".

WEM monitoring port . A listening port on the infrastructure server used by the monitoring service. The port defaults to 8287. (Not yet implemented.)

WEM UI Agent executable. Legacy term for "session agent".

Windows account impersonation. When a service runs under the identity of a Windows account.

Windows AppLocker. A Windows feature that allows you to specify which users or groups can run particular applications in your organization based on unique identities of files. If you use AppLocker, you can create rules to allow or deny applications from running.

Windows authentication. In SQL Server, the default authentication mode in which specific Windows user accounts and group accounts are trusted to log in to SQL Server. An alternate mode of authentication in SQL Server is mixed mode authentication.

Windows security. Legacy term for "Windows authentication".

Workspace Environment Management (WEM) service . A Citrix Cloud service which delivers WEM management components as a SaaS service.

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

Workspace Environment Management™ Document History

The following table describes the important changes to the Workspace Environment Management 2603 documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
30 Apr 2026	Initial release of Workspace Environment Management 2603	What's new in Workspace Environment Management

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