Workspace Environment Management™ service

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

Contents

Workspace Environment Management™ service 6

What's new 9

Deprecation 86

Third party notices 87

Known issues 87

Known issues in previous releases 88

System requirements 113

Limits 116

Get started: Plan and build a deployment 117

Install agents 120

Enroll agents 134

Upgrade 143

Migrate 145

Manage (legacy console) 150

Ribbon 156

Actions 160

Action Groups 161

Group Policy Settings 172

Applications 179

Printers 187

Network Drives 188

Virtual Drives 189

Registry Entries 190

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

Environment Variables 193

Ports 193

Ini Files 195

External Tasks 196

File System Operations 200

User DSN 201

File Associations 202

Filters 207

Assignments 210

System Optimization 212

CPU Management 212

Memory Management 218

I/O Management 220

Fast Logoff 221

Citrix Optimizer 222

Multi-session Optimization 225

Policies and Profiles 226

Environmental Settings 226

Microsoft USV Settings 228

Citrix Profile Management Settings 229

Security 239

Active Directory Objects 257

Transformer Settings 261

Advanced Settings 265

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

Administration 275

Monitoring 281

Manage (web console) 283

Home page 284

Configuration Sets 286

Actions 292

Security 344

Assignments 352

Triggers 367

System Optimization 373

Profiles 387

Scripted Tasks 406

App package delivery 409

Advanced settings 413

Transformer settings 427

Directory Objects 431

Monitoring 436

Administration 437

Insights 449

Reports 452

Logging 459

Scripts for scripted tasks 461

Files 483

Enrollment 484

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

Enrolled Agents 484

Invitation 486

Access control 491

Manage non-domain-joined machines 494

Manage Basic Deployment agents 495

Upload files 502

REST APIs 504

Accelerate logon performance using Citrix Environment Tool Hub and WEM 504

Aggregate assigned applications in one place 510

Analyze logon duration using scripted tasks 514

Analyze logon performance using Citrix Environment Tool Hub 526

Automatically apply Windows updates using scripted tasks 536

Automatically back up configuration sets using WEM APIs and Windows PowerShell 541

Configure file type associations 549

Configure FSLogix Profile Container using WEM GPO 552

Configure MSIX app attach using scripted and external tasks 560

Configure Profile Management health check 568

Configure SMB shares for Profile Management to use 572

Configure startup and shutdown triggers for scripted tasks 576

Manage DaaS-provisioned non-domain-joined machines using WEM 581

Migrate FSLogix profiles to Citrix Profile Management 585

Protect Citrix Workspace™ environments using process hierarchy control 592

Troubleshoot Login Time Issues Using Citrix Environment Tool Hub and WEM 599

Troubleshoot scripted task execution problems in Monitor 609

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

Troubleshoot unregistered VDAs using scripted tasks in Monitor **612**

Troubleshoot VDA registration and session launch issues using scripted tasks **618**

Use Windows events as triggers to detect VDA registration issues **623**

Agent event logs **627**

Agent Insights **635**

Agent in CMD and UI mode **639**

Agent-side refresh operations **641**

Citrix Environment Tool Hub **642**

Common Control Panel applets **666**

Customer data management **669**

Dynamic tokens **670**

Environmental Settings registry values **680**

Filter conditions **703**

Log parser **719**

Port information **720**

WEM health check tool **721**

XML printer list configuration **723**

Glossary **728**

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

Workspace Environment Management™ service

September 7, 2025

> **Note:**
>
> - The Workspace Environment Management service is available globally, with US-based, EU-based, and Asia Pacific South based instances. We are working to enable Workspace Environment Management service instances in more regions.
> - Workspace Environment Management service is also available in Citrix Cloud Japan, a cloud that is isolated and separate from Citrix Cloud. Japanese customers can use the service in a dedicated Citrix-managed environment. For more information, see Citrix Cloud Japan.
> - For information about Workspace Environment Management service customer data storage, retention, and control, see Customer data management.
> - Since July 2023, Microsoft has renamed Azure Active Directory (Azure AD) to Microsoft Entra ID. In this document, any reference to Azure Active Directory, Azure AD, or AAD now refers to Microsoft Entra ID.

Introduction

The Workspace Environment Management service uses intelligent resource management and Profile Management technologies to deliver the best possible performance, desktop logon, and application response times for the following deployments:

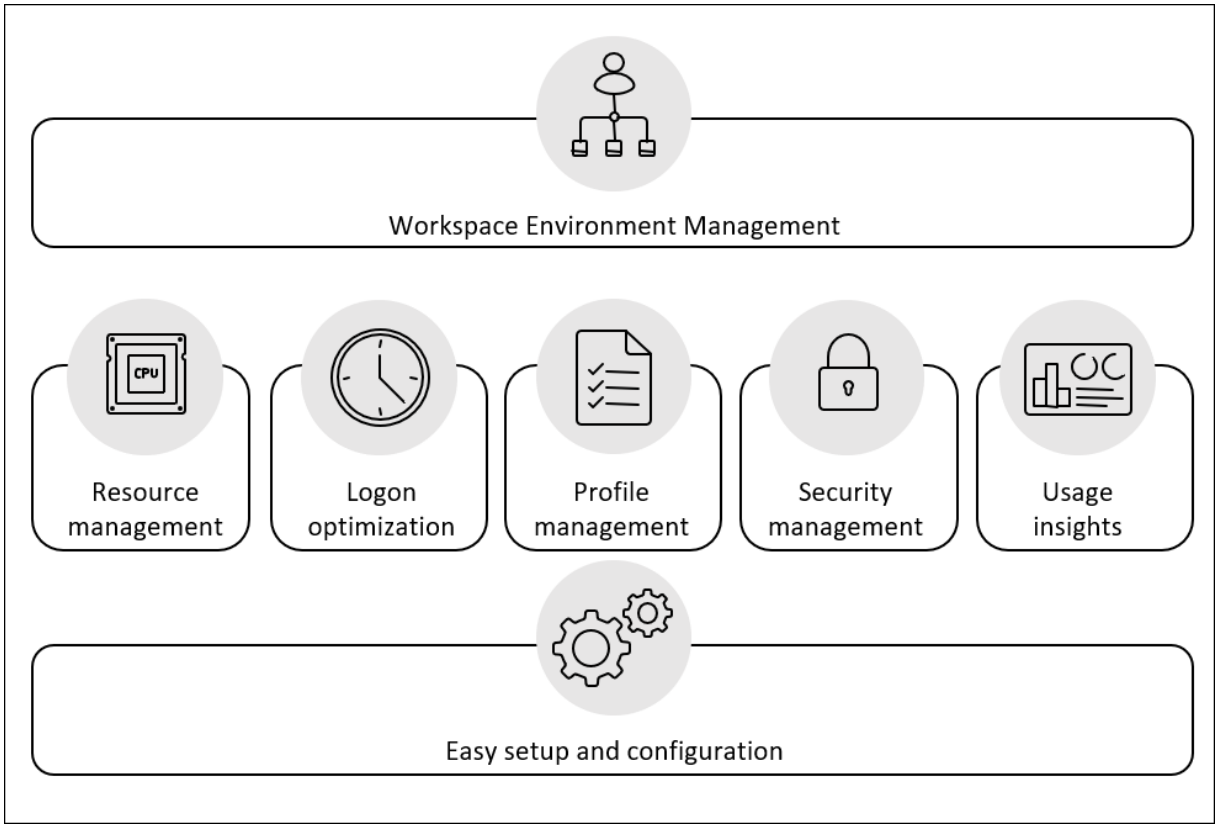
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) and Citrix Virtual Apps and Desktops

It is a lightweight, scalable user environment management solution that simplifies IT administration and optimizes desktops for the best possible user experience.

> **Important:**
>
> To manage Azure Virtual Desktop with the Workspace Environment Management service, you must purchase the Citrix Optimization Pack.

The following are highlights of the Workspace Environment Management service:

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



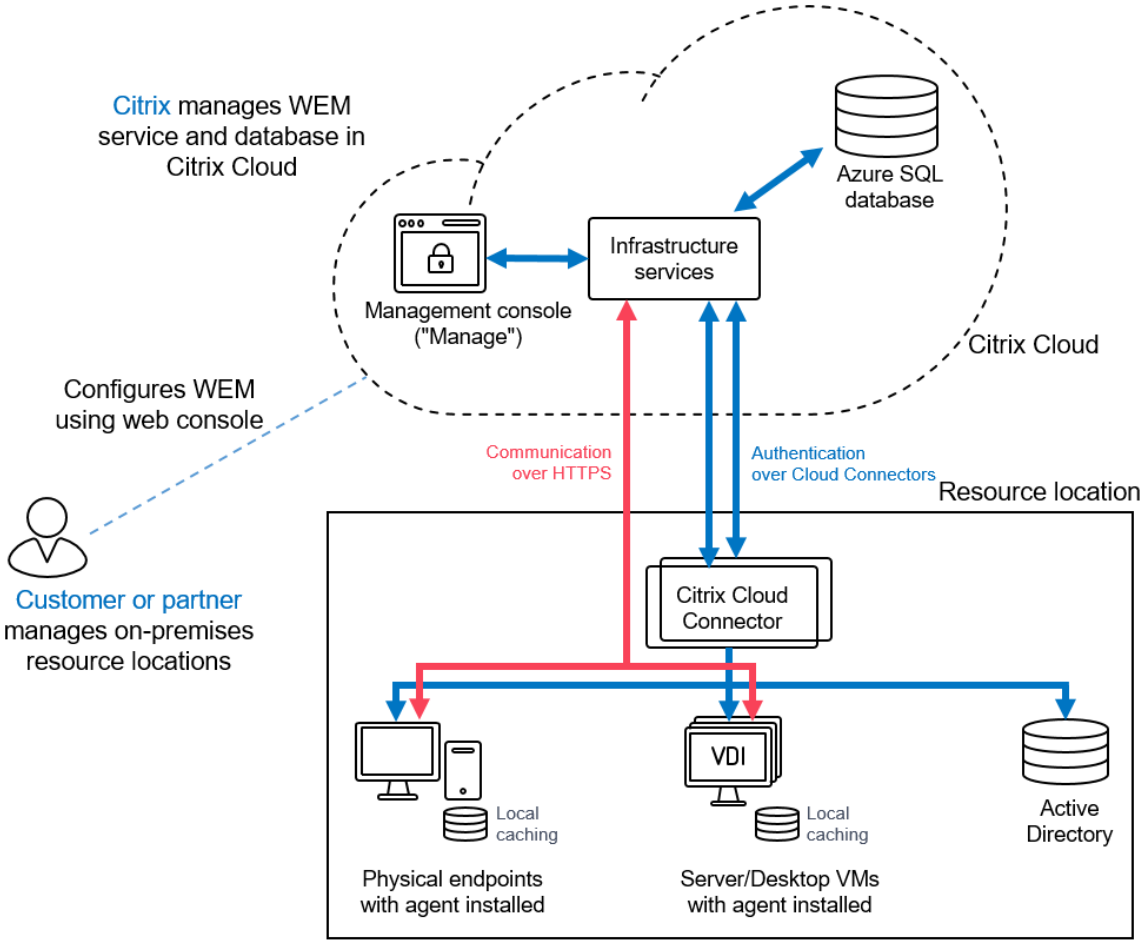
- **User workspace management**
  - Manages applications, printers, network drives, external tasks, and more
  - Filters assignments
- **User resources management**
  - Monitors and analyzes application behavior in real time
  - Adjusts RAM, CPU, and I/O intelligently in the user environment
  - Preserves the amount of resources required by applications in focus
  - Throttles background processes without compromising the user experience
  - Improves application responsiveness
- **User profiles management**
  - Uses Citrix Profile Management to manage user profiles across sessions and endpoints
- **Logon performance optimization**
  - Delays unessential processes from the logon process to improve logon times
  - Applies logon-related configuration in the background, after a user logs on
- **Easy setup and configuration**

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

- Eliminates most of the setup tasks that the on-premises version of Workspace Environment Management requires

Technical overview

Workspace Environment Management (WEM) service has the following architecture:



The following components are hosted in Citrix Cloud™ and administered by Citrix as part of the service:

- **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). We ensure that sufficient infrastructure services are provided on Citrix Cloud.
- **Administration console**. You use the administration console, available on the service's **Manage** tab, to manage your user environment using your web browser. The administration console is hosted on a Citrix Cloud-based Citrix virtual Apps™ server. The server provides a Citrix

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

Workspace™ app for HTML5 connection to the administration console.

- **Azure SQL Database**. Workspace Environment Management service settings are stored in a Microsoft Azure SQL Database service, deployed in an elastic pool. This component is managed by Citrix.

The following components are installed and managed in each resource location by the customer/partner:

- **Agent**. The Workspace Environment Management service agent connects to the Workspace Environment Management infrastructure services and enforces the settings you configure in the administration console. All communications are over HTTPS using the Citrix Cloud Messaging Service. 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.

  All agents use local caching, ensuring that agents can continue using the latest settings if the network connection is interrupted.

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

- **Microsoft Active Directory Server**. The Workspace Environment Management service requires access to your Active Directory to push settings to your users. The infrastructure service communicates with your Active Directory using the Citrix Cloud identity service.
- **Cloud Connector**. The Citrix Cloud Connector™ is required to allow machines in your resource locations to communicate with Citrix Cloud. Install Citrix Cloud Connector on at least one machine in every resource location that you are using. For continuous availability, install multiple Cloud Connectors in each of your resource locations. We recommend at least two Cloud Connectors in each resource location to ensure high availability. If one Cloud Connector is unavailable for any period of time, the other Cloud Connectors can maintain the connection.

Get started

To set up a Workspace Environment Management deployment, see Build a deployment.

To install the agent, see Install and configure.

What's new

September 1, 2026

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

A goal of Citrix® is to deliver new features and product updates to Workspace Environment Management™ (WEM) service customers when they are available. New releases provide more value, so there is no reason to delay updates. Updates are rolled out to the service release approximately every four weeks.

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

In general, updates to the documentation are made available before new features and product updates are accessible to all customers.

For information about the service level goal for the WEM service for cloud scale and service availability, see Service Level Goals. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

September 2026

Self-healing for Group Policy settings

With the new **Enforce processing of GPOs** option under **Process GPOs**, the WEM agent automatically reprocesses Group Policy settings on every refresh cycle, even when no configuration changes are detected. Reprocessing corrects any drift on the agent machine and keeps policies consistently enforced.

For more information, see Group Policy settings.

- Minimum agent version required: 2608

Privilege elevation for applications on network shares and mapped drives

In addition to local drives, the **Privilege elevation** security feature now supports applications hosted on UNC paths (network shares) or mapped drives.

You can create executable, MSI, and self-elevation rules (using path, publisher, or hash criteria) for these applications. To evaluate publisher or hash criteria on files that the agent service cannot read directly, WEM reads the file in the user's session context, so applications on network shares and mapped drives are matched and elevated the same way as local applications.

This feature applies only to Citrix Virtual Apps and Desktops deployments. For more information, see Privilege elevation.

- Minimum agent version required: 2608

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

Improved administrative template (ADMX/ADML) import

When you import GPO administrative templates in the WEM web console, your files are now validated before upload, with clear feedback identifying which files have issues, such as:

- Unpaired ADMX or ADML files.
- Duplicate ADML files (each ADMX supports only one ADML language folder).
- Schema (XSD) or parsing errors.

If some templates fail validation, those that pass are still imported, and the failed templates are listed by name.

For more information, see Import templates.

Configuration templates

You can now apply configuration templates in the WEM web console. Templates provide reusable, pre-defined settings that standardize configurations across sites and environments and reduce repetitive configuration tasks.

For more information, see Apply recommended settings.

Fixes

- The Ivanti Migration tool might lose certain GPO configurations during migration when non-standard GPO types are present. [WEM-53554]

July 2026

Administrative logging

You can now track all configuration changes made by any administrators in the WEM web console using administrative logging. Each log entry captures the identity of the administrator who performed the action, the affected object, the operation type, and a before-and-after change summary.

Logs are retained for 180 days, with a maximum of 100,000 records. Your role controls log visibility: WEM Full administrators can view all logs, and WEM Restricted administrators can view logs scoped to their assigned configuration sets.

For more information, see Logging.

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

Modeling wizard

The Modeling Wizard helps you understand what WEM actions and security apply to a specific user. Select a user to instantly see all assigned items organized by action type, along with the user's group membership and OU placement in the directory.

For more information, see Modeling wizard.

Summary view on the Reports page

The **Reports** page now includes a **Summary** view that displays four charts: **Event type**, **Action processing results**, **Configuration set**, and **Script execution results**, giving you a quick statistical overview of your report data.

For more information, see Summary view.

Enhancements to the Profile tab in Agent Insights

The **Profile** tab in Agent Insights now supports a broader range of user profile types, beyond profile containers. It also shows real-time scan progress with an estimated time remaining while profile data is being refreshed.

For more information, see Agent Insights.

New built-in scripts for AOT diagnostics and log collection

WEM now includes five new built-in scripts to help you diagnose and collect Citrix Always On Tracing (AOT) and diagnostic data:

- **Diagnose Citrix AOT issues**: Validates Citrix Always On Tracing (AOT) configuration, diagnoses common issues, and generates an AOT diagnostic report to support troubleshooting.
- **Collect Citrix diagnostic logs**: Collects Citrix AOT logs and Windows Event Logs from the VDA and saves them as a timestamped ZIP file.
- **Collect Windows Event Logs**: Collects Windows Event Logs from the Virtual Delivery Agent (VDA) and saves them as a timestamped ZIP file.
- **Collect Citrix Scout diagnostics**: Runs ScoutCLI.exe to collect Citrix diagnostic data from the VDA and saves the output as a timestamped ZIP file.

For more information, see Scripts for scripted tasks.

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

Fixes

- The WEM Agent might consume excessive resources during session launch when the Logoff External Task trigger is enabled and many GPOs are configured. [WEM-51116]

June 2026

Transformer settings

You can now configure transformer settings directly through the WEM web console. For more information, see Transformer settings.

Environment settings

You can now configure environment settings directly through the WEM web console. To migrate existing configurations from the legacy console, use the built-in migration experience. For more information, see Environment settings.

Profile Management

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

- **Enable BindLink redirection**. If enabled, Profile Management uses the Microsoft BindLink API to handle file system redirections within profile containers. This feature is supported only on Windows 11 24H2, Windows Server 2025, or later.

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

April 2026

Enhanced logon duration diagnostics

You can now view more detailed logon diagnostics through improved metric organization. Shell Startup–related metrics have been enhanced with clearer structure, descriptions, and consolidated guidance, making it easier to identify and troubleshoot logon performance delays. For more information, see Windows Logon Analysis.

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

Create external tasks directly from scripts

You can now create external tasks directly from existing scripts. This enhancement simplifies script reuse by allowing you to quickly generate external tasks from the **Scripted Tasks** page, improving manageability and efficiency. For more information, see Create an external task from a script.

New Profile Management health check tools in Citrix Environment Tool Hub

Citrix Environment Tool Hub now includes two new tools to help you maintain a healthy Profile Management environment:

- **Profile Management Log Parser**: Analyzes log files and surfaces session-level details, detected errors, and active policy settings to help you resolve profile issues faster.
- **Profile Management Health Check**: Scans your local configuration, policy settings, and event logs, then presents the results with health status indicators and remediation recommendations to help you proactively catch and fix misconfigurations.

For more information, see Profile Management Log Parser and Profile Management Health Check.

Fixes

- The `gpt.ini` file might become corrupted when an external task is configured with a **logoff** trigger. As a result, local group policies might not apply correctly. [WEM-50049]

March 2026

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.

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 Manage Active Directory objects.

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

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 allows the user profile to be resumed after the machine recovers from hibernation, ensuring session continuity.

  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.

January 2026

Run scripted tasks in a logged-on user session

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, see Add a scripted task.

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.

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.

Migrate legacy action groups to assignment groups

You can now migrate action groups from the legacy console to assignment groups in the web console. This capability provides a quick, seamless way to move existing configurations and adopt the modern interface without disruption. For more information, see Migrate legacy action groups to assignment groups.

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

Fixes

- The **Discover Citrix Cloud Connector from CVAD service** WEM Agent policy might not take effect when **Let Machine Creation Services do it automatically** is selected during master image preparation. [WEM-47738]
- Importing AppLocker rules might fail if the rule file size exceeds 100 KB. [WEM-48164]
- The WEM agent might create a DWORD registry key instead of a STRING registry key for `HKCU\Control Panel\Desktop\DragFullWindows`. [WEM-48698]

December 2025

Enhancement to Group Policy Migration Tool

We've enhanced **Group Policy Migration Tool** to include support for migrating Windows shortcut management policies to Workspace Environment Management (WEM). This update makes policy migration more straightforward and boosts administrative efficiency during configuration transitions.

For more information, see Group Policy Migration Tool

New migration tool for Ivanti Workspace Control

You can now use a new tool in Citrix Environment Tool Hub to migrate configurations from Ivanti Workspace Control to Citrix Workspace Environment Management. This migration path reduces manual effort and helps your organization transition smoothly with minimal disruption. After migration, you can manage user environments through WEM's modern, centralized platform for improved flexibility and scalability.

For more information, see Migration Tool for Ivanti Workspace Control.

Fixes

- Restoring configuration might time out when the configuration includes a large number of printers. [WEM-48187]

October 2025

New built-in scripted tasks for easier troubleshooting

You can now use new built-in scripted tasks to simplify diagnostics and reduce manual effort. These tasks automate common troubleshooting actions across your Citrix environment, helping you quickly

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

identify and resolve issues.

The following scripted tasks are now available:

- **AOT Log Collection**: Automates the collection and processing of AOT logs.
- **Check DNS Settings**: Verifies DNS configuration and identifies potential issues.
- **Check RDS License**: Verifies RDS licensing configuration and compliance.
- **Diagnose VDA Unregistration**: Runs diagnostic checks to identify causes of VDA unregistration.
- **Run Profile Management health check:** Examines your Citrix Profile Management configuration and analyzes logs to identify profile-related issues.
- **Set profile reset trigger:** Backs up the user's existing profile to create a clean profile folder on the next logon.

For more information, see Built-in scripted tasks.

Time-range condition template for application security management

A new time-range condition template is now available. You can use this template to define the periods during which application security rules are active, gaining greater control and flexibility to align rule enforcement with your needs.

For more information, see Create filters from templates.

Fixes

- Logon analysis data might not be generated for Azure AD user logons on Azure AD-joined machines. [WEM-45767]
- Importing template-based group policies that contain default values might fail. [WEM-47612]
- Tab functionality does not work in the transformer webpage. [WEM-47420]
- Migration of on-premises database into the WEM cloud service might fail if the database version is less than 2411. [WEM-47677]
- Agent cache synchronization might fail with the following exception: `System.TypeLoadException: Could not load type 'Microsoft.Extensions.Logging.Abstractions.Internal.NullScope'from assembly 'Microsoft.Extensions.Logging.Abstractions, Version=8.0.0.1'`. [WEM-47627]

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

September 2025

Description column in Security rules tables

A new **Description** column is now available in the tables on the **Application security**, **Privilege elevation**, and **Process hierarchy control** pages. The column shows the rule descriptions, making it easier to review and understand configured rules.

Filter conditions support folder paths for delivery groups and machine catalogs

You can now use delivery groups and machine catalogs stored in subfolders as filter conditions. When you create or manage filter conditions using **Delivery group name** or **Machine catalog name**, you can include items in subfolders by specifying the full path in the name.
Example: `Subfolder name\Delivery group name`, `Subfolder name\Machine catalog name`

Enhancements to the Agent Statistics page

The **Agent Statistics** page includes the following improvements:

- A new **MAC address** column is available. To display it, select **Columns to display**, and then select **MAC address**. You can also use the MAC address as a filter criterion, except for agents that do not have unique MAC addresses and have **Use the alternative agent identifier** enabled.
- Three new filter conditions for agent versions: **Does not contain**, **Is earlier than**, and **Is later than**.

Role-Based Access Control support

Workspace Environment Management now supports Role-Based Access Control (RBAC) to help you manage administrative access in large or complex enterprise environments.

This enhancement introduces a granular permissions model that strengthens security and improves operational efficiency. With RBAC, WEM full administrators can delegate specific responsibilities to teams without granting unnecessary levels of access. By giving each administrator only the permissions required for their role, RBAC helps reinforce your organization's security posture, reduce operational risk, and improve administrative agility.

Setting up RBAC involves three steps:

1. **Role designation:** Assign each administrator a role in Citrix Cloud —either WEM Full administrator (unrestricted access) or WEM Restricted administrator (limited access based on scopes). For more information, see Manage administrator permissions.

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

2. **Scope definition:** Define scopes for restricted administrators in the WEM web console. For more information, see Create a scope.
3. **Scope assignment:** Assign scopes to restricted administrators to apply the associated access policies and permissions. For more information, see Assign scopes to a restricted administrator.

Enhanced logon duration diagnostics

You can now view more details for diagnosing logon duration. The metrics User Profile Loading and Group Policy Processing include more sub-metrics and tips that help you identify and resolve issues more effectively. For more information, see Windows Logon Analysis.

Support for configuring default registry values

You can now configure data for the **(Default)** value name under a registry key by leaving the **Value name** field empty. This enhancement expands the range of configurable registry entries and applies in the following scenarios:

- Creating or editing **Registry entries** actions.
- Creating, editing, or importing **Registry-based Group Policy settings** actions

For more information, see Create a registry-based GPO and Add a registry entry.

Rule Generator for App Access Control supports importing FSLogix Apps rule sets

The Rule Generator for App Access Control now supports importing FSLogix Apps rule sets. This enhancement lets you reuse existing FSLogix configurations to quickly create equivalent App Access Control rules, simplifying migration and ensuring consistent application access rules. For more information, see Import FXLogix rule sets.

Fixes

- Script-based external tasks configured with the **Run Once** setting might still run multiple times instead of only once. [WEM-46555]
- The first user logon might experience a delay due to an Active Directory query timeout. [WEM-46640]

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

July 2025

Agent Insights panel

This release introduces **Agent Insights**, a new feature in the WEM agent that helps you and your users monitor and troubleshoot session performance, profile container usage, and logon activity. Users can open the panel from the agent icon in the notification area to view detailed metrics that help identify and troubleshoot issues quickly.

The release also includes new settings to control how the panel is displayed and how agent-generated reports are collected and stored.

For more information, see Agent Insights.

Reporting for script-based external tasks

You can now view execution result reports for script-based external tasks directly in the WEM web console. This enhancement improves visibility across your environment, helping you track task success or failure more easily. By reducing the need to check logs manually, it streamlines monitoring and supports faster issue resolution.

For more information, see Enable and view reports for script-based external tasks.

Simplified privilege elevation for domain-joined environments

Privilege elevation no longer requires assigning accounts to specific Active Directory groups. Previously, accounts had to be members of groups such as **Authenticated Users** in the **Pre-Windows 2000 Compatible Access** group and **Enterprise Domain Controllers** in the **Windows Authorization Access Group**. With this enhancement, you can now enable privilege elevation without these group assignments, making security configuration simpler and more flexible.

For more information, see Privilege elevation.

Fixes

- Registry updates might time out during bulk operations. [WEM-44587]
- Deleting expired users might cause the WEM service to hang or fail if the number of expired users is large. [WEM-42936]
- When you configure application security mode as **Merge**, the WEM service might still operate in **Overwrite** mode. [WEM-45562]

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

June 2025

Support for creating filters from templates

You can now create filters using predefined templates. This enhancement simplifies filter creation by prepopulating conditions. Currently, two templates are available to help you quickly create filters for identifying Citrix Virtual Apps and Citrix Virtual Desktops deployments. For more information, see Create filters from templates.

Increased character limit for condition values

When creating a condition for use in assignment filters, you can now enter up to 10,000 characters in the condition values—up from the previous limit of 256 characters. This enhancement applies to all condition types and gives you more flexibility when defining complex conditions. For more information, see Create a condition.

Improved "View reports"button behavior

The **View reports** button now updates dynamically based on report status. While a report is being generated, the button remains disabled and checks automatically every five seconds for up to 30 seconds. Once the report is ready, the button is enabled. If the report isn't ready after 30 seconds, the button becomes active again, allowing you to retry. This enhancement helps prevent confusion about when a report is available. For more information, see Agents.

May 2025

Scripted task validation tool

Validating scripts within the WEM using scripted tasks previously required you to follow a complex and time-consuming workflow.

You can now use the new scripted task validation tool to quickly validate WEM scripted tasks without requiring a full deployment. This enhancement simplifies script development by allowing you to test and adjust scripts locally, speeding up troubleshooting, and reducing testing time. By validating scripts before rollout, you can ensure greater reliability, improve efficiency, and minimize the risk of user impact.

This feature is applicable to all environments with the WEM agent installed and with version greater than or equal to 2505.1.0.1

For more information, see Validate WEM scripted tasks using scripted task validation tool.

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

Fixes

- When you enable **Run Weekly** for Citrix Optimizer processing, the agent on a non-English system might throw an exception and fail to run the scheduled task. [WEM-43923]
- When you select a high-resolution icon for an application, the agent might display it as blurry or low-resolution. [WEM-43961]

April 2025

Support for importing AppLocker rules in WEM web console

The WEM web Console now supports importing application security rules in bulk using an `AppLocker` XML file. Previously, you had to create rules individually through the console, which was repetitive and inefficient in environments with extensive application control needs.

With the new import interface, you can quickly bring in multiple rules from existing AppLocker configurations, streamlining setup, and improving consistency across environments. For more information, see Import AppLocker rules in WEM web console.

Profile cleanup tool

A profile cleanup tool is now available in the WEM Tool Console. This tool helps you efficiently manage storage space and enhance security by deleting or archiving inactive user profiles. 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 in 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.

  For more information, see Profile Cleanup Tool.

Windows roaming profiles support for Profile Migration Tool

You can now use the Citrix Profile Migration Tool to migrate data from Windows roaming profiles to Citrix container-based profiles. This enhancement makes it easier for you to transition to the Citrix container-based profile solution. For more information, see Profile Migration Tool.

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

Profile Management

Workspace Environment Management now supports all *supported* versions of Profile Management through *2503*:

- **Set profile loading timeout.** With this setting, you can now specify the number of seconds 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 feature is available under each configuration set in **Profiles > Profile Management Settings > Advanced settings.** For more information, see Citrix Profile Management Settings.

- **Limit number of user stores synced at logoff.** When the **Replicate user stores** setting is enabled, this setting lets you speed up logoff by limiting the number of user stores to sync during user logoffs. The remaining user stores (if any) are synced after logoff is complete.

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

March 2025

UI Enhancements

The WEM UI enhancements are as follows:

- **Agent UI Update**: All UI interfaces in the **Agent** section have been updated to adopt the **Windows 11 theme style**.
- **System Tray Icon Context Menu**: The right-click menu of the Agent UI's system tray icon has been optimized with a new modern design.
- **Light and Dark Mode Support**: All Agent UI elements, including the system tray icon's context menu, now support **Light Mode** and **Dark Mode**. These modes automatically align with the **System theme** settings.
- **Agent Skin Customization**: Starting from version 2502.1.0.1, the ability to change skins through the **Console's Workspace Environment Management > Configuration sets > UI agent personalization** feature has been removed for newer agents. Agents from versions before 2502.1.0.1 continue to support skin customization. For more information, see UI Agent Personalization under the web console. Additionally, see the **UI Agent Skin** option under UI agent options.
- Minimum agent version required: 2502.1.0.1

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

Summary View for Agent Statistics

- This enhancement includes a new summary view with four charts displaying statistical results and a rearranged layout, moving the search bar and filter. For more information, see the Summary view.
- Minimum agent version required: 2502.1.0.1

Enhanced Analysis of Process Activities During User Logon

We have introduced an analysis of process activities during user logon in the **Windows Logon Analysis** to help users identify more logon performance issues. For more information, see Process activity and details.

Improved Security for Password Storage in Configurations

We have updated the internal workflow to store passwords contained in configurations, such as network drives and printers, more securely. This change is compatible with version 2005.2.0.1 and newer.

Using older versions before 2005.2.0.1 might result in the following issues:

- WEM agents older than version 2005.2.0.1 are unable to process configurations containing passwords correctly.
- When importing configuration sets exported with a console older than version 2005.2.0.1, configurations containing passwords are not imported.
- When restoring actions or settings backed up with a console older than version 2005.2.0.1, configurations containing passwords are not restored.
- When migrating from on-premises older than version 2005.2.0.1 to the cloud service, configurations containing passwords are not migrated.

New Functionalities in the Web Console

The new functionalities in the web console are as follows:

- **Save and Assign** button: A new **Save and Assign** button has been added, allowing for continuous action creation.
- **Manage Assignments** link: A new **Manage Assignments** link has been added to the toast notification.
- **Registry Operations** column: A **Registry Operations** column has been added to the data table.

For more information, see Create a GPO and Manage assignments for a GPO.

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

Enhanced Performance of Assignment Targets and Directory Objects

Previously, loading the **Directory objects** and **Assignment target** pages triggerred numerous translation requests leading to slow load times, especially with large datasets.

With this enhancement, the object names are stored in the database, translating them only when necessary, significantly improving the performance. You can manually refresh individual records to see the updated names. Additionally, **Refresh** options are added to refresh all or selected records or only usernames. For more information, see Assignment targets and the **Note** in Add a machine or machine group.

Fixes

- When the `.zip` file content of the imported GPO registry `.zip` file is not valid, an error prompt gets displayed whereas though the `.zip` file is valid, the conversion of content to the registry fails. [WEM-41987]
- When a customer configures process hierarchy control rules with a hash type, agents with versions before 2412 generate an error in the service log when retrieving the process hierarchy control rules. [WEM-41997]
- When the customer creates action groups and adds external tasks to them, the legacy console crashes while viewing the action group content under **Legacy Console** > **Actions** > **Action Groups**, or under **Legacy Console** > **Assignments** > **Action Assignment** while viewing the assignments associated with these action groups. [WEM-41903]
- When restoring a configuration site that includes action groups containing process hierarchy control rules, the process hierarchy control rules are lost in these action groups. [WEM-41589]

January 2025

Expanded Access for Non-Administrator Users

- Non-administrator users can now directly access the WEM Tool Hub with a subset of its features. This subset includes **Windows Logon Analysis** and third-party applications pinned by users. A switch to the top of the main page is recommended when a non-administrator user must use the restricted functions. This update broadens accessibility, enabling more users to utilize key functionalities efficiently, while maintaining robust security and control.

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

Process Hierarchy Control

- This release introduces the **Process hierarchy control** feature in the web console. This feature allows you to control whether specific child processes can be initiated by their parent processes. You create a rule by defining parent processes and then designating an allow list or a block list for their child processes. You then assign the rule on a per user or per user group basis. The following rule types are available:
  - **Path**. Applies the rule to an executable according to the executable file path.
  - **Publisher**. Applies the rule according to publisher information.
  - **Hash**. Applies the rule to identical executables as specified.
- For more information, see Process Hierarchy Control.
- Minimum agent version required: 2501.1.0.1

Unique Identification Support in WEM Agent

- Previously, WEM agents used the MAC address as the device identifier. In certain scenarios, the MAC address was not unique that led to the malfunctioning of some WEM features.
- With this enhancement, you can use the agent identity concept to replace the MAC address as the device identifier for WEM agents. This feature is applicable to both domain-joined and non-domain-joined agents.
- For more information, see Settings.
- Minimum agent version required: 2501.1.0.1

Enhancement to the WEM Optimizer Template

You can now use the WEM service to perform template-based system optimizations for Windows 11 2009 and Windows Server 2025 2009 machines. The WEM optimizer template is now updated to support the memory compression and cache disc mount enhancement in the Citrix optimizer.

Fixes

- During user logon, additional delays are caused by the WEM user logon service accompanied by the following Windows event log failed to retrieve user information for CVAD session launch event and AD query timed out exception. [WEM-41478, WEMHELP-356]
- Task execution result trigger does not take affect if the trigger source is a machine startup scripted task. [WEM-40747]

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

- The source profile path does not match the actual user store profile path for some profiles in Windows 10 machines. [WEM-38037]

December 2024

Accurate Search of OUs (Organizational units) with Precise Criteria

- Previously due to a large number of duplicate-named OUs in the domain controller, WEM was unable to locate the target OU accurately. This used to create significant inconvenience for the IT administrators.
- This feature now introduces a location configuration option allowing IT administrators to restrict the OU search scope to a specific location node. This helps in finding the desired target OU quickly.
- For more information, see Add an assignment target and Add machines in an OU.

Support the New Filter Design to Save Update or Delete Existing Filters

- You can now save the filters used as filter sets and directly manage these filter sets. You can conveniently switch between different filter sets when you try to query the required data. This functionality is available for use on the **Reports** page, **Agent statistics** page, and **User statistics** page.
- For more information, see Columns to display and filters.

Fixes

- The configuration set restore process may be slow if the configuration set contains a large number of security rules, such as AppLocker rules. You might encounter a timeout error when using the web console, even though the back-end restore process may succeed, despite the error. [WEM-41112]

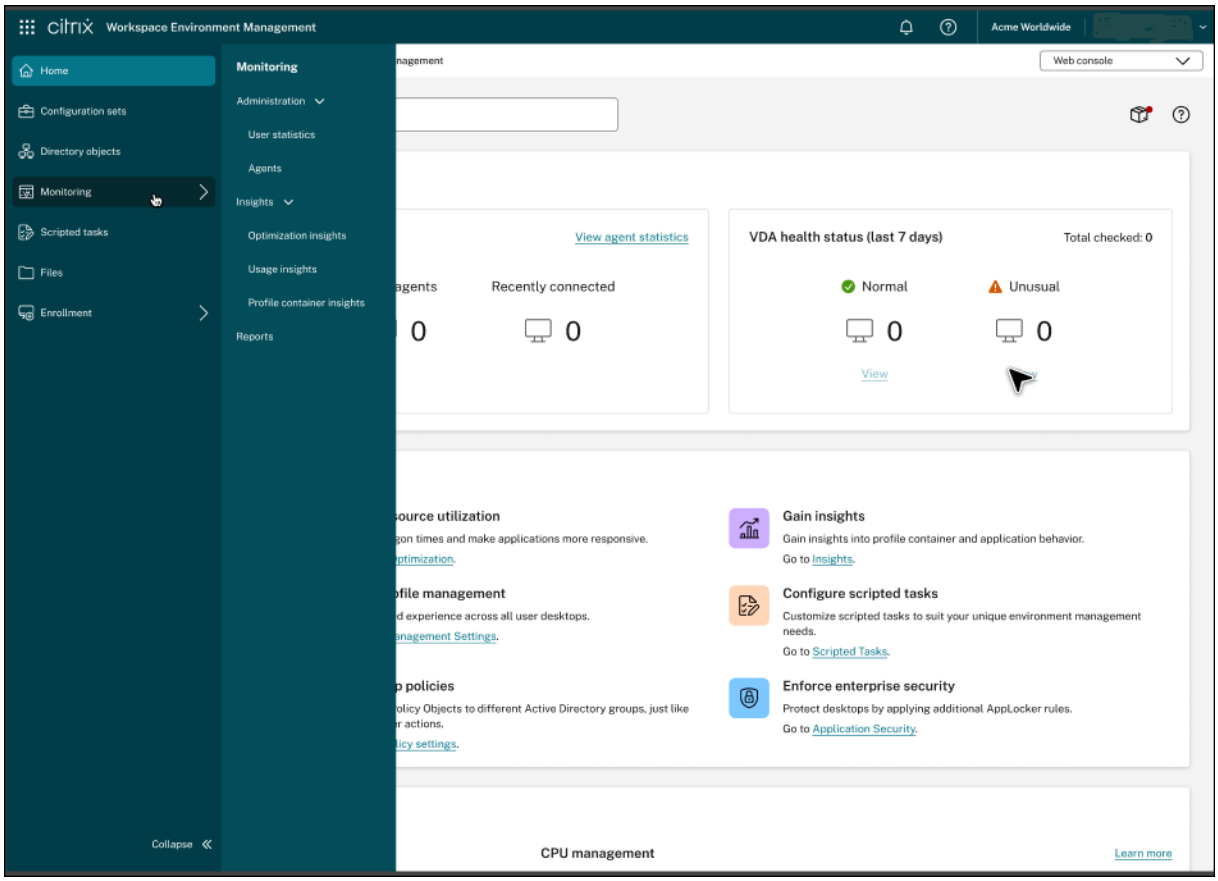
November 2024

Unified Platform Experience for Navigation

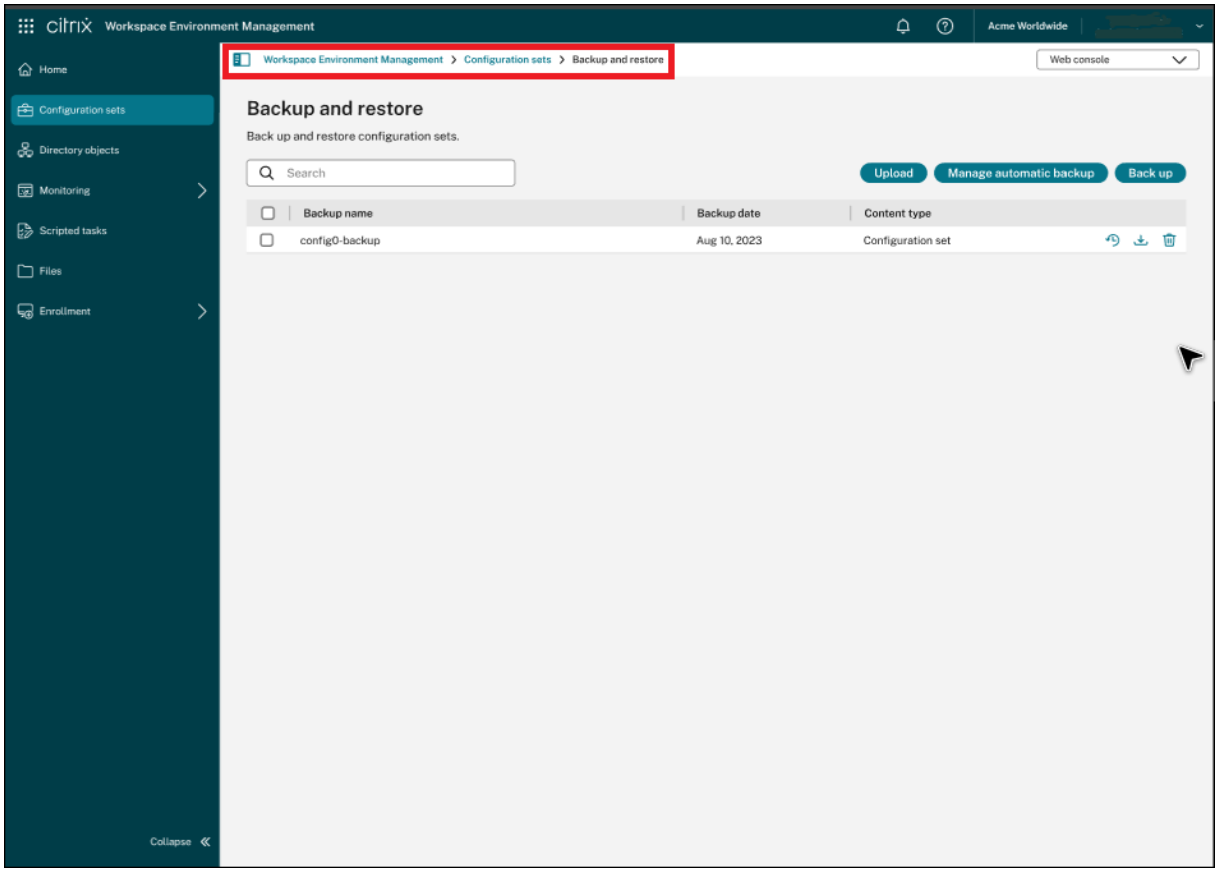
The primary navigation menu is now expanded to include a secondary navigation menu for the **Monitoring** and **Enrollment** menu items on the WEM web console. Navigation breadcrumbs are now displayed on the top of every page. To provide a unified platform experience, a drop-down menu is now

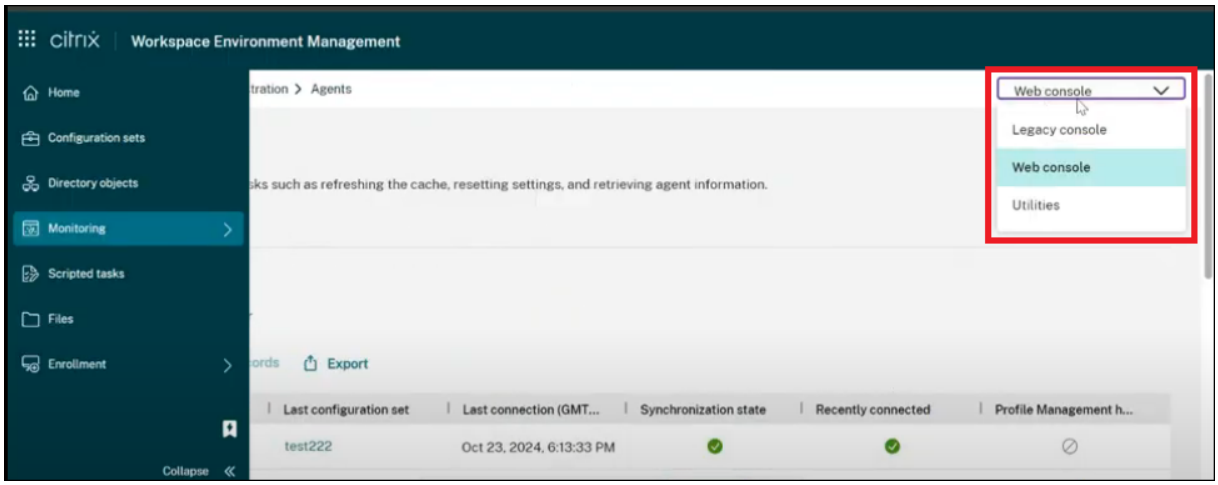
© 1997–2026 Citrix Systems, Inc. All rights reserved.

included on the top right-hand corner of the page that lets you switch to either the **Legacy console**, **Utilities**, or to the **Web console**. The screenshots depicting the changes are as follows:



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





User Statistics Quick Search and Refresh Icon

This enhancement provides the ability to search in the user statistics table using the user name and other relevant properties, such as, display name and email.

You can now use the refresh icon that appears when you hover your mouse on every record or user display name instead of the SID. For more information, see User statistics.

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

Upload Scripts for External Tasks

Previously, to use the external task feature, the path to a script (or executable) on the agent machine (or network storage) had to be specified. This required maintenance of the script files either on network storage locations or locally on a VDA running WEM causing inconvenience.

With this feature, you can now directly upload scripts when configuring external tasks. To create an external task, you now have an option to upload the script file for the task to run. After uploading, you can also view the content of the script.

For more information, see Create an external task.

Minimum agent version required: 2410.1.0.1

Rule Generator Updated with Expanded App Access Control Features

The Rule Generator for App Access Control tool now supports the expanded features of the App access control policy. With this tool, you can now create redirection rules and configure exclusions for rule assignments.

For more information, see Rule Generator for App Access Control.

Enhancements to Group Policy Migration Tool

This feature enables you to auto-configure `script path` and parameters when you migrate the Windows Logon scripts to WEM external tasks using the **Group Policy Migration** Tool.

For more information, see Group Policy Migration Tool

New details to Diagnose Logon Duration

This feature introduces new details to diagnose the logon duration. You can find more details for the sub-metrics, **FSLogix profile loading** and WEM logon services in the table that lists all the metrics, submetrics, and tips in detail.

For more information, see Windows Logon Analysis.

Profile Management

Workspace Environment Management now supports all *supported* versions of Profile Management through *2411*. The following features are now available in the web console.

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

- **Alert user when profile size exceeds quota.** This feature helps prevent data loss by notifying users when their profile size exceeds a quota. You can customize the quota limit and the notification content based on the default settings.
  The feature is available under each configuration set in **Profiles > Profile Management Settings > Advanced settings**. For more information, see Citrix Profile Management Settings.
- **Enable UWP app load acceleration.** This feature accelerates the loading of UWP apps and improves 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.
  The feature is available under each configuration set in **Profiles > Profile Management Settings > Advanced settings**. For more information, see Citrix Profile Management Settings.
- **App access control policy expanded**. With the policy, you can now implement machine-level redirections for files, folders, registry keys, and registry values. In addition, you can now exclude specific users, machines, and processes from rule enforcement for more precise control.
  The feature is available under each configuration set in **Profiles > Profile Management Settings > App access control**. For more information, see Citrix Profile Management Settings.
- **Folder redirection policy enhanced for more secure access control**. With a new option, **Grant access to specific users and groups**, you can now grant specific users or groups Read and Execute permissions on the redirection target folders. For more information, see Citrix Profile Management Settings.
- Minimum agent version required: 2411.1.0.1

Fixes

No issues have been observed in this release.

October 2024

Group Policy Migration to WEM

- You can now use the Group policy migration to migrate Group policy preferences that cause slow sign-ons into WEM actions to improve your sign-on experience. In the WEM Tool Hub, you can begin the migration workflow either within a logon duration report, while viewing GPO processing times, or from the **Group Policy Migration Tool**. This tool allows you to scan for currently applied GPOs.

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

- You can select from the listed items supported for migration. Selected items are exported as a ZIP file to the local machine, which is later imported as WEM actions. This feature is enhanced to guide you through the process of creating an assignment group with the exported settings, and also assign the group to the respective user.
- For more information, see Group Policy Migration Tool and Create an assignment group using the exported settings.

Introducing New Insights to Monitor and Diagnose Logon Duration

- This enhancement introduces profile container and GPP processing insights to monitor and diagnose logon duration. This feature enables you to identify the possible issues, which may cause slow logon and to also provide recommendations to resolve issues.
- For more information, see Windows Logon analysis and Analyze logon duration using scripted tasks.

Centralized Configuration Set Level Agent Cache Synchronization

- This feature is introduced to enhance the existing agent cache synchronization mechanism.
- Based on the new mechanism, you can avoid performance issues for large WEM deployments and the database cost on the Cloud is also reduced. For more information, see Agents and Agent cache utility options.
- Minimum agent version required: 2409.1.0.1

Fixes

- While creating Start menu shortcuts and pinning applications to the Start menu, shortcuts are generated in the root folder of the Start menu instead of being created in the path specified. This issue occurs only on Windows Server 2022/2019 but not on Windows Server 2016. [WEM-32923, CVADHELP-24045]

September 2024

Support Data Export to Splunk

Previously, you were restricted only to Grafana when exporting agent reports to third-party platforms.

With this feature, you can now effortlessly export the data to Splunk as well.

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

For more information, see Reports.

Privilege Elevation

- This enhancement enables you to configure privilege elevation rules and assign them to users using the web console.
  You can now use the existing **File Info Viewer** in WEM Tool Hub to get the file information needed for rule configuration, such as, path, publisher, and hash values.
- For more information, see Privilege elevation, Manage assignments for a target, and Create an assignment group using security rules.
- Minimum agent version required: 2408.1.0.1

WEM Agent Support for Persistent Cache on Non-Persistent Machines

- This enhancement enables the WEM agent to automatically detect non-persistent machines provisioned by MCS or PVS and use the persistent data location provided by the underlying Provisioning Service to persist agent cache and other crucial information. This improves the WEM performance and resiliency on non-persistent machines. Also, the WEM agent enrollment now supports non-persistent machines. You can now enroll the master image and the provisioned non-persistent machines are automatically enrolled.
- For more information, see Prerequisites, Determine which setup method to use, and Introduction.
- Minimum agent version required: 2408.1.0.1

Configuring Registry and GPO Settings with a New Registry Value Type

- `REG_NONE` registry value type is introduced for more customized configurations by providing a way to specify settings or parameters that do not fit into other predefined data categories, such as, strings, integers, or binary data. You can use this flexibility to handle unique or specialized configurations.
- `REG_NONE` registry value type supports the following functions:
  - In creating/updating registry entry action
  - In creating/updating registry entry-based GPO action
  - When importing a registry entry-based GPO
  - On the agent side
  - For legacy console

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

    - For backup and restore from the web console and the legacy console
- For more information, see Create a GPO and Import Group Policy settings.
- Minimum agent version required: 2408.1.0.1

Selective WEM Reset Feature

- WEM is enhanced to selectively reset WEM actions tracking cache. When you enable **Allow Users to reset Cached Actions**, the **Reset Cached Actions** is turned on. On clicking it, a new wizard gets displayed and then you can choose the cached actions that need a reset. This enhancement enables you to reset the process history for JSON files or the user group policy objects. After the reset, the actions get processed during the subsequent user logons.
- Minimum agent version required: 2408.1.0.1

Fixes

- An output is not generated when you run the scripted task with parameters. [WEM-39324]
- The scripted task service can run an unknown binary file with a special path because the service path contains space and is not enclosed within quotes. [WEM-39477]
- When you try to sign in to Workspace using **WEM Tool Hub** > **Application assistance** using your Active directory and Token, you won't see a blank workspace window. [WEM-37723]

August 2024

Enhancements to the selection of Microsoft Entra ID (Azure AD) groups or users

Policies, including actions and security rules, assigned to Microsoft Entra ID (Azure AD) groups or users now automatically take effect on the agent side without requiring manual user-device associations. To ensure the proper functioning of this feature, adhere to the following requirements:

- The agent version must be 2407.2.0.1 or higher.
- In **Citrix WEM User Logon Service Properties** dialog, set the **Startup type** as **Automatic**.
- Log out of your local machine and login again.

Add new built-in scripted tasks to reduce operation efforts

Added more valuable built-in script tasks that help admins use built-in scripted tasks directly and reduce operation efforts. This feature resolves unregistered VDA issues and sets CDF trace configurations. For more information, see Scripted Tasks.

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

VHD disk compaction report

Administrators can now view the VHD disk compaction reports in the web console by enabling VHD disk compaction report collection. For more details, see Reports and Monitoring preferences.

Profile Management

Workspace Environment Management now supports all *supported* versions of Profile Management through 2407. The following features are now available in the web console.

- **Enable in-session profile container failover among user stores** Specifies whether to enable in-session profile container failover among user stores. This feature enhances profile redundancy in the contain-based solution by expanding the container failover scope from occurring *only at user logons* to *throughout the entire session*.

  The feature is available under each configuration set in **Profiles > Profile Management Settings > Advanced settings > Replicate user stores**. For more information, see Citrix Profile Management Settings.
- **Folder redirection** enhanced with two new options:
  - **Redirect to the local user profile**, allowing you to redirect a folder to the local user profile.
  - **Move contents to new location**, allowing you to decide whether to move contents from the previous folder to the new one when setting or modifying redirection target folders.

  For more information, see Citrix Profile Management Settings.
- Minimum agent version required: 2407.1.0.1

Fixes

- In the cloud environment, if the selected WEM agent version is outdated, it should give an error prompt when editing the delivery task. [WEM-37688]
- When the WEM transformer is visible on the screen, the unlock feature through a hotkey (CTRL+ALT+U) does not work. If you change the focus to the app, the unlock hotkey works again. [WEM-37678]

June 2024

Support for testing the app access control rules

You can now validate app access control rules on the local machine before deploying in the testing or production environment. For more information, see Rule Generator for App Access Control.

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

View a GPO

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

For more information, see Group Policy settings.

Support data export to third-party platforms for flexible management

Previously, you were restricted to exporting reports solely to cloud storage or local machines, hindering your ability to effectively analyze and monitor task outcomes.

With this feature, you can now effortlessly configure and export report data to third-party platforms such as Grafana. This enhancement helps to seamlessly integrate and utilize external analytics tools for comprehensive performance monitoring and analysis, whether automatically scheduled or manually initiated.

For more information, see Reports.

Integration of the WEM Health Check tool into the WEM Tool Hub

- The WEM Health Check tool is now integrated and listed within the WEM Tool Hub Home page for ease of access and use. This tool runs checks on the WEM agent or infrastructure server and identifies potential issues with your WEM deployment. For more information, see WEM Health Check tool.
- Minimum agent version required: 2401.1.0.1

Hub agents

- This feature allows you to promote the WEM agent to a hub agent role. The hub agent can be configured to manage multiple configuration sets, assisting in the utilization of on-premises resources. Currently, the hub agent provides two key benefits:
  - Application Package Delivery: Once the hub agent is configured, it enables you to browse files from the SMB share in your on-premises environment when you add an application package.

> **Note:**
>
> The hub agent must be set to manage the site where the SMB share is located.

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

  - On-Demand Task Execution: If you initiate agent on-demand tasks from the WEM console and the cloud connector is not reachable, notifications are sent to the hub agent managing the configuration set, to which the target agent belongs. The hub agent then attempts to notify the target agents on the same subnet to execute its tasks.

- For more information, see Hub agents
- Minimum agent version required: 2406.1.0.1

Profile Migration Tool in the WEM Tool Hub

With the new Profile Migration Tool, you can now migrate different types of profiles to the Citrix container-based profile solution. This feature simplifies the profile migration process, ensuring a smooth transition and minimal disruption to user workflows. The following types of profiles are supported:

- **FSLogix profile container**
- **Citrix file-based solution**
- **Local profile**

For more information, see Profile Migration Tool.

Application security rules for WEM web console

- This feature allows you to create and configure different types of application security rules and assign them to users in the web console. This feature uses the same workflow that is used for action assignments. You can now import rules configured with AppLocker to manage them in WEM. You can also use the WEM Tool Hub to retrieve information needed for rule configuration, such as path, publisher, and hash values. For more information, see Application security, File Info Viewer, and Assignment Groups.
- Minimum agent version required: 2406.1.0.1

Fixes

- User can now access the **Reports** page from the **Task history** page with the specific type **UPM health check**. [WEM-36422]
- When you upgrade to Workspace Environment Management version 2402, the **Actions > External Tasks > Run Once** configuration doesn't work as expected in some cases. [WEM-37104]
- The WEM agent fails to enumerate all the groups to which the user belongs. Only `Everyone` and `Administrator` are listed. [WEM-37201]

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

May 2024

Windows event-based triggers for external tasks

- Windows event-based triggers for external tasks now allow you to associate external tasks (session-level tasks) with them. When the Windows events meet the defined criteria, the trigger is activated. This trigger begins to perform the associated external tasks that help in automatically managing the session-level tasks, based on Windows events. For more information, see Considerations.
- Minimum agent version required: 2404.1.0.1

WEM agent basic deployment mode

- A basic deployment mode for the WEM agent is introduced to provide basic agent functions, such as system optimization and logon duration analysis without the need to connect to the infrastructure service. WEM has powerful capabilities for user environment management that require deploying backend components such as Broker, database, and consoles for the entire deployment. Some of you might want to use only the basic features. For example, previously, if you wanted to use only the optimization functionality you had to deploy all of the backend components. This feature now provides a lightweight method to deploy WEM. You can use this deployment method for utilizing WEM basic functionalities easily. The WEM health check tool runs checks for these types of agents providing the ability to reconfigure the agent as an on-premises or service agent. You can now start the health check tool on an agent in basic deployment mode to run checks. You can also switch the agent type to on-premises or the service agent by providing necessary information about the infrastructure service or cloud connectors. For more information, see Install the agent, Manage Basic Deployment agents, and Windows Logon analysis.
- Minimum agent version required: 2404.1.0.1

Profile Management

Folder redirection settings: This feature lets you configure rule sets for redirecting 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.

To configure folder redirection for a configuration set, locate the set, go to **Profiles > Profile Management Settings > Folder redirection**, and then add rule sets. For more information, see Citrix Profile Management Settings.

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

Fixes

- During user logon, additional delays are caused by the WEM user logon service accompanied by the following Windows event log **Failed to retrieve user information for CVAD session launch event** and **AD query timed out** exception. [WEM-35792]
- Some applications only have the 32-bit version. Windows 2010 OS VDIs redirect the path `system32` to `syswow64` by default if the caller is a 32-bit application. When the elevation engine tries to access files such as `OptionalFeatures.exe`, the file is not found. Disabling the default redirect behavior elevates the application. [WEM-35650]

March 2024

Enhanced automatic backup limit for configuration sets

WEM provides automatic backup of configuration sets. The automatic backup limit is now enhanced to support storage of up to 25 backup files for each configuration set before overwriting the oldest existing file. This enhancement reduces the operation effort, especially for large and complex environments. For more information, see Manage automatic backup.

Customizing the Start menu layout for Windows 11

- To support user level assignments, you can now apply the WEM action **JSON files** for the Windows 11 Start menu configuration. Using the new tool **Start Menu Configurator for Windows 11** in the WEM Tool Hub, you can now select applications that you prefer to add to the **Pinned** section of the **Start** menu and arrange the layout as needed. After customizing the layout, copy the configuration data and paste the data in the web console, when you add a new JSON object in the **JSON Files** page. For more details, see Customize the Start menu layout for Windows 11.
- Minimum agent version required: 2403.1.0.1

User Store Creation Tool

This tool is introduced in the WEM Tool Hub to help you create user stores. The user store is the central network location for storing Citrix user profiles. This tool helps you to set up user stores by creating file shares and setting appropriate permissions to them according to your specifications. This tool simplifies the configuration process and reduces errors. You can choose to create the user store on the current machine (running the tool) or on a different machine. For more details, see User store creation tool.

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

Fixes

- Creating or duplicating Printers, Network drives, or User DSNs is very slow on the WEM web console. [WEM-32997]
- Upgrading the WEM database successively, results in the error **The given key was not present in the dictionary**. [WEM-34849]
- The Profile Management health column might show a question mark even when the **Profile Management** is configured correctly. This issue occurs when the `UpmConfigCheck.ps1` script used by the WEM agent does not work as expected. This issue affects the machines installed with the Profile Management 2203 LTSR. [WEM-34822, CVADHELP-24723]

February 2024

Assignment Groups (Preview)

This feature lets you group individual actions and manage their assignments in one place. Assignments are created per action rather than at the group level. You can now add actions to a group and select assignment targets, create, edit, and delete assignment groups. Assignment details like filters and options are maintained at the individual item level. For more details, see Assignment groups.

Health check enhancements in the web console

You can now gain a clearer and more detailed insight into the status of Profile Management through Workspace Environment Management:

- **Invalid**: Indicates that Profile Management is either not found or not enabled.
- **Error**: Indicates configuration issues in Profile Management.
- **Warning**: Identifies a suboptimal state of Profile Management.
- **Notice**: Identities an acceptable state of Profile Management.
- **Good**: Identities Profile Management is in a healthy state.

For more details, see the description for **Profile Management health** column in Statistics.

Enhanced analysis capability for Windows Logon

- This enhancement provides a more detailed data analysis for **User profile** and **Citrix Profile Management**. **Group policy objects** sub-metric is now introduced with **HDX connection** sub-metric being enabled. For more details, see Windows Logon analysis.
- Minimum agent version required: 2401.1.0.1

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

WEM health check tool

You can now open the WEM standalone tool to check the status of the WEM components and troubleshoot. This tool can run on WEM agents or the infrastructure server providing results for different selected (check) items respectively. After completing a check, a report is saved to their machine. You can turn on the debug mode and retrieve the log files to the specified location. You can also fix some configuration issues automatically. For more details, see WEM health check tool.

Fixes

- When the WEM agent runs on Windows Server 2022, the memory usage limit you apply to specific processes might not work as expected. [WEM-28773]

January 2024

User Data source name

Using the web console, you can now add user data source names (DSNs) and assign them to users. For more details, see User DSN.

Ports

Using the web console, you can now add port mappings and assign them to users. For more details, see Ports.

INI files

Using the web console, you can now add INI file operations and assign them to users. For more details, see INI files.

Agent on-demand task history

This enhancement allows you to check the progress and results of tasks initiated in the last 24 hours. You can see the task status for each of the target agents after you trigger a task. You can also view the history of recent tasks and their statuses. For tasks with reports, you can access those reports directly from the **Reports** tab. For more details, see Agents.

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

Enhanced filter condition capability for report management

This enhancement lets you filter and add multiple values by separating each value with a semicolon when you choose the **Result summary** condition, providing a flexible method for report management that enables you to monitor and optimize the system.

Profile Management

Workspace Environment Management now supports all *supported* versions of Profile Management through 2311. The following features are now available in the web console.

- **User store selection method.** Specifies the user store selection method when multiple user stores are available. Options include:

  - **Configuration order.** Lets Profile Management select the earliest configured store.
  - **Access performance.** Lets Profile Management select the store with the best access performance.

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

- **Deduplicate files this size or larger (MB).** Specifies the minimum size of files to deduplicate from profile containers. The default size is 256 MB.

  The feature is available under each configuration set in **Profiles > Profile Management Settings > File deduplication > Enable file deduplication**. For more information, see Citrix Profile Management Settings.

- **Log off users when profile container is not available during logon.** Specifies whether to force log-off users when the profile container is unavailable during user logon.

  The feature is available under each configuration set in **Profiles > Profile Management Settings > Profile container > Enable profile container**. For more information, see Citrix Profile Management Settings.

- **Set users and groups to access profile container.** Specifies which AD domain users and groups have `Read` & `Execute` permission on profile containers. By default, a profile container is accessible only to its owner.

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

- Minimum agent version required: 2311.1.0.1

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

Fixes

- Using the Agent auto upgrade feature results in the upgrade failure on the x32 platform. [WEM-32783]
- Machine-level GPOs assigned to the agent might fail when other AD objects have the same name as the agent in the domain. [WEM-32315, CVADHELP-23868]

November 2023

Automatic agent upgrade

The following enhancements are made to the automatic agent upgrade feature:

- You can select the desired agent package from the centralized SMB share package storage location, and schedule automatic upgrades for all agent machines in a configuration set.
- You can now specify the time period and schedule the day(s) of the week on which you want WEM to automatically roll out the upgrade to all agent machines in a configuration set.
- You can now specify the device name and IP of agent machines in a configuration set for which you want WEM to automatically roll out the upgrades. For more details, see App Package Delivery.
- Minimum agent version required: 2310.1.0.1

Extended limit for the Memory Usage Limit functionality

- This feature is enhanced to extend the limitation set for the maximum value of the Memory Usage Limit functionality from 4 GB to 32 GB in 64-bit OS. This enhancement provides more flexibility based on real situations in the customer system environment.
- Minimum agent version required: 2310.1.0.1

Windows Logon analysis

This tool collects the logon duration data and generates reports about the recent logon duration data. Each logon report is categorized further allowing you to identify potential issues and bottlenecks. For more details, see Windows Logon analysis.

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

Application security log reports

- Administrators can now review the Application security logs in the web console by enabling application security log collection per configuration set and get the corresponding reports. The administrator can view the logs by subtype within the details of each report. For more details, see **Application Security logs** under Reports and the description for **Security logs** in Monitoring preferences.
- Minimum agent version required: 2310.1.0.1

Fixes

No issues have been observed in this release.

October 2023

Registry Entries

Using the web console, you can now add registry entries as assignable actions, which let you create, set, or delete registry values in the user environment. The feature has been enhanced to provide a better user experience. Additionally, you are now able to add tags to registry entries and assign multiple registry entries at the same time. For more information, see Registry Entries.

Enhancements to extended data in reports

Two new export options are introduced for agent reports, **CSV (formatted)** and **JSON (formatted)**. These options enhance the readability of extended data within the reports. For more information, see Export reports.

Categorize Profile Management settings in the web console

This feature lets you reorganize your view of Profile Management settings. The three built-in tags, **File-based**, **Container-based**, and **App access control** act like filters, helping you concentrate on the settings available to the selected tag. The latest selected tags are retained as your administrator preference. For more information, see Profile Management Settings.

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

Enhancements to optimization and usage insights

This feature lets you configure the list of excluded applications by providing the application names. You can add, edit, and delete the excluded applications using the settings under **Preferences**. For more information, see Excluded applications.

Support for File Type Association (FTAs) settings on web console

This feature lets the administrators create, manage FTAs, and assign them to the users. Administrators can also use the **File Type Association Assistant** tool in the **WEM Tool Hub** to easily get the information they need for configuring FTAs in the web console. For more information, see File Type Associations.

Enhanced Agent Settings

- A new setting **Enable agent to use cached domain search results** is added to the agent settings. When enabled, the agent uses the cache for domain query results to improve performance and resiliency. You can also update WEM group policies when the agent cannot contact the domain. For more details, see Agent Settings.
- Minimum agent version required: 2309.2.0.1

Enhancements to the health check report functionality in web console

This feature improves the user experience of configuring Profile Management through WEM. When you follow the link on the Agent health check result page to **Profile Management** settings, you can see the errors/warnings in the results with its corresponding setting highlighted in the **Profile Management** configuration page on the web console. You can then modify the settings according to the results displayed in the footer. For more information, see Reports.

New version of WEM Tool Hub

A new version of WEM Tool Hub is now available: `2309.2.0.1`. This version includes performance enhancements, support for AAD/NDJ object selector support, and bug fixes. For more information, see WEM Tool Hub.

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

Fixes

- The application disappeared at times, when the customer exported the application setting to the file, saved the file to the ASCII encoding, and imported the modified file to WEM again. [WEM-31180]
- After the machine reboots, the WEM agent may lose previous SMB shares configured in **Advanced Settings** > **File Shares**. [WEM-30209]

September 2023

Support for the Windows 11 and Windows Server 2022 in Citrix Optimizer

- We added support for the Windows 11 version 21H2 (build 2009) and Windows Server 2022 21H2 (build 2009) in Citrix Optimizer. You can now use the WEM service to perform template-based system optimizations for Windows 11 2009 and Windows Server 2022 2009 machines. In addition, we have updated all existing templates to reflect changes introduced in the latest standalone Citrix optimizer.
  For information about using Citrix Optimizer, see Citrix Optimizer.
- Minimum agent version required: 2309.1.0.1

Enhancements to the manual backup limit

We have now enhanced the maximum manual export limit from 10 to 25 per account. For more information, see Back up a configuration set.

Enhancements to the optimization and usage insight application limit

We have now enhanced the optimization insight application and usage insight application limit from 10 to 20. For more information, see Insights.

Registry Entries (Preview)

Using the web console, you can now add registry entries as assignable actions, which let you create, set, or delete registry values in the user environment. The feature has been enhanced to provide a better user experience. Additionally, you are now able to add tags to registry entries and assign multiple registry entries at the same time. For more information, see Registry Entries.

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

AAD/NDJ object selector tool

- You can now assign app access rules to AAD users/groups and NDJ machines in addition to AD users/groups and domain-joined machines that are currently supported. A tool **AAD/NDJ object selector** is now available on the web console, where you can get the object data and paste them into the Rule Generator. For more information, see Assigning app access rules to AAD users/groups and NDJ machines.
- Minimum agent version required: 2309.1.0.1

File System Operations in web console

Administrators can create and manage file system operations and assign them to the users now using the web console. For more information, see File System Operations.

User-level Profile Management settings

This feature lets you configure 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. For more information, see User-level Profile Management settings.

Support reporting through agent reports

- Administrators can now review the privilege elevation logs in the web console by enabling security log collection per configuration set and get the corresponding reports. The administrator can view the logs by subtype within the details of each report. For more information, see the description for **Security logs** in Monitoring preferences.
- Minimum agent version required: 2309.1.0.1

Profile Management

- Workspace Environment Management now supports all supported versions of Profile Management through 2308. The following features are now available in the web console:
    - **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 (%)**, **Auto-expansion increment (GB)**, **Auto-expansion limit (GB)**.

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

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

- **Default capacity of VHD containers**. Specifies the default storage capacity (in GB) of each VHD container.

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

- **Enable exclusive access to profile container**. If enabled, the profile container allows only one access at a time.

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

- **Enable exclusive access to OneDrive container**. If enabled, the OneDrive container allows only one access at a time.

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

- **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 computers.

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

- Minimum agent version required: 2307.1.0.1

Configure task settings

A new option **Configure task settings** is introduced in the **Scripted Tasks** page that directs you to the specifically chosen filtered task wizard in the **Scripted Task Settings** page. For more information, see Configure task settings option.

New version of WEM Tool Hub

A new version of WEM Tool Hub is now available: `2309.1.0.1`. This version includes performance enhancements, support for AAD/NDJ object selector support, and bug fixes. For more information, see WEM Tool Hub.

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

Fixes

- The Profile Management health column might show errors even when Profile Management is configured correctly. This issue occurs because the `UpmConfigCheck.ps1` script used by the WEM agent does not work as expected. This issue affects machines with Profile Management setting, **Path to log file** enabled, with the path containing `%SystemRoot%` in it. [WEM-29519]
- The WEM agent now refreshes the SMB connection every time the policy settings get refreshed instead of waiting for the next refresh, which is every 15 minutes. [WEM-29142, CVADHELP-21957]

July 2023

User-level Profile Management settings (preview)

- This feature lets you configure 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. For more information, see User-level Profile Management settings.
- To enable this feature, go to **Home**, click the **preview features** icon in the upper-right corner, and enable **User-level Profile Management settings**. See Preview features.

Enhanced WEM agent event logging

We have made enhancements to WEM agent event logging, aiming at improving troubleshooting capabilities. The enhancements include:

- Comprehensive event logs: We have provided comprehensive event logs, giving you a complete picture of agent activities.
- Unique event IDs: Each event log now has a distinct ID, making it easier for you to filter and identify specific events.

For more information, see Agent event logs.

Microsoft Edge browser support for WEM Transformer

- The WEM Transformer now supports the latest version of the Microsoft Edge browser.
- Minimum agent version required: 2307.1.0.1

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

JSON object assignment

- You can now 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). This feature is available only in the web console. For more information, see Actions.
- Minimum agent version required: 2306.1.0.1

Add local applications for quick access

- This feature lets you add local applications to the WEM Tool Hub for quick access. The added applications are considered your personal data and are retained when you switch machines within the Profile Management environment. You can add and remove multiple applications at a time. For more information, see Add local applications for quick access.

New version of WEM Tool Hub

A new version of WEM Tool Hub is now available: `2307.1.0.1`. The version includes performance enhancements and bug fixes. For more information, see WEM Tool Hub.

Fixes

- Attempts to restore a configuration set might fail if it contains too many (for example, 10,000) template-based GPOs. [WEM-28447]

June 2023

Enhancements to CPU spike protection

- This release introduces enhancements to the CPU spike protection feature, giving you more granular control. The enhancements include the following changes:
  - We have reorganized CPU spike protection options with intuitive logic for easier configuration.
  - When customizing CPU spike protection, you can now configure the CPU usage limit using non-integer values.
  - A new option **Set limit relative to single CPU core**, is now available, letting you set a limit on CPU usage based on a single CPU core as a reference.

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

For more information, see CPU spike protection.

- Minimum agent version required: 2306.1.0.1

Environment variables

- Using the web console, you can now add environment variables as assignable actions. When assigned, those environment variables are created or set in the user environment. The feature has been enhanced to provide a better user experience. For more information, see Environment variables.
- Minimum agent version required: 2306.1.0.1

Dynamic token support for Group Policy settings

You can now use dynamic tokens in Group Policy settings. This feature allows for more adaptable policy configuration in different environments, reduces manual configuration, and simplifies policy management. For more information, see Dynamic token support for Group Policy settings.

Group Policy setting processing results

This release introduces the action processing results report feature. With this feature, you can now view the results of every action assigned to a user in a consolidated report that updates every 4 hours. The report includes information such as the name of the action, the assigned user, the filter used, and the processing result. This feature is designed for all actions but currently supports only Group Policy setting processing results. To use the feature, first enable result collection for Group Policy settings. For more information, see Reports and Monitoring preferences.

JSON object assignment (preview)

- You can now 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). This feature is available only in the web console. For more information, see Actions.
- To enable this feature, go to Home, click the preview features icon in the upper-right corner, and enable JSON object assignment. See Preview features.
- Minimum agent version required: 2306.1.0.1

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

May 2023

Profile Management backup and quick setup

- You can now back up and restore your Profile Management settings. For more information, see Back up and restore. Plus, a quick setup feature is now available, letting you quickly set up Profile Management, whether you want to start with a fresh template or restore from a backup. For more information, see Quick setup.
- Minimum agent version required: 2304.2.0.1

Network drives

- Using the web console, you can now add network drives as assignable actions. When assigned, those network drives are available for use within the user's desktop. The feature has been enhanced to provide a better user experience. For more information, see Actions.
- Minimum agent version required: 2304.2.0.1

Virtual drives

- Using the web console, you can now add virtual drives as assignable actions. When assigned, those virtual drives are available for use within the user's desktop. The feature has been enhanced to provide a better user experience. For more information, see Actions.
- Minimum agent version required: 2304.2.0.1

Improved advanced settings now available in the web console

Advanced settings have been migrated to the web console and are available in **Advanced Settings** under each configuration set. We have reorganized the settings to provide a better user experience. For more information, see Advanced Settings.

Set your start page

You can now set one of the following pages as your start page so that you land on it every time you sign in to the web console:

- Agents
- Reports
- User Statistics

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

- Usage Insights
- Optimization Insights
- Profile Container Insights

If no start page is set, you land on the Home page instead. After setting your start page, you can access it quickly by clicking the lightning icon () on the left navigation of the console.

New version of WEM Tool Hub

A new version of WEM Tool Hub is now available: 2304.2.0.1. The version includes performance enhancements and bug fixes. For more information, see WEM Tool Hub.

Fixes

- The Profile Management health column might show errors even when Profile Management is configured correctly. This issue occurs because the `UpmConfigCheck.ps1` script used by the WEM agent does not work as expected. This issue affects machines with only one system volume. [WEM-27498]

April 2023

App access control

- Using the web console, you can now add rules to control user access to items such as files, folders, and registries. A typical use case is to apply rules to control user access to apps installed on machines —whether to make apps invisible to relevant users. This feature can simplify application and image management. For example, using the feature, you can deliver identical machines to different departments while meeting their different application needs, thus reducing the number of images. For more information, see App access control.
- Minimum agent version required: 2304.1.0.1

Printers

- Using the web console, you can now add printers to assign to your users. When assigned, those printers are available for use within the user's desktop. The feature has been enhanced to provide a better user experience. For more information, see Actions.
- Minimum agent version required: 2304.1.0.1

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

WEM Tool Hub (preview)

The following two tools are now available in WEM Tool Hub:

- **Printer assistant**. Use it to get a list of printers from your print server so that you can add them as assignable actions in the management console.
- **Rule generator for app access control**. Use it to create rules to control user access to items such as files, folders, and registries. The rules are implemented through Citrix Profile Management. A typical use case is to apply rules to control user access to apps installed on machines —whether to make apps invisible to relevant users.

For more information, see WEM Tool Hub.

Profile Management

- Workspace Environment Management now supports all *supported* versions of Profile Management through 2303. The following features are now available in both the legacy console and the web console.
  - **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.
    - In the web console, the feature is available under each configuration set in **Profiles > Profile Management Settings > Basic settings**. For more information, see Citrix Profile Management Setting.
    - In the legacy console, the feature is available in **Policies and Profiles > Citrix Profile Management Settings > Main Citrix Profile Management Settings**. For more information, see Citrix Profile Management Setting.
  - **Enable app access control**. If enabled, Profile Management controls user access to items (such as files, folders, and registries) based on the rules you provide.
    - In the web console, the feature is available under each configuration set in **Profiles > Profile Management Settings > App access control**. For more information, see Citrix Profile Management Setting.
    - In the legacy console, the feature is available in **Policies and Profiles > Citrix Profile Management Settings > App Access Control**. For more information, see Citrix Profile Management Setting.
  - **Enable VHD disk compaction**. If enabled, VHD disks are automatically compacted on user logoff when certain conditions are met. This option enables you to save the storage space consumed by profile container, OneDrive container, and mirror folder container.

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

    - In the web console, the feature is available under each configuration set in **Profiles > Profile Management Settings > Profile container**. For more information, see Citrix Profile Management Setting.
    - In the legacy console, the feature is available in **Policies and Profiles > Citrix Profile Management Settings > Profile Container Settings**. For more information, see Citrix Profile Management Setting.
  - **Set free space ratio to trigger VHD disk compaction**, **Set number of logoffs to trigger VHD disk compaction**, and **Disable defragmentation for VHD disk compaction**. If **Enable VHD disk compaction** is enabled, use these three policies to adjust the default VHD compaction settings and behavior.
    - In the web console, the feature is available under each configuration set in **Profiles > Profile Management Settings > Advanced settings**. For more information, see Citrix Profile Management Setting.
    - In the legacy console, the feature is available in **Policies and Profiles > Citrix Profile Management Settings > Advanced Settings**. For more information, see Citrix Profile Management Setting.
- Minimum agent version required: 2304.1.0.1

February 2023

Applications

- Using the web console, you can now 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. The feature has been enhanced to provide a better user experience. For more information, see Actions.
- Minimum agent version required: 2302.1.0.1

WEM Tool Hub (preview)

A tool set **WEM Tool Hub**, is now available for WEM administrators. It includes a collection of tools that aims to simplify the configuration experience for administrators. To download it, go to **Citrix Cloud > WEM service > Utilities**. For more information, see WEM Tool Hub.

New settings added to external tasks

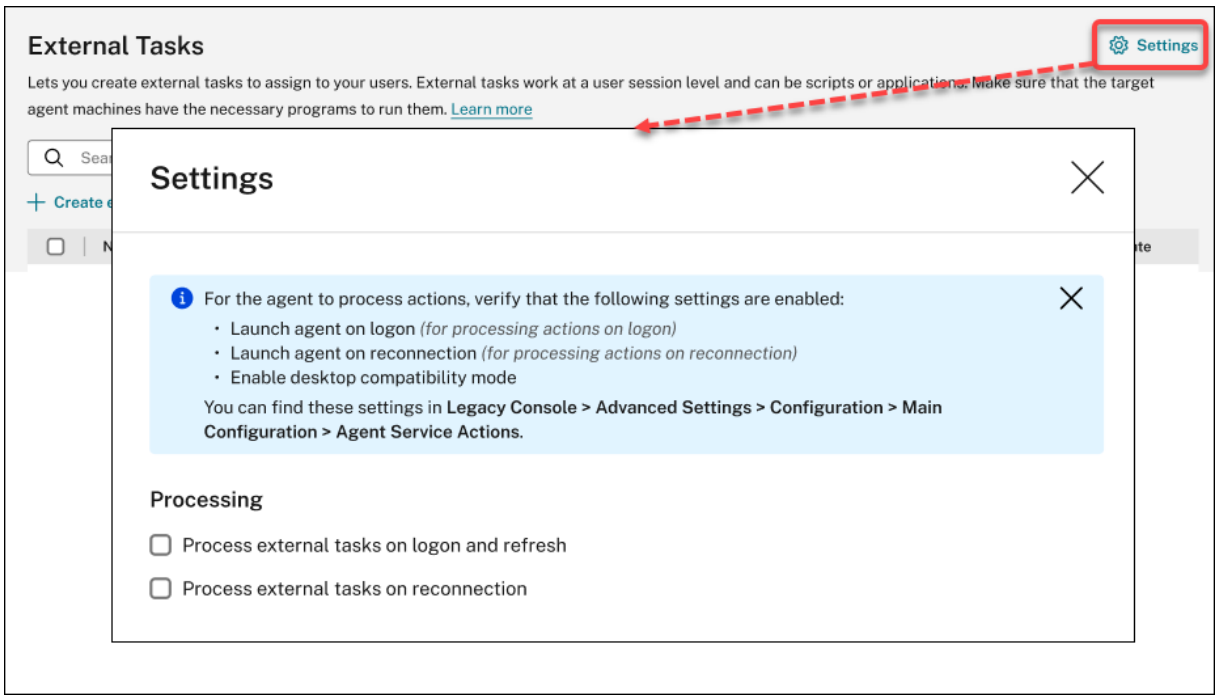
When using external tasks in the web console, you can now directly configure when the agent processes external tasks without going to **Legacy Console > Advanced Settings** for related settings.

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

The newly added settings are:

- Process external tasks on logon and refresh
- Process external tasks on reconnection

This enhancement also provides detailed information on how to ensure that the agent processes external tasks. For more information about external tasks, see Actions.



Fixes

- If you use the Studio policy, **Citrix Cloud™ Connectors**, to configure Cloud Connectors for Workspace Environment Management, the policy does not work as expected. [WEM-25697]
- In the legacy console, when you click the **State** column heading to sort, items are not sorted as expected. [WEM-25978, WEMHELP-274]
- In the legacy console, the **Backup Actions** button is not available when you use the backup wizard to back up Group Policy settings even if the configuration set does not contain any resources created using the web console. [WEM-26240]
- The privilege elevation feature might fail to work as expected. The issue occurs because the certificate used to sign the Citrix WEM software has expired. As a workaround, bypass the certificate validity check by creating a DWORD registry value under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Agent Host` and setting the value to 1. [WEM-26420, WEMHELP-284]

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

January 2023

Enhancements to automatic agent upgrade

- The automatic agent upgrade feature has been migrated to the web console and is available in **Advanced Settings > Agent Settings** under each configuration set. The feature now provides a better user experience and offers extra capabilities. In addition to scheduling automatic upgrades for the agents, you now have the flexibility to control whether to apply agent upgrades to persistent or non-persistent machines. For more information, see Advanced Settings.
- Minimum agent version required: 2301.1.0.1

Automatically bind non-domain-joined agents to desired configuration sets

- You can now set up binding rules for *unbound* non-domain-joined agents. Those rules dictate which configuration set to bind the matching agents to. This feature simplifies the process of adding non-domain-joined agents for WEM to manage. For more information, see Directory Objects.
- Minimum agent version required: 2301.1.0.1

Support for assigning GPOs to organizational units

- Using the web console, you can now assign GPOs to organizational units. This eliminates the need to change your Active Directory structure for use with WEM. For more information, see Add an assignment target.
- Minimum agent version required: 2301.1.0.1

Fixes

- When running in offline mode, the agent can't connect to the SMB shares you configured in **Advanced Settings > File Shares**. This issue does not affect the functionality of the agent. [WEM-25318]

November 2022

External task

- Using the web console, you can now create external tasks to assign to your users. External tasks can be scripts or applications. Specify when to run external tasks to manage your user environment precisely and effectively. Also, the web console provides an extra capability for external

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

tasks —letting you associate the scheduled trigger with external tasks to schedule when to run. For more information, see External tasks.

- Minimum agent version required: 2211.1.0.1

Agents to download configuration data only when needed

- Previously, WEM agents periodically connected to the WEM service to download configuration data whether or not there was a configuration change. Agents now periodically check with the service to see if any configuration changes were made:
  - If yes, agents download the configuration data.
  - If no, the configuration data is not downloaded.

  This enhancement significantly reduces bandwidth consumption, especially if you have a large deployment with many agents.
- Minimum agent version required: 2211.1.0.1

Fixes

- If you restore settings from a previous backup, you experience issues with user store-related credentials.
  - In the legacy console, you can't save changes made to the credentials.
  - In the web console, the restored credentials fail to appear in **Advanced Settings > File Shares**. [WEM-23466]
- On Mozilla Firefox browsers, the built-in scripted task Cloud Health Check fails to appear above custom scripted tasks. [WEM-24166]
- An application security rule fails to work when both of the following conditions are met:
  - It's an exception rule of the publisher type.
  - "And above"or "And below"is selected for the file version. [WEM-24327, CVADHELP-21205]
- If a registry file contains a registry key without a registry value, the scan of the file for import to Workspace Environment Management stops. Registry keys already scanned appear in the list. [WEM-24767]

Filter enhancements

- This feature lets you use the **AND** and **OR** operators to build filters. You can use the operators to combine two or more conditions into a compound condition. This feature gives you more

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

flexibility to build filters for use with assignments and scripted tasks. For more information, see Filters.

- Minimum agent version required: 2210.2.0.1

October 2022

Additional trigger types available

- The following built-in trigger types are now available when you create triggers:
  - **Machine shutdown**. Activates the trigger when machines shut down.
  - **Machine startup**. Activates the trigger when machines start up.
- You can create triggers of these types and associate tasks with them. When activated, the triggers start those tasks in the user environment. The two additional trigger types give you more flexibility to control when to run your scripted tasks. For more information, see Triggers.
- Minimum agent version required: 2210.1.0.1

Support for using task results as triggers

- The following trigger types are now available when you create triggers
  - **Cloud Health Check result**. Activates the trigger when Cloud Health Check returns specified health statuses.
  - **Profile Management health check result**. Activates the trigger when Profile Management health check returns specified health statuses.
  - **Custom scripted task result**. Activates the trigger when scripted tasks return specified results.

  You can create triggers of these types and associate tasks with them. When activated, the triggers start those tasks in the user environment. These trigger types let you automatically manage your user environments based on task execution results. For more information, see Triggers.
- Minimum agent version required: 2210.1.0.1

Profile Management

- Workspace Environment Management now supports all *supported* versions of Profile Management through 2209. The following feature is now available in both the legacy console and the web console.

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

- **File deduplication**. If enabled, Profile Management removes duplicate files from the user store and stores one copy of them in a central location. Doing so reduces the load on the user store by avoiding file duplication, thus reducing your storage cost.
  - In the web console, the feature is available under each configuration set in **Profiles > Profile Management Settings > File deduplication**. For more information, see Citrix Profile Management Setting.
  - In the legacy console, the feature is available in Policies and Profiles > Citrix Profile Management Settings > File Deduplication. For more information, see Citrix Profile Management Setting.
- **Enable multi-session write-back for profile containers**. Replaces **Enable multi-session write-back for FSLogix Profile Container** of previous releases to accommodate multi-session write-back support for Citrix Profile Management profile containers.
- **Enable Profile Streaming for Folders**. If enabled, folders are fetched only when they are being accessed.
- **Set free space ratio to trigger VHD disk compaction**, **Set number of logoffs to trigger VHD disk compaction**, and **Disable defragmentation for VHD disk compaction**. If **Enable VHD disk compaction** is enabled, use these three policies to adjust the default VHD compaction settings and behavior.
  - In the web console, the feature is available under each configuration set in **Profiles > Profile Management Settings > Advanced settings**. For more information, see Citrix Profile Management Setting.
  - In the legacy console, the feature is available in **Policies and Profiles > Citrix Profile Management Settings > Advanced Settings**. For more information, see Citrix Profile Management Setting.

- Minimum agent version required: 2210.1.0.1

View the registration status of agents

In the web console, a tab, **Registrations**, is now available in **Monitoring > Administration > Agents**. The tab lets you view the registration status of agents in your WEM deployment. With the information, you can troubleshoot agent registration issues. For more information, see Administration.

Support for cloning assignment targets

You can now clone assignment targets (users and groups) from one configuration set to another, without the need to add them from scratch. For more information, see Assignment targets.

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

Fixes

- In the web console, when you use the filter, **Last logon**, to refine results in **Monitoring > Administration > User Statistics**, the filter might not work as expected. The issue occurs when you leave the end date unspecified. As a workaround, specify an end date when using the filter. [WEM-23705]
- In **Legacy Console > Policies and Profiles > Citrix Profile Management Settings**, there is no option to add user groups for which streamed profiles and cross-platform profiles are used. [WEM-23874, CVADHELP-20951, WEMHELP-256]

September 2022

Install and upgrade: Workspace Environment Management agent

The Workspace Environment Management agent is no longer included as an additional component in the VDA installation. To install it, use the standalone WEM agent installer or the full-product installer on the Citrix Virtual Apps and Desktops product ISO.

August 2022

Use Windows events as triggers

- A new trigger type, **Windows event**, is now available when you create triggers. It lets you create a Windows event-based trigger. You can then associate tasks with it. When the Windows events meet the defined criteria, the trigger is activated and starts the associated tasks. This trigger type lets you automatically manage your user environments based on Windows events. For more information, see Triggers.
- Minimum agent version required: 2208.1.0.1

Use file shares for file downloads on the agent side

- Previously, file downloads on the agent side always occurred through Citrix Cloud. You can now let file downloads on the agent side occur through file shares. Doing so reduces network resources needed for other critical operations. This feature reduces traffic on networks and reduces the time to download files to agent machines. For more information, see File Shares.
- Minimum agent version required: 2208.1.0.1

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

Set timeouts for scripted tasks

- An option, **Set a timeout value**, is now available when you configure a scripted task. The option lets you specify the time (in minutes) after which the task is forced to end. If you do not specify a timeout, the task might keep running, thus preventing other tasks from running. For more information, see Scripted Task Settings.
- Minimum agent version required: 2207.2.0.1

Invite users to enroll agents

- A new node, **Enrollment**, is now available in the web console. The node contains two pages:
  - **Enrolled Agents**. Lists all enrolled agents. You can manage them as needed.
  - **Invitation**. Lets you send enrollment invitations to users. Each invitation includes an invitation code and the steps needed to complete the enrollment.

  For more information, see Enrollment.
- Minimum agent version required: 2207.2.0.1

Contextualize scripted tasks

- An option, **Filter**, is now available in **General** when you configure a scripted task. The option lets you use a filter to contextualize the task. As a result, the WEM agent runs the task only when all conditions in the selected filter are met. For more information, see Configure a scripted task.
- Minimum agent version required: 2207.2.0.1

Fixes

When you add a scripted task larger than 10 MB, the following error message appears even if the task is added successfully: `Failed to add the scripted task`. After you refresh the view, the task appears. [WEM-21241]

July 2022

Support for performing administrative tasks for non-domain-joined and enrolled agents

- You can now perform administrative tasks (such as refreshing the cache, resetting settings, and retrieving agent information) for *non-domain-joined* and *enrolled* agents through the administration console, just like you do for other agents. Technically, this feature is a different imple-

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

mentation. The target agents are not immediately notified of performing those tasks. The notifications are sent when the target agents or other agents on the same subnet connect to Citrix Cloud to refresh settings. So, there might be a delay until the tasks run on the agent side. The more agents you have on the same subnet, the shorter the delay.

- This feature is available in both the legacy console and the web console.
  - In the web console, go to **Monitoring > Administration > Agents**. For more information, see Administration.
  - In the legacy console, go to **Administration > Agents**. For more information, see Administration.
- Minimum agent version required: 2207.1.0.1

Configure Windows GPOs by using Group Policy Administrative Templates

- In the web console, a tab, **Template-based**, is now available in **Actions > Group Policy Settings** under each configuration set. The tab lets you configure Windows GPOs by using Group Policy Administrative Templates. You can configure GPOs at a machine and user level. After that, you deploy them by assigning them to your users, just like you do for registry-based GPOs. For more information, see Group Policy Settings.
- Minimum agent version required: 2207.1.0.1

New features available in scripted task settings

- The following new features are now available when you configure a scripted task:
  - **File path**. A parameter type that lets you pass a file path as a parameter to the `System.IO.FileInfo` class.
  - **Collect output even if runtime errors occur**. An option that controls whether to collect output file content and console output even if errors occur while running the task.

  For more information, see Scripted Task Settings.
- Minimum agent version required: 2207.1.0.1

Fixes

- If you assign application security rules (AppLocker rules) to built-in administrators, the rules might not take effect on the agent machine even if the logged-on user belongs to the administrators group. [WEM-21133, WEMHELP-229]

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

- When you view the health status of Profile Management in the management console, you might see errors even if Profile Management is configured correctly. The issue occurs when the local system account under which the agent is running does not have permission to the user store. [WEM-21247, CVADHELP-19963]
- In the web console, attempts to add or edit registry operations of the following types might fail: `REG_QWORD` and `REG_QWORD_LITTLE_ENDIAN`. The issue occurs when you type a decimal value that exceeds `9007199254740991` or a hexadecimal value that exceeds `1FFFFFFFFFFFFF`. As a workaround, use the legacy console instead.

  If you use the web console to edit registry operations of the two types whose value exceeds the limit, you see the following error message: **Invalid value or format**. You can dismiss the message. [WEM-22217]

Deploy GPOs through the web console

- In the web console, you can now manage Group Policy settings. The management takes the form of configuring Windows Group Policy Objects (GPOs). After you add or import your settings, you deploy them by assigning them to your users. For more information, see Group Policy Settings.
- Minimum agent version required: 2206.2.0.1

Profile Management

- Workspace Environment Management now supports all versions of Profile Management through 2206. The following new options are now available in both the legacy console and the web console.
  - **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.
    - In the web console, the option is available under each configuration set in **Profiles > Profile Management Settings > Streamed user profiles**. For more information, see Citrix Profile Management Setting.
    - In the legacy console, the option is available in **Policies and Profiles > Citrix Profile Management Settings > Streamed user profiles**. For more information, see Citrix Profile Management Setting.
  - **Enable concurrent session support**. Provides native Outlook search experience in concurrent sessions. If enabled, each concurrent session uses a separate Outlook OST file. You can specify the maximum number of VHDX disks for storing Outlook OST files.

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

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. This ensures that the actual processing mode is applied each time users log on.

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.

- In the web console, the three options are available under each configuration set in **Profiles > Profile Management Settings > Advanced settings**. For more information, see Citrix Profile Management Setting.
- In the legacy console, the three options are available in **Policies and Profiles > Citrix Profile Management Settings > Advanced settings**. For more information, see Citrix Profile Management Setting.

- Minimum agent version required: 2206.2.0.1

Application launcher

- An application launcher tool, **AppLauncherUtil.exe**, is now available in the agent installation folder. The tool aggregates all applications you assigned to your users through the administration console. Using the tool, users can launch all assigned applications in one place. For more information, see Application launcher.
- Minimum agent version required: 2206.2.0.1

Fixes

- When you use VUEMRSAV.exe to view results about actions applied through an action group for the current user, the **Applied Actions** tab might display the incorrect source of the actions. Example: Two action groups (`Group1` and `Group 2`) were assigned to the user and `Group1` contains `Application1`. The **Applied Actions** tab might also show that `Application1` is from `Group2` even if `Group2` does not contain `Application1`. (By default, VUEMRSAV.exe is located in the agent installation folder: %ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMRSAV.exe.) [WEM-20002]

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

May 2022

Enroll agents without configuring Citrix Cloud Connectors

- Previously, you had to configure Cloud Connectors for WEM agents to manage them. You can configure Cloud Connectors in two ways:
  - Configure Cloud Connectors while installing the agent. For more information, see Install the agent.
  - Configure the **Discover Citrix Cloud Connector from CVAD service** policy. So, the agent discovers Cloud Connector information from the relevant Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) deployment and then connects to the corresponding Cloud Connector machines. For more information, see Configure group policies (optional).

  Starting with this release, you can enroll WEM agents without configuring Citrix Cloud Connectors. The enrollment applies to both domain-joined and non-domain-joined machines. For more information, see Enroll the agent.
- Minimum agent version required: 2205.1.0.1

Scripted task updates

- The following features are now available with scripted tasks:
  - **Support for bundling multiple files into a single zip file to upload**. When adding a scripted task, you can now bundle multiple files into a single zip file to upload. This feature is useful when you want to run a scripted task that comprises multiple script files. After uploading the zip file, you specify an entry point, indicating which file to run at the beginning of the task. For more information, see Scripted Tasks.
  - **Include only regular expression matches in scripted task reports**. A new option, **Include only regular expression matches in reports**, is now available in **Output** when you configure a scripted task. The option controls whether to include the entire output content in reports or only content that matches the regular expression. Enabling the option reduces the amount of data transmitted to Citrix Cloud. For more information, see Scripted Tasks.
  - **Ability to use tags to identify scripted tasks**. You can now use tags to identify your scripted tasks. Also, the tags act as filters, letting you rearrange your view of tasks depending on criteria that are important to you. For more information, see Scripted Tasks.

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

- **More scheduling options available with scripted tasks**. You now have additional options to control when scripted tasks run. In addition to the hourly recurring pattern, you can now set daily, weekly, and monthly recurrence patterns. You can also specify the date and time at which you want scripted tasks to run, giving you more precise control. For agents earlier than 2205.1.0.1, be aware of the considerations when using the feature. For more information, see Configure a scripted task.

- Minimum agent version required: 2205.1.0.1

Enhancements to Profile Management health check

- This release includes the following enhancements to the Profile Management health check feature:

  - In the **More** menu of **Monitoring > Administration > Agents**:

    - Renamed **Refresh Profile Management configuration check** to **Run Profile Management health check** to make it easy to understand.
    - Added an option, **View Profile Management health check report**. The option provides quick access to Profile Management health reports related to the target agent machines.

    For more information, see Administration.

  - In **Advanced Settings > Monitoring Preferences** under a configuration set:

    - Added a section, **Profile Management health check**. The section lets you specify which aspects to cover in Profile Management health check reports. For more information, see Advanced Settings.

- Minimum agent version required: 2205.1.0.1

New agent version

A new version of the WEM service agent is now available: `2205.1.0.1`.

Fixes

- When you import your AppLocker rules exported from the Microsoft AppLocker console into WEM, rules of the hash type cannot be imported. [WEM-20436]

- When using **Legacy Console > Assignments > Modeling Wizard**, you might not be able to view the resultant actions for a user in a nested group. The issue occurs when the user does not

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

reside in the top group to which the actions or action groups are assigned. Example: The top group is `GroupA`, `GroupB` is its member, and `UserA` is in `GroupB`. If you assign actions or action groups to `GroupA`, you cannot view the resultant actions for `UserA` by using **Modeling Wizard**. [WEM-20842, WEMHELP-225]

Ability to import Group Policy settings from registry files

An option, **Import Group Policy settings from Registry Files**, is now available in **Legacy Console > Actions > Group Policy Settings**. With the option, 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:

- 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 deletion operations associated with registry keys and values that you define in .reg files.

For more information, see Group Policy Settings.

Filters now available in the web console

In the web console, a new page, **Filters**, is now available within **Assignments** under each configuration set. Using that page, you can add filters for controlling when to assign actions to your users. For more information, see Filters.

New agent version

A new version of the WEM service agent is now available: `2204.2.0.1`.

Fixes

- With self-elevation or privilege elevation disabled, the WEM agent might write the following error to the Windows Event Log even if users experience no issues with their environment: `System.ArgumentException: Cannot delete a subkey tree because the subkey does not exist`. [WEM-20441]

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

April 2022

Updates to the More menu in Monitoring > Administration

- This release organizes existing options in the **More** menu in **Web Console > Monitoring > Administration** into the following groups: **Agent**, **Profile**, and **Power management**. The update makes it easier for you to find what you need. The workflows for using the options remain the same.
- Other updates to the **More** menu include:
  - Renaming **Wake up agents** to **Wake** and moving it to the **Power management** group
  - Adding the following four power management options:
    - **Shut down**. Lets you shut down agents.
    - **Restart**. Lets you restart agents.
    - **Sleep**. Lets you put agents into sleep mode.
    - **Hibernate**. Lets you put agents into hibernate mode.

  For more information, see Administration.
- Minimum agent version required: 2204.1.0.1

Support for cloning scripted tasks

You can now clone an existing scripted task to use as a template for a new one, without the need to create a similar task from scratch. For more information, see Scripted Tasks.

Fixes

- Attempts to restore self-elevation rules to a different configuration set might fail. [WEM-18602]

Manage Azure Virtual Desktop using Citrix Optimization Pack

Citrix Optimization Pack for Azure Virtual Desktop is a new Citrix offering for optimizing Azure Virtual Desktop workloads. The WEM service is the primary offering included in this Citrix Optimization Pack. With the pack, you can use the WEM service to manage, optimize, and secure your native Azure Virtual Desktop environments.

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

March 2022

Profile Management now available in the web console

In the web console, you can now use Citrix Profile Management to manage user profiles across sessions and desktops. For more information, see Profile Management Settings.

Ability to pass parameters to scripted tasks

- Using the web console, you can now provide inputs as parameter variables in a scripted task at runtime. Doing that lets you control how the scripted task behaves without changing the underlying code. Also, WEM provides you with flexibility in what parameters you want to use —parameters that accept only objects of a specific type (such as, string, integer, switch) and named parameters (using the name of the parameter). For more information, see Scripted Task Settings.
- Minimum agent version required: 2203.2.0.1

Option to upgrade agents on demand

- You can now upgrade your WEM agents from the console on demand. The option is available in both the legacy console and the web console. To use the feature:
  - In the legacy console, go to **Administration > Agents**, right-click an agent, and then select **Upgrade agent to latest version**. For more information, see Administration.
  - In the web console, go to **Monitoring > Administration > Agents**, select one or more agents, click **More**, and then select **Upgrade agent to latest version**. For more information, see Administration.
- Minimum agent version required: 2203.2.0.1

Updates for the web console

This release introduces the following pages to the web console:

- **Home**. Provides an overview of your 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**. Provides an overview of your WEM deployments.
  - **Quick access**. Provides quick access to a subset of the key features that WEM offers.
  - **Highlights**. Shows the key features that WEM offers.

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

    - **Preview features**. Shows features that are currently in preview. You can enable or disable preview features yourself.

  For more information, see Home page.

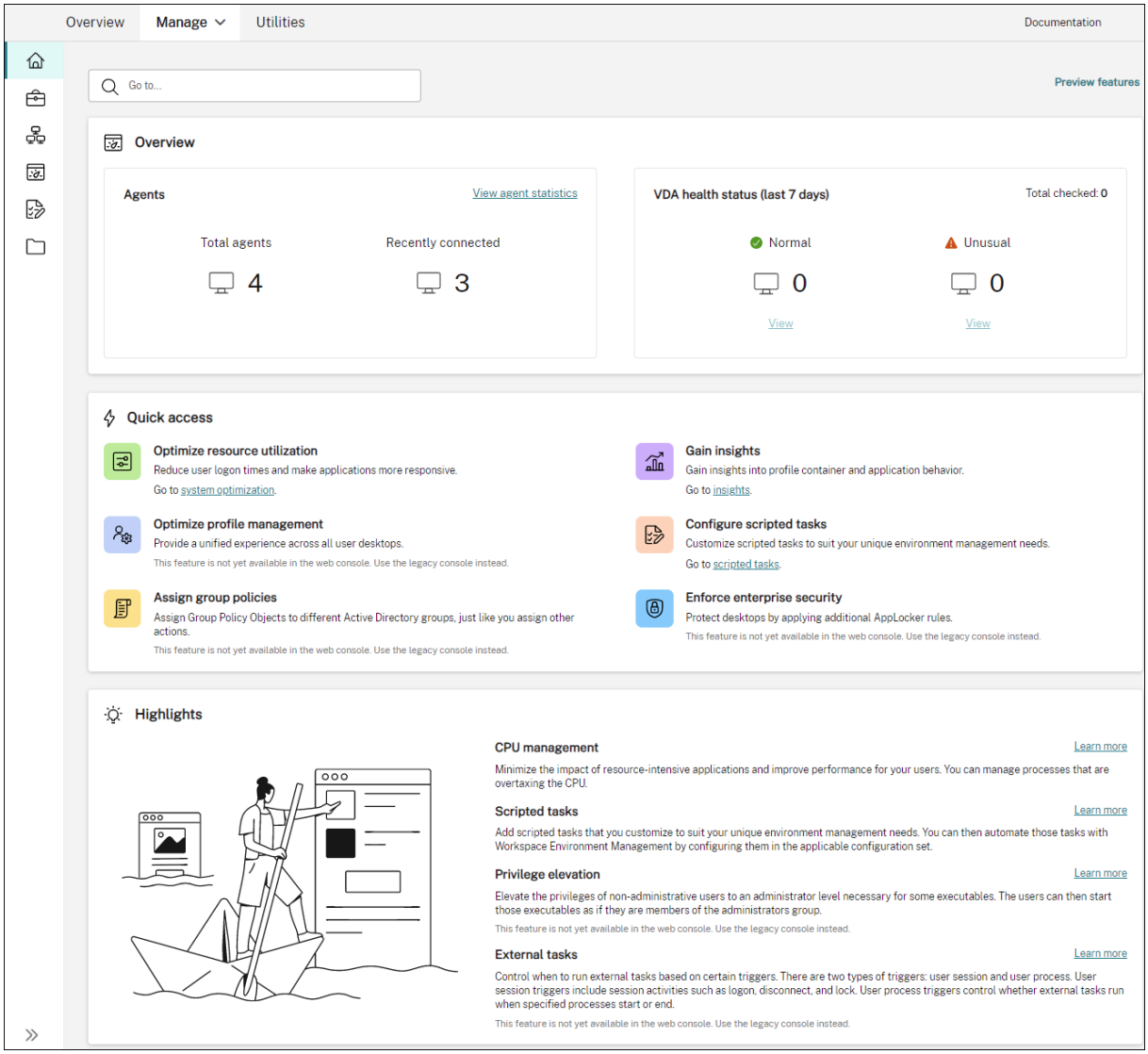
- **Directory Objects**. Lets you add machines, groups, OUs, and more, that you want WEM to manage. You can now do the following:

    - Add machines, groups, Organizational Units (OUs), and more, that you want WEM to manage.
    - Apply settings to agents that are not bound to any configuration set. So, you can control how unbound agents behave.

  For more information, see Directory Objects.

- **Assignment Target**. Lets you add users and groups (targets) so that you can assign actions and security rules to them. For more information, see Assignments.

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



Support for migrating your service instance yourself

If your WEM service instance does not reside in your current region, you can now migrate the instance to the current region yourself, without the need to contact Citrix Technical Support. Sign in to Citrix Cloud, go to **Workspace Environment Management > Utilities**, select **Start migration**. After the migration completes successfully, you receive a notification. It can take up to two days to receive the notification. We encourage you to migrate the instance to the current region for best performance.

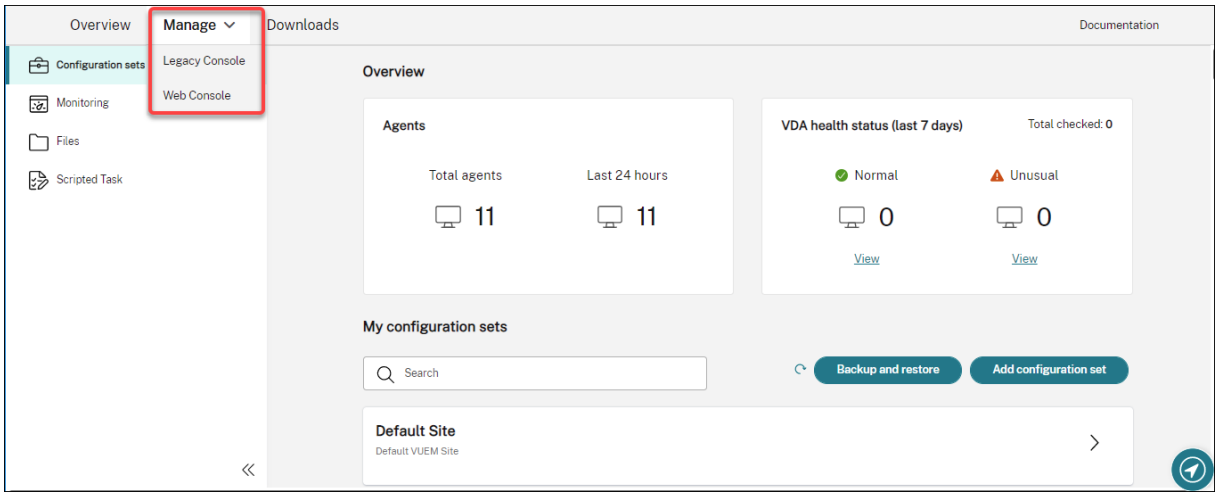
© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 2022

Web console now available as a preview

A new, web-based Workspace Environment Management (WEM) console is now available. We are in the process of migrating the full set of functionalities from the legacy console to the web console. The web console generally responds faster than the legacy console. You can easily switch between the web console and the legacy console from within the **Manage** tab to perform your configuration or deployment management tasks. Click the down arrow next to **Manage** and select an option:

- **Legacy Console**. Takes you to the legacy console.
- **Web Console**. Takes you to the new, web-based console.



The following features are available only in the web console:

- **Run scripted tasks**. You can add scripted tasks that you customize to suit your unique environment management needs. You can then automate those tasks with WEM by configuring them in the applicable configuration set. For more information, see Scripted Tasks.
- **Save a backup of a configuration set automatically**. You can manage automatic backup for your configuration sets. For more information, see Configuration Sets.
- **Scan large files in profile containers**. You can enable the WEM agent to run a scan of large files on profile containers when container usage exceeds the specified threshold value. For more information, see Advanced Settings.
- **Prevent child processes from inheriting CPU priority**. When you apply CPU spike protection, the CPU priority of a process that triggers CPU spike protection is adjusted to a lower level. That process'child process automatically inherits the lowered CPU priority. We added an option, **Prevent child processes from inheriting CPU priority**, to the **Configuration Sets > System Optimization > CPU Management > Enable CPU spike protection** tile. The option lets you

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

specify processes whose child processes you do not want to inherit the CPU priority. For more information, see System Optimization.

- **Language localization support for the web console**. The web console is adapted for use in languages other than English. The web console supports non-English characters and keyboard input even when the console itself is not localized in the preferred language of an administrator. The supported languages are as follows: French, German, Spanish, and Japanese.

Apply settings to unbound agents

- You can now apply settings to agents that are not bound to any configuration set. The feature lets you control how unbound agents behave. For more information, see Active Directory Objects.
- Minimum agent version required: 2201.2.0.1

Support for managing non-domain-joined machines in Citrix Virtual Apps and Desktops Standard for Azure deployments

- You can now use WEM service to manage non-domain-joined machines in Citrix Virtual Apps and Desktops Standard for Azure deployments. This support enables you to assign policies and settings to non-domain-joined machines as you do with domain-joined machines. For more information, see Manage non-domain-joined machines.
- Minimum agent version required: 2201.2.0.1

Support for enumerating Azure AD users and groups

WEM service now supports enumerating Azure Active Directory (AD) users and groups. After connecting your Citrix Cloud account to your Azure AD, you can add Azure AD users and groups that you want WEM to manage. For information about connecting your Citrix Cloud account to Azure AD, see Connect Azure Active Directory to Citrix Cloud.

External task

- This release includes enhancements to the external task feature. The feature now provides you with three additional options to control when to run external tasks:
  - **Disconnect**. Controls whether to run the external task when a user disconnects from a machine where the agent is running.

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

- **Lock**. Controls whether to run the external task when a user locks a machine where the agent is running.
- **Unlock**. Controls whether to run the external task when a user unlocks a machine where the agent is running.

For more information, see External Tasks.

- Minimum agent version required: 2201.1.0.1

Profile Management

- Workspace Environment Management now supports all versions of Profile Management through 2112. Also, the following new options are now available in the **Administration Console > Policies and Profiles > Citrix Profile Management Settings** interface:

  - **Enable File Exclusions for Profile Container**. Available on the **Profile Container Settings** tab, the option controls whether to exclude the listed files from the profile container.
  - **Enable File Inclusions for Profile Container**. Available on the **Profile Container Settings** tab, the option controls whether to keep the listed files in the profile container when their parent folders are excluded.
  - **Customize storage path for VHDX files**. Available on the **Advanced Settings** tab, the option controls whether to store VHDX files of different policies in different folders under the specified storage path.

  This release also adds wildcard support for Profile Management. When specifying files or folders, you can now use wildcards. For more information, see Citrix Profile Management Settings.

- Minimum agent version required: 2110.2.0.1

Administrative access to WEM service based on Azure Active Directory (AD) group membership

You can now manage administrative access to WEM service based on Azure AD group membership. Users (administrators) within the Azure AD group can directly onboard to Citrix Cloud and access WEM service –you do not need to manually add them in Citrix Cloud. A general workflow to use the feature is as follows:

1. Connect your Citrix Cloud account to your Azure AD.
2. Add the applicable group to Citrix Cloud from Azure AD.

Users can then sign in to Citrix Cloud by using their Azure AD credentials. For more information, see Connect Azure Active Directory to Citrix Cloud.

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

Fixes

- On the **Administration Console > Policies and Profiles > Microsoft USV Settings > Folder Redirection** tab, with both **Redirect AppData (Roaming)** and **Delete Local Redirected Folders** enabled, the WEM agent fails to apply the following settings:
  - **Redirect Contacts**
  - **Redirect Downloads**
  - **Redirect Links**
  - **Redirect Searches** [WEM-15016, CVADHELP-18196]
- After you upgrade to 2103 or later, the WEM agent might write errors to the Windows Event Log every five minutes even if users experience no issues with their environment. [WEM-15466, CVADHELP-18352]
- When you use VUEMRSAV.exe to view results about excluded actions or excluded action groups for the current user, the **Excluded Actions** tab fails to display Action Groups. (By default, VUEMRSAV.exe is located in the agent installation folder: %ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMRSAV.exe.) [WEM-17075]

November 2021

Message about instance migration

If you use a service in another region, a message now appears when you sign in to the administration console. The message reminds you to migrate your service instance to your current region. We encourage you to do that for optimal performance. If necessary, contact Citrix Technical Support.

An option to export statistics

We added an option, **Export statistics**, to the migration tool. Use the option to control whether to export agent and user statistics. For more information, see Migrate.

Fixes

- When you click **Apply** to save your environment settings, the administration console might exit unexpectedly. The issue occurs because the **Style** setting of **Environmental Settings > Start Menu > Set Wallpaper** is left empty. (If you previously set **Style** to **Fill** or **Fit**, the setting became empty after you upgraded the administration console to version 2109.) Workaround: Do not leave the **Style** setting empty. [WEM-16351, WEMHELP-159]

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

October 2021

Allow users to self-elevate certain applications

- This release introduces self-elevation for the privilege elevation feature. 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 reason is for auditing purposes. If the criteria are met, the elevation is applied, and the files run successfully with administrator privileges. In addition, self-elevation gives you flexibility to choose the best solution for your needs. You can create allow lists for the files you permit users to self-elevate or block lists for files you want to prevent users from self-elevating. For more information, see Self-elevation.
- Minimum agent version required: 2109.2.0.1

Bind a Citrix DaaS™ catalog to a configuration set

You can now use the Full Configuration management interface of Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) to bind a catalog to a WEM configuration set. Doing so lets you use WEM service to optimize the user experience based on your Citrix DaaS deployment. You can quickly deliver the best possible workspace experience to your users by reusing an existing catalog setup. For more information, see Create machine catalogs and Manage machine catalogs.

Workspace Environment Management now available in Citrix Cloud Japan

Workspace Environment Management service is now available in Citrix Cloud Japan, a cloud that is isolated and separate from Citrix Cloud. Japanese customers can use the service in a dedicated Citrix-managed environment. The service requires Citrix Cloud Connector version `6.29.0.58841` or later. For more information, see Citrix Cloud Japan.

Support for Windows 11

The support requires minimum agent version 2109.2.0.1.

Fixes

- The WEM agent can consume a significant amount of memory usage. Sometimes, its memory consumption can increase to 3 GB per session. [WEM-14682, WEMHELP-133]

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

September 2021

More granular control over applying privilege elevation to child processes

- Previously, when you used the **Apply to Child Processes** setting in a rule, you applied the rule to all child processes that the executable started. This release provides you with three additional options, giving you more granular control over applying privilege elevation to child processes.

  - **Apply only to executables in the same folder**
  - **Apply only to signed executables**
  - **Apply only to executables of the same publisher**

  For more information, see Privilege elevation.

- Minimum agent version required: 2109.2.0.1

Support for Windows Server 2022

The support requires minimum agent version 2109.2.0.1.

Fixes

- When you use the WEM PowerShell SDK module to export or import a WEM configuration set, certain settings, such as application security (AppLocker) rules, are not included. [WEM-12811, CVADHELP-18383]
- When you apply privilege elevation to a 32-bit executable, the privilege of the executable can be successfully elevated on machines running a 64-bit Windows operating system. However, its child processes automatically inherit the privilege whether or not the **Apply to Child Processes** setting is selected in the executable rule. [WEM-13592]
- When you use WEM to pin certain applications to the taskbar, they might not be pinned successfully. The issue occurs with Windows multi-session OS machines. [WEM-14812]
- WEM fails to deploy registry keys if their path contains a forward slash (/). The issue occurs because WEM incorrectly treats the forward slash as a separator. [WEM-15561, WEMHELP-146]

August 2021

Enablement of Asia Pacific South based instances

The WEM service is available globally. Initially, it had only US-based and EU-based instances. In addition, we now offer Asia Pacific South based instances.

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

July 2021

Notifications about new agent versions

This release updates the email notification feature available on the **Utilities** tab. Previously, you could decide whether to get notifications about upcoming upgrades to your WEM service. Starting with this release, you don't receive notifications about upgrades to your WEM service. You can decide whether to let us inform you that a new version of the Workspace Environment Management service agent is available.

Fixes

- On a non-English version of the Microsoft Windows operating system, the WEM agent during logon writes errors to the Windows Event Log even if users experience no issues with their environment. [WEM-12603, CVADHELP-17381]
- The WEM agent writes errors to the Windows Event Log each time the **Optimize Memory Usage for Idle Processes** feature comes into effect. The agent might also write errors to the Windows Event Log when the feature fails to work. [WEM-12934]
- If you use the `[ADAttribute:objectSid]` dynamic token to extract the `objectsid` attribute, the WEM agent fails to extract the attribute of the corresponding AD object. [WEM-13746]
- If you use the administration console to set desktop wallpaper, the WEM agent fails to fill, fit, or tile the wallpaper. [WEM-14408]

June 2021

Parameter matching for privilege elevation

- This release introduces parameter matching for the privilege elevation feature. Parameter matching gives you more granular control by letting you restrict privilege elevation to executables that match the specified parameter. A parameter works as a match criterion. To further expand the criterion, you can use regular expressions. For more information, see Privilege elevation.
- Minimum agent version required: 2106.2.0.1

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

Privilege elevation support for Windows installer files

- Starting with this release, you can apply privilege elevation to `.msi` and `.msp` Windows installer files. Using the feature, you elevate the privileges of non-administrative users to an administrator level necessary for some Windows installer files. As a result, those users can run those files as if they are members of the administrators group. For more information, see Privilege elevation.
- Minimum agent version required: 2105.1.0.1

Profile Management

- Workspace Environment Management now supports all versions of Profile Management through 2106. The **Administration Console > Policies and Profiles > Citrix Profile Management Settings** user interface has changed:
  - **Replicate user stores**. A new option that lets you replicate a user store to multiple paths on each logon and 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. This feature does not currently support full container solutions.
  - **Accelerate folder mirroring**. A new option that accelerates folder mirroring. Enabling the option lets Profile Management stores mirrored folders on a VHDX-based virtual disk. As a result, Profile Management attaches the virtual disk during logons and detaches it during logoffs, eliminating the need to copy the folders between the user store and local profiles.
  - **User Store Credentials**. A new tab that lets you control whether to let Profile Management impersonate the current user when accessing user stores. To allow Profile Management to impersonate the current user, disable the setting. To prevent Profile Management from impersonating the current user, enable the setting. As a result, Profile Management uses the specified user store credentials to access the user stores on behalf of the user.

  For more information, see Citrix Profile Management Settings.
- Minimum agent version required: 2106.2.0.1

Fixes

- If you assign a printer to a user based on a filter and the assignment satisfies the filter criteria, the WEM agent assigns the printer to the user. However, the agent still assigns the printer to the user the next time the user logs on even when the assignment does not satisfy the filter criteria. [WEM-11680, CVADHELP-16818]

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

- With the Windows PowerShell script execution policy set to **Allow only signed scripts** on the agent host machine, WEM fails to perform Profile Management health checks. With the policy set to **Allow local scripts and remote signed scripts** or **Allow all scripts**, WEM can perform Profile Management health checks but writes error information to the Windows Event Log. [WEM-11917]
- When you assign an action to a user or user group through an action group, the action still takes effect even if it is set to **Disabled** in the administration console. [WEM-12757, CVADHELP-17406]
- The WEM agent installs VUEMRSAV.exe (**Workspace Environment Management Resultant Actions Viewer**), a utility that lets users view the WEM configuration defined for them by administrators. However, on the **Agent Settings** tab of the utility, users cannot see the setting that is associated with the **Use Cache to Accelerate Actions Processing** option configured in the administration console. [WEM-12847]

May 2021

Configure user processes as triggers for external tasks

- This release includes enhancements to the external task feature. The feature now provides you with two additional options to control when to run external tasks:
  - **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.

  Using the two options, 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. For more information, see External Tasks.
- Minimum agent version required: 2104.1.0.1

Enhancements to process hierarchy control

- This release introduces enhancements to the process hierarchy control feature that improve overall performance and stability. The enhancements include the following changes:
  - The **AppInfoViewer** tool has been updated to include the following two options: **Enable Process Hierarchy Control** and **Disable Process Hierarchy Control**. For the process hierarchy control feature to work, you must first use the tool on each agent machine to enable

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

the feature. Every time you use the tool to enable or disable the feature, a machine restart is required.
- In certain scenarios, you must restart your agent machine after upgrading or uninstalling the agent. See Considerations for details.

- Minimum agent version required: 2105.1.0.1

Fixes

- If you assign a file system operations action and update the action later, the files or folders that were previously copied to the user environment might be deleted. The issue occurs because the WEM agent reverts the assignment made earlier after you update the action. [WEM-11924, CVADHELP-16916]
- With **Agent Type** set to **CMD** on the **Advanced Settings > Configuration > Main Configuration** tab, the **Monitoring > Daily Reports > Daily Login Report** tab might fail to display a summary of logon times across all users connected to the current configuration set. [WEM-12226]

April 2021

Process hierarchy control

- This release introduces the process hierarchy control feature. The feature lets you control whether certain child processes can be started through their parent processes. You create a rule by defining parent processes and then designating an allow list or a block list for their child processes. You then assign the rule on a per user or per user group basis. The following rule types are available:
  - **Path**. Applies the rule to an executable according to the executable file path.
  - **Publisher**. Applies the rule according to publisher information.
  - **Hash**. Applies the rule to identical executables as specified.

  For more information, see Process Hierarchy Control.
- Minimum agent version required: 2103.2.0.1

Overwrite or merge application security rules

This release adds two settings, **Overwrite** and **Merge**, to the **Administration Console > Security > Application Security** tab. The settings let you determine how the agent processes application security rules.

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

- Select **Overwrite** if you want to overwrite existing rules. When selected, the rules that are processed last overwrite rules that were processed earlier. We recommend that you apply this setting only to single-session machines.
- Select **Merge** if you want to merge rules with existing rules. When conflicts occur, the rules that are processed last overwrite rules that were processed earlier.

For more information, see Application Security.

Fixes

- The WEM agent might become unresponsive when processing applications, failing to process them successfully. [WEM-11435, CVADHELP-16706]
- You might experience performance issues such as slow logon or slow session disconnect when launching or disconnecting from published application sessions. The issue occurs with WEM agent 2005 and later. [WEM-11693]

March 2021

Discover Citrix Cloud Connectors from the CVAD service

This release introduces a policy setting titled **Discover Citrix Cloud Connector from CVAD service**. If you have not yet configured Cloud Connectors for the agent, use the setting to control whether the agent discovers Cloud Connector information from the relevant Citrix Virtual Apps and Desktops (CVAD) service deployment. The agent then connects to the corresponding Cloud Connector machines automatically. For more information, see Step 2: Configure group policies (optional).

Support for the Windows 10 2009 template

We added support for the Windows 10 2009 (also known as 20H2) template introduced in Citrix optimizer. You can now use WEM service to perform template-based system optimizations for Windows 10 2009 machines. In addition, we have updated all existing templates to reflect changes introduced in the latest standalone Citrix optimizer. For information about using Citrix optimizer, see Citrix optimizer.

Brand-new home page

This release replaces the home page of the WEM administration console with a quick-start page that provides information necessary for you to get started with the WEM service. Follow the on-screen instructions to start configuring your WEM deployment. To reopen the quick-start page, click **Quick**

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

Start (available in the ribbon) in the upper-right corner of the console. For more information, see Get started with your Workspace Environment Management service.

Profile Management

Workspace Environment Management service now supports all versions of Profile Management through 2103. Also, the following new options are now available in the **Administration Console > Policies and Profiles > Citrix Profile Management Settings** interface:

- **Enable Local Cache for Profile Container**
  - Available on the **Profile Container Settings** tab.
  - If enabled, each local profile serves as a local cache of its profile container.
- **Enable multi-session write-back for profile containers**
  - Available on the **Advanced Settings** tab.
  - Replaces **Enable multi-session write-back for FSLogix Profile Container** of previous releases to accommodate multi-session write-back support for Citrix Profile Management profile containers.
- **Enable Profile Streaming for Folders**
  - Available on the **Streamed User Profiles** tab.
  - If enabled, folders are fetched only when they are being accessed.

For more information, see Citrix Profile Management Settings.

Fixes

- For logging level changes to take effect immediately, the WEM agent might access certain registry keys very frequently, thus affecting performance. [WEM-11217]
- With an action group assigned to multiple users or user groups, if you unassign it from a user or user group, the assignment might not work as expected. For example, you assign an action group to two user groups: **Group A** and **Group B**. If you unassign the action group from **Group A**, the action group is unassigned from **Group B** rather than **Group A**. [WEM-11459, WEMHELP-75]
- When you configure an environment variable (**Actions > Environment Variables**), attempts to use the `$Split(string,[splitter],index)$` dynamic token might fail. The issue occurs because the dynamic token does not support multi-line strings. [WEM-11915]

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

January 2021

Microsoft Sync Framework 2.1 deprecation

Microsoft Sync Framework 2.1 reached End of Life on January 12, 2021. WEM has removed the legacy sync service based on that framework and instead uses a new sync framework, *Dotmim.Sync*, an open-source sync framework. How does this change impact you?

- If you use WEM agent version 1911 or later, this change does not require action on your part.
- If you use WEM agent version earlier than 1911, upgrade the agent to 1911.

WEM agent integration with the Citrix Virtual Apps and Desktops product software

The WEM agent is integrated with the Citrix Virtual Apps and Desktops product software, letting you include the WEM agent when installing a Virtual Delivery Agent (VDA). This integration is reflected in the Citrix Virtual Apps and Desktops 2012 product software and later. For more information, see Install VDAs.

Support for condition-based assignment of Group Policy settings

- Starting with this release, 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. For more information, see Contextualize Group Policy settings.
- Minimum agent version required: 2101.1.0.1

Privilege elevation

- This release introduces the privilege elevation feature. The feature lets you elevate the privileges of non-administrative users to an administrator level necessary for some executables. As a result, those users can start those executables as if they are members of the administrators group.

  The feature enables you to implement rule-based privilege elevation for specific executables. The following rule types are available:

  - **Path**. Applies the rule to an executable according to the executable file path.
  - **Publisher**. Applies the rule according to publisher information.
  - **Hash**. Applies the rule to identical executables as specified.

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

You can configure how a rule behaves according to the type of the operating system. You can also configure whether a rule takes effect at a particular time or within a particular time range. You assign a rule on a per user or per user group basis. For more information, see Privilege elevation.

- Minimum agent version required: 2010.2.0.1

Fixes

- The privilege elevation feature might fail to work properly. The issue occurs with the following versions of the WEM agent: **2010.2.0.1**, **2011.1.0.1**, and **2101.1.0.1**. The issue occurs because the certificate used to sign the Citrix WEM software has expired. To work around the issue, uninstall the relevant WEM agent, install the latest WEM agent, and then restart the agent host. [WEM-11918]
- While the WEM agent performs application processing during logon, Windows might display the **Problem with Shortcut** dialog box, prompting end users to delete a shortcut that no longer works properly. The issue occurs when the item to which the shortcut refers has been changed or moved. [WEM-10257, CVADHELP-15968]
- When using the application security feature, you see a green checkmark next to a user or user group in the **Assigned** column of the **Assignments** section in the **Edit Rule** or **Add Rule** window. The green checkmark icon does not necessarily indicate that the rule is assigned to that user or user group. Only a user or user group with a blue background is the one to which the rule is assigned. [WEM-10047]

What's new in earlier releases

For What's new in earlier releases, see What's new history.

Deprecation

September 7, 2025

This article gives you advanced notice of Workspace Environment Management™ (WEM) service features that are being phased out so that you can make timely business decisions. Citrix® monitors customer use and feedback to determine when features are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.

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

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

Deprecations and removals

The following table shows the WEM service features that are deprecated or removed.

Deprecated items are not removed immediately. Citrix continues to support them but they will be removed in a future release.

Removed items are removed, or no longer supported, in WEM service.

Item	Announced in	Removed in	Alternative
Support for the legacy agent cache sync service based on Microsoft Sync Framework 2.1.	September 2020	January 2021	If you use WEM agent version earlier than 1911, upgrade the agent to 1911 or later.

Third party notices

December 3, 2019

Workspace Environment Management might include third-party software licensed under the terms defined in the following document:

Workspace Environment Management Third Party Notices

Known issues

September 1, 2026

This release contains the following known issues:

- Importing or restoring a configuration set might fail if the backup file was created in a previous release. If you need a workaround script, contact Citrix Support. [WEM-54462]
- Restoring a backup that was exported before 2.44 (schema version 2605 or earlier) into 2.44 or later (schema version 2606 or later) fails with the message "Unable to restore. Try again later." The upload might also show "invalid content."This issue affects only older backups. Backups exported from 2.44 or later restore as expected. [WEM-54462]

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

For known issues identified in earlier versions of the WEM service, see Known issues in previous releases.

Known issues in previous releases

October 16, 2025

Workspace Environment Management service 2507.1.0.1

- Logon analysis data might not be generated for Azure AD user logons on Azure AD-joined machines. [WEM-45767]

Workspace Environment Management service 2505.1.0.1

- When updating registry entries, the operation might time out during bulk updates. As a workaround, process the updates page by page. [WEM-44587]
- When deleting expired users, the service might hang or fail if the number of expired users is too large. [WEM-42936]

Workspace Environment Management service 2504.1.0.1

- Cloud Health check fails if PowerShell execution policy is set to `RemoteSigned`. The issue is caused when the customer sets the policy to `RemoteSigned`. [WEM-42745, WEMHELP-366]
- WEM web console shows SIDs instead of user names in the **Manage assignments** window. Assignment targets only display SID in **Manage assignments** window. [WEM-42652, CVADHELP-27549]

Workspace Environment Management service 2501.1.0.1

- When the `.zip` file content of the imported GPO registry `.zip` file is not valid, an error prompt gets displayed whereas though the `.zip` file is valid, the conversion of content to the registry fails. [WEM-41987]
- When a customer configures process hierarchy control rules with a hash type, agents with versions before 2412 generate an error in the service log when retrieving the process hierarchy control rules. [WEM-41997]

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

- When the customer creates action groups and adds external tasks to them, the legacy console crashes while viewing the action group content under **Legacy Console** > **Actions** > **Action Groups**, or under **Legacy Console** > **Assignments** > **Action Assignment** while viewing the assignments associated with these action groups. [WEM-41903]
- When restoring a configuration site that includes action groups containing process hierarchy control rules, the process hierarchy control rules are lost in these action groups. [WEM-41589]

Workspace Environment Management service 2412.1.0.1

- The source profile path does not match the actual user store profile path for some profiles in Windows 10 machines. [WEM-38037]

Workspace Environment Management service 2410.1.0.1

- The source profile path does not match the actual user store profile path for some profiles in Windows 10 machines. [WEM-38037]

Workspace Environment Management service 2409.1.0.1

- The source profile path does not match the actual user store profile path for some profiles in Windows 10 machines. [WEM-38037]

Workspace Environment Management service 2408.1.0.1

- While creating **Start** menu shortcuts and pinning applications to the **Start** menu, shortcuts are generated in the root folder of the **Start** menu instead of being created in the path specified. This issue occurs only on Windows Server 2022/2019 but not on Windows Server 2016. [WEM-32923, CVADHELP-24045]

Workspace Environment Management service 2407.2.0.1

- When you create an application security rule and add publisher conditions, it is deleted when you open the legacy console. The publisher condition's file path value is null which is specified as an invalid rule by the legacy console. [WEM-39011]
- When you try to log in to the Workspace via **Citrix Environment Tool Hub > Application assistance** using your Active Directory and Token, you see a blank workspace window. [WEM-37723]

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

- While creating **Start** menu shortcuts and pinning applications to the **Start** menu, shortcuts are generated in the root folder of the **Start** menu instead of being created in the path specified. This issue occurs only on Windows Server 2022/2019 but not on Windows Server 2016. [WEM-32923, CVADHELP-24045]

Workspace Environment Management service 2403.1.0.1

- While creating **Start** menu shortcuts and pinning applications to the **Start** menu, shortcuts are generated in the root folder of the **Start** menu instead of being created in the path specified. This issue occurs only on Windows Server 2022/2019 but not on Windows Server 2016. [WEM-32923, CVADHELP-24045]

Workspace Environment Management service 2401.1.0.1

- While creating **Start** menu shortcuts and pinning applications to the **Start** menu, shortcuts are generated in the root folder of the **Start** menu instead of being created in the path specified. This issue occurs only on Windows Server 2022/2019 but not on Windows Server 2016. [WEM-32923, CVADHELP-24045]

Workspace Environment Management service 2311.1.0.1

No issues have been observed in this release.

Workspace Environment Management service 2310.1.0.1

No issues have been observed in this release.

Workspace Environment Management service 2309.2.0.1

No issues have been observed in this release.

Workspace Environment Management service 2309.1.0.1

- Certain applications of the "Citrix Workspace™ (StoreFront™) resource"type, for example, SaaS applications, might fail to start on the agent machine. [WEM-26968]
- When the WEM agent runs on Windows Server 2022, the memory usage limit you apply to specific processes might not work as expected. [WEM-28773]

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

Workspace Environment Management service 2307.1.0.1

- Certain applications of the "Citrix Workspace (StoreFront) resource"type, for example, SaaS applications, might fail to start on the agent machine. [WEM-26968]
- When the WEM agent runs on Windows Server 2022, the memory usage limit you apply to specific processes might not work as expected. [WEM-28773]
- When the WEM agent fails to retrieve the policy settings during startup, the intended SMB connections (as configured by the SMB share settings) are not immediately accessible. In this scenario, you must wait for the next connection refresh, which occurs every 15 minutes. [WEM-29142]

Workspace Environment Management service 2306.1.0.1

- Certain applications of the "Citrix Workspace (StoreFront) resource"type, for example, SaaS applications, might fail to start on the agent machine. [WEM-26968]
- You might see the following error that appears intermittently in the Windows Event Log: `HostDirectoryServicesController.IsCurrentDomainReachable(): Checking domain status timed out`. Each time WEM fails to check that the domain is reachable, the error is written in the Windows Event Log. The checks are necessary when WEM processes policies. This issue does not affect the functionality of the WEM agent. [WEM-27435, CVADHELP-22396]
- Attempts to restore a configuration set may fail if it contains too many (for example, 10,000) template-based GPOs. [WEM-28447]
- When the WEM agent runs on Windows Server 2022, the memory usage limit you apply to specific processes might not work as expected. [WEM-28773]

Workspace Environment Management service 2304.2.0.1

- Certain applications of the "Citrix Workspace (StoreFront) resource"type, for example, SaaS applications, might fail to start on the agent machine. [WEM-26968]

Workspace Environment Management service 2304.1.0.1

- Certain applications of the "Citrix Workspace (StoreFront) resource"type, for example, SaaS applications, might fail to start on the agent machine. [WEM-26968]

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

Workspace Environment Management service 2302.1.0.1

- Certain applications of the "Citrix Workspace (StoreFront) resource"type, for example, SaaS applications, might fail to start on the agent machine. [WEM-26968]

Workspace Environment Management service 2301.1.0.1

- In the legacy console, when you click the **State** column header to sort, items are not sorted as expected. [WEM-25978, WEMHELP-274]
- In the legacy console, the **Backup Actions** button is not available when you use the backup wizard to back up Group Policy settings. The issue occurs even if the configuration set does not contain any resources created using the web console. [WEM-26240]

Workspace Environment Management service 2211.1.0.1

- When running in offline mode, the agent can't connect to the SMB shares you configured in **Advanced Settings > File Shares**. This issue does not affect the functionality of the agent. [WEM-25318]

Workspace Environment Management service 2210.2.0.1

- If you restore settings from a previous backup, you experience issues with user store-related credentials.
  - In the legacy console, you can't save changes made to the credentials.
  - In the web console, the restored credentials fail to appear in **Advanced Settings > File Shares**. [WEM-23466]
- On Mozilla Firefox browsers, the built-in scripted task Cloud Health Check fails to appear above custom scripted tasks. [WEM-24166]
- An application security rule fails to work when both of the following conditions are met:
  - It's an exception rule of the publisher type.
  - "And above"or "And below"is selected for the file version. [WEM-24327, CVADHELP-21205]

Workspace Environment Management service 2210.1.0.1

- If you restore settings from a previous backup, you experience issues with user store-related credentials.

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

  - In the legacy console, you can't save changes made to the credentials.
  - In the web console, the restored credentials fail to appear in **Advanced Settings > File Shares**. [WEM-23466]

- On Mozilla Firefox browsers, the built-in scripted task Cloud Health Check fails to appear above custom scripted tasks. [WEM-24166]

Workspace Environment Management service 2208.1.0.1

- In the web console, when you use the filter, **Last logon**, to refine results in **Monitoring > Administration > User Statistics**, the filter might not work as expected. The issue occurs when you leave the end date unspecified. As a workaround, specify an end date when using the filter. [WEM-23705]

Workspace Environment Management service 2207.2.0.1

No issues have been observed in this release.

Workspace Environment Management service 2207.1.0.1

No issues have been observed in this release.

Workspace Environment Management service 2206.2.0.1

- In the web console, attempts to add or edit registry operations of the following types might fail: `REG_QWORD` and `REG_QWORD_LITTLE_ENDIAN`. The issue occurs when you type a decimal value that exceeds `9007199254740991` or a hexadecimal value that exceeds `1FFFFFFFFFFFFF`. As a workaround, use the legacy console instead.

  If you use the web console to edit registry operations of the two types whose value exceeds the limit, you see the following error message: **Invalid value or format**. You can dismiss the message. [WEM-22217]

Workspace Environment Management service 2205.1.0.1

- When you use VUEMRSAV.exe to view results about actions applied through an action group for the current user, the **Applied Actions** tab might display the incorrect source of the actions. Example: Two action groups (`Group1` and `Group 2`) were assigned to the user and `Group1` contains `Application1`. The **Applied Actions** tab might also show that `Application1` is

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

from `Group2` even if `Group2` does not contain `Application1`. (By default, VUEMRSAV.exe is located in the agent installation folder: %ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMRSAV.exe.) [WEM-20002]

Workspace Environment Management service 2204.2.0.1

- When you use VUEMRSAV.exe to view results about actions applied through an action group for the current user, the **Applied Actions** tab might display the incorrect source of the actions. Example: Two action groups (`Group1` and `Group 2`) were assigned to the user and `Group1` contains `Application1`. The **Applied Actions** tab might also show that `Application1` is from `Group2` even if `Group2` does not contain `Application1`. (By default, VUEMRSAV.exe is located in the agent installation folder: %ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMRSAV.exe.) [WEM-20002]
- When you import your AppLocker rules exported from the Microsoft AppLocker console into WEM, rules of the hash type cannot be imported. [WEM-20436]
- When using **Legacy Console > Assignments > Modeling Wizard**, you might not be able to view the resultant actions for a user in a nested group. The issue occurs when the user does not reside in the top group to which the actions or action groups are assigned. Example: The top group is `GroupA`, `GroupB` is its member, and `UserA` is in `GroupB`. If you assign actions or action groups to `GroupA`, you cannot view the resultant actions for `UserA` by using **Modeling Wizard**. [WEM-20842, WEMHELP-225]

Workspace Environment Management service 2204.1.0.1

- When you import your AppLocker rules exported from the Microsoft AppLocker console into WEM, rules of the hash type cannot be imported. [WEM-20436]
- With self-elevation or privilege elevation disabled, the WEM agent might write the following error to the Windows Event Log even if users experience no issues with their environment: `System.ArgumentException: Cannot delete a subkey tree because the subkey does not exist`. [WEM-20441]

Workspace Environment Management service 2203.2.0.1

- Attempts to restore self-elevation rules to a different configuration set might fail. [WEM-18602]

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

Workspace Environment Management service 2201.2.0.1

- On Windows 10 and Windows 11 machines, certain settings such as environment settings that you configured in the administration console might not work. [WEM-14193]
- Attempts to restore self-elevation rules to a different configuration set might fail. [WEM-18602]

Workspace Environment Management service 2201.1.0.1

- On Windows 10 and Windows 11 machines, certain settings such as environment settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2110.2.0.1

- On Windows 10 and Windows 11 machines, certain settings such as environment settings that you configured in the administration console might not work. [WEM-14193]
- On the **Administration Console > Policies and Profiles > Microsoft USV Settings > Folder Redirection** tab, with both **Redirect AppData (Roaming)** and **Delete Local Redirected Folders** enabled, the WEM agent fails to apply the following settings:
  - **Redirect Contacts**
  - **Redirect Downloads**
  - **Redirect Links**
  - **Redirect Searches** [WEM-15016, CVADHELP-18196]
- After you upgrade to 2103 or later, the WEM agent might write errors to the Windows Event Log every five minutes even if users experience no issues with their environment. [WEM-15466, CVADHELP-18352]

Workspace Environment Management service 2110.1.0.1

- On Windows 10 and Windows 11 machines, certain settings such as environment settings that you configured in the administration console might not work. [WEM-14193]
- After Windows Update installs KB5005033 on an agent host, assigned printers do not work. The issue occurs because the update prevents the automatic start of the Windows Print Spooler service. As a workaround, start the service manually. [WEM-15028]
- 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. [WEM-15353]

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

- After you upgrade to 2103 or later, the WEM agent might write errors to the Windows Event Log every five minutes even if users experience no issues with their environment. [WEM-15466, CVADHELP-18352]
- When you click **Apply** to save your environment settings, the administration console might exit unexpectedly. The issue occurs because the **Style** setting of **Environmental Settings > Start Menu > Set Wallpaper** is left empty. (If you previously set **Style** to **Fill** or **Fit**, the setting became empty after you upgraded the administration console to version 2109.) Workaround: Do not leave the **Style** setting empty. [WEM-16351, WEMHELP-159]

Workspace Environment Management service 2109.2.0.1

- On Windows 10 and Windows 11 machines, certain settings such as environment settings that you configured in the administration console might not work. [WEM-14193]
- After Windows Update installs KB5005033 on an agent host, assigned printers do not work. The issue occurs because the update prevents the automatic start of the Windows Print Spooler service. As a workaround, start the service manually. [WEM-15028]
- 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. [WEM-15353]
- When you click **Apply** to save your environment settings, the administration console might exit unexpectedly. The issue occurs because the **Style** setting of **Environmental Settings > Start Menu > Set Wallpaper** is left empty. (If you previously set **Style** to **Fill** or **Fit**, the setting became empty after you upgraded the administration console to version 2109.) Workaround: Do not leave the **Style** setting empty. [WEM-16351, WEMHELP-159]

Workspace Environment Management service 2107.2.0.1

- When you apply privilege elevation to a 32-bit executable, the privilege of the executable can be successfully elevated on machines running a 64-bit Windows operating system. However, its child processes automatically inherit the privilege whether or not the **Apply to Child Processes** setting is selected in the executable rule. [WEM-13592]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2107.1.0.1

- If you use the `[ADAttribute:objectSid]` dynamic token to extract the `objectsid` attribute, the WEM agent fails to extract the attribute of the corresponding AD object. [WEM-

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

13746]

- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2106.2.0.1

- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2105.1.0.1

- If you assign a printer to a user based on a filter and the assignment satisfies the filter criteria, the WEM agent assigns the printer to the user. However, the agent still assigns the printer to the user the next time the user logs on even when the assignment does not satisfy the filter criteria at that time. [WEM-11680, CVADHELP-16818]
- When you assign an action to a user or user group through an action group, the action still takes effect even if it is set to **Disabled** in the administration console. [WEM-12757, CVADHELP-17406]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2104.1.0.1

- If you assign a printer to a user based on a filter and the assignment satisfies the filter criteria, the WEM agent assigns the printer to the user. However, the agent still assigns the printer to the user the next time the user logs on even when the assignment does not satisfy the filter criteria at that time. [WEM-11680, CVADHELP-16818]
- If you assign a file system operations action and update the action later, the files or folders that were previously copied to the user environment might be deleted. The issue occurs because the WEM agent reverts the assignment made earlier after you update the action. [WEM-11924, CVADHELP-16916]
- With **Agent Type** set to **CMD** on the **Advanced Settings > Configuration > Main Configuration** tab, the **Monitoring > Daily Reports > Daily Login Report** tab might fail to display a summary of logon times across all users connected to the current configuration set. [WEM-12226]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

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

Workspace Environment Management service 2103.2.0.1

- You might experience performance issues such as slow logon or slow session disconnect when launching or disconnecting from published application sessions. The issue occurs with WEM agent 2005 and later. [WEM-11693]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2101.2.0.1

- For logging level changes to take effect immediately, the WEM agent might access certain registry keys frequently, thus affecting performance. [WEM-11217]
- With an action group assigned to multiple users or user groups, if you unassign it from a user or user group, the assignment might not work as expected. For example, you assign an action group to two user groups: **Group A** and **Group B**. If you unassign the action group from **Group A**, the action group is unassigned from **Group B** rather than **Group A**. [WEM-11459, WEMHELP-75]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2101.1.0.1

- When using the application security feature, you see a green checkmark next to a user or user group in the **Assigned** column of the **Assignments** section in the **Edit Rule** or **Add Rule** window. The green checkmark icon does not necessarily indicate that the rule is assigned to that user or user group. Only a user or user group with a blue background is the one to which the rule is assigned. [WEM-10047]
- The privilege elevation feature might fail to work properly. The issue occurs with the following versions of the WEM agent: **2010.2.0.1**, **2011.1.0.1**, and **2101.1.0.1**. The issue occurs because the certificate used to sign the Citrix WEM software has expired. To work around the issue, uninstall the relevant WEM agent, install the latest WEM agent, and then restart the agent host. [WEM-11918]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2011.1.0.1

- When using the application security feature, you see a green checkmark next to a user or user group in the **Assigned** column of the **Assignments** section in the **Edit Rule** or **Add Rule** window.

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

The green checkmark icon does not necessarily indicate that the rule is assigned to that user or user group. Only a user or user group that has a blue highlight in the background is the one to which the rule is assigned. [WEM-10047]

- The privilege elevation feature might fail to work properly. The issue occurs with the following versions of the WEM agent: **2010.2.0.1** and **2011.1.0.1**. The issue occurs because the certificate used to sign the Citrix WEM software has expired. To work around the issue, uninstall the relevant WEM agent, install the latest WEM agent, and then restart the agent host. [WEM-11918]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2010.2.0.1

- After you upgrade the WEM agent to version 1912, the memory consumption of **Citrix WEM Agent Host Service** might exceed 2G. If debug mode is enabled, you can see that the following messages appear many times in the **Citrix WEM Agent Host Service Debug.log** file:
  - **Adding history entry to the DB writer queue**
  - **Initializing process limitation thread for process** [WEM-9432, CVADHELP-15147]
- After you upgrade the WEM agent to version 2005, **Citrix WEM Agent Host Service** might consume between 10% and 30% of the total CPU resources, affecting the user experience. [WEM-9902, WEMHELP-47]
- When using the application security feature, you see a green checkmark next to a user or user group in the **Assigned** column of the **Assignments** section in the **Edit Rule** or **Add Rule** window. The green checkmark icon does not necessarily indicate that the rule is assigned to that user or user group. Only a user or user group that has a blue highlight in the background is the one to which the rule is assigned. [WEM-10047]
- After you select a registry file in the **Import from Registry File** window, the **Manage** tab displays a black screen if you press **ESC** to exit the window and then click **Yes**. [WEM-10103]
- The privilege elevation feature might fail to work properly. The issue occurs with the WEM agent version 2010.2.0.1. The issue occurs because the certificate used to sign the Citrix WEM software has expired. To work around the issue, uninstall the relevant WEM agent, install the latest WEM agent, and then restart the agent host. [WEM-11918]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

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

Workspace Environment Management service 2010.1.0.1

- After you upgrade the WEM agent to version 1912, the memory consumption of **Citrix WEM Agent Host Service** might exceed 2G. If debug mode is enabled, you can see that the following messages appear many times in the **Citrix WEM Agent Host Service Debug.log** file:
  - **Adding history entry to the DB writer queue**
  - **Initializing process limitation thread for process** [WEM-9432, CVADHELP-15147]
- After you upgrade the WEM agent to version 2005, **Citrix WEM Agent Host Service** might consume between 10% and 30% of the total CPU resources, affecting the user experience. [WEM-9902, WEMHELP-47]
- When using the application security feature, you see a green checkmark next to a user or user group in the **Assigned** column of the **Assignments** section in the **Edit Rule** or **Add Rule** window. The green checkmark icon does not necessarily indicate that the rule is assigned to that user or user group. Only a user or user group that has a blue highlight in the background is the one to which the rule is assigned. [WEM-10047]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2009.1.0.1

- After you upgrade the WEM agent to version 1912, the memory consumption of **Citrix WEM Agent Host Service** might exceed 2G. If debug mode is enabled, you can see that the following messages appear many times in the **Citrix WEM Agent Host Service Debug.log** file:
  - **Adding history entry to the DB writer queue**
  - **Initializing process limitation thread for process** [WEM-9432, CVADHELP-15147]
- After you upgrade the WEM agent to version 2005, **Citrix WEM Agent Host Service** might consume between 10% and 30% of the total CPU resources, affecting the user experience. [WEM-9902, WEMHELP-47]
- The WEM administration console might fail to display the changes you made to the working directory for an installed application the next time you edit the application. [WEM-10007, CVADHELP-15695]
- In non-persistent environments, changes you make through the administration console might fail to take effect on the agent hosts. The issue occurs because the agent cache file in the base image might cause cache synchronization problems. As a workaround, users must first delete the cache on their agent hosts and then refresh the cache manually to synchronize the cache with the infrastructure services.

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

The recommended best practice is to use a persistent location for the agent cache. If the agent cache resides in a non-persistent location, take these steps before sealing the base image:

1. Stop **Citrix WEM Agent Host Service**.
2. Delete these agent local database files: **LocalAgentCache.db** and **LocalAgentDatabase.db**. [WEM-10082]

- The following options are not mutually exclusive. However, the administration console does not allow you to configure them at the same time.
    - **Hide Specified Drives from Explorer** and **Restrict Specified Drives from Explorer** (on the **Policies and Profiles > Environmental Settings > Windows Explorer** tab) [WEM-10172, WEMHELP-52]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2008.1.0.1

- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2007.2.0.1

- When editing a default packaged rule, you are prompted to provide valid values on the **Publisher** tab of the **Edit Rule** window, with the **OK** button grayed out. However, the **OK** button remains grayed out even if you provide valid values on the **Publisher** tab later. [WEM-9498]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2007.1.0.1

- When you finish importing your Group Policy settings into WEM, the following message might appear even if you are the only administrator that is using the administration console:
    - Configuration Change Update: An administrator has made configuration-related changes. Click OK to reflect the changes in the current administration console. [WEM-9234]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

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

Workspace Environment Management service 2006.2.0.1

- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2006.1.0.1

- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2005.1.0.1

- In Transformer (kiosk) mode, and with **Enable Window Mode** enabled, the WEM agent might exit unexpectedly. [WEM-8119]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2004.1.0.1

- Attempts to start an application from the **My Applications** icon list in the agent UI might fail. The issue occurs with application shortcuts that are created using StoreFront URLs. [WEM-7578, CVADHELP-14171]
- Agents might fail to synchronize with the WEM service in Citrix Cloud. The issue occurs when you configure an HTTPS proxy to define how agents communicate with the service. [WEM-7579, CVADHELP-14168]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 2002.1.0.1

- On the agent host, attempts to start a published application as an application shortcut might fail. The issue occurs with application shortcuts that are created using StoreFront URLs. [WEM-7348, CVADHELP-14061]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

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

Workspace Environment Management service 2001.1.0.1

- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- Registry entries might not take effect if you assign them to a user or user group through an action group. However, they do take effect if you assign them directly. The issue occurs when you assign registry entries to be created in one of the following locations:
  - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Policies
  - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies

  [WEM-5253]
- Workspace agent refreshes might take a long time to complete. The issue occurs when the current user belongs to many user groups and there are action groups or many actions for the agent to process. [WEM-6582]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1911.1.0.1

- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- Registry entries might not take effect if you assign them to a user or user group through an action group. However, they do take effect if you assign them directly. The issue occurs when you assign registry entries to be created in one of the following locations:
  - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Policies
  - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies

  [WEM-5253]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1910.1.0.1

- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display

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

the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]

- The Restore wizard might take a long time to load the Active Directory (AD) objects after you select **Machines** as the type of AD objects you want to restore and click **Next**. The issue occurs when there are many OUs (for example, 4,000). [WEM-5169]
- Registry entries might not take effect if you assign them to a user or user group through an action group. However, they do take effect if you assign them directly. The issue occurs when you assign registry entries to be created in one of the following locations:
  - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Policies
  - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies [WEM-5253]
- The **Use Cache Even When Online** option on the **Administration Console > Advanced Settings > Configuration > Agent Options** tab might not work. [WEM-6118]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1908.2.0.1

- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary because the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]
- In Transformer (kiosk) mode, and with Log Off Screen Redirection enabled, WEM might fail to redirect the user to the logon page after logging off. [WEM-3133]
- The Restore wizard might take a long time to load the Active Directory (AD) objects after you select **Machines** as the type of AD objects you want to restore and click **Next**. The issue occurs when there are many OUs (for example, 4,000). [WEM-5169]
- Registry entries might not take effect if you assign them to a user or user group through an action group. However, they do take effect if you assign them directly. The issue occurs when you assign registry entries to be created in one of the following locations:
  - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Policies

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

    - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies [WEM-5253]

- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1908.1.0.1

- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- On the **Active Directory Objects** tab of the administration console, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management™ allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary because the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]
- In Transformer (kiosk) mode, and with Log Off Screen Redirection enabled, WEM might fail to redirect the user to the logon page after logging off. [WEM-3133]
- The Restore wizard might take a long time to load the Active Directory (AD) objects after you select **Machines** as the type of AD objects you want to restore and click **Next**. The issue occurs when there are many OUs (for example, 4,000). [WEM-5169]
- Registry entries might not take effect if you assign them to a user or user group through an action group. However, they do take effect if you assign them directly. The issue occurs when you assign registry entries to be created in one of the following locations:

    - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Policies
    - %ComputerName%\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies [WEM-5253]

- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

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

Workspace Environment Management service 1907.2.0.1

- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- On the **Active Directory Objects** tab of the administration console, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary because the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]
- In Transformer (kiosk) mode, and with Log Off Screen Redirection enabled, WEM might fail to redirect the user to the logon page after logging off. [WEM-3133]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1907.1.0.1

- Instances of Adobe Reader installed on Windows Server 2012 R2 prevent Workspace Environment Management from associating PDF files with other PDF reader applications. Users are forced to select the PDF reader application each time they open a PDF. [WEM-33]
- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- On the **Active Directory Objects** tab of the administration console, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary be-

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

cause the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]

- In Transformer (kiosk) mode, and with Log Off Screen Redirection enabled, WEM might fail to redirect the user to the logon page after logging off. [WEM-3133]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1906

- Instances of Adobe Reader installed on Windows Server 2012 R2 prevent Workspace Environment Management from associating PDF files with other PDF reader applications. Users are forced to select the PDF reader application each time they open a PDF. [WEM-33]
- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- On the **Active Directory Objects** tab of the administration console, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary because the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]
- In Transformer (kiosk) mode, and with Log Off Screen Redirection enabled, WEM might fail to redirect the user to the logon page after logging off. [WEM-3133]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1904

- Instances of Adobe Reader installed on Windows Server 2012 R2 prevent Workspace Environment Management from associating PDF files with other PDF reader applications. Users are forced to select the PDF reader application each time they open a PDF. [WEM-33]

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

- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- On the **Active Directory Objects** tab of the administration console, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary because the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]
- In Transformer (kiosk) mode, and with Log Off Screen Redirection enabled, WEM might fail to redirect the user to the logon page after logging off. [WEM-3133]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1812.1.0.1

- Instances of Adobe Reader installed on Windows Server 2012 R2 prevent Workspace Environment Management from associating PDF files with other PDF reader applications. Users are forced to select the PDF reader application each time they open a PDF. [WEM-33]
- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- On the **Active Directory Objects** tab of the administration console, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary because the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]

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

- In Transformer (kiosk) mode, and with Log Off Screen Redirection enabled, WEM might fail to redirect the user to the logon page after logging off. [WEM-3133]
- When you click Apply Filter or Refresh Report on the **Administration Console > Monitoring > User Trends > Devices Types** tab, you might not be able to view the report. Instead, you are returned to the **Administration Console > Actions > Applications > Application List** tab. [WEM-3254]
- On Windows 10 version 1809 and Windows Server 2019, Workspace Environment Management fails to pin the applications to the task bar. [WEM-3257]
- After WEM upgrades to the latest version, if you still use the earlier versions of the agent, the agent fails to work properly in offline mode. This issue occurs because of the scope changes of the agent local cache file in the latest release. As a workaround, delete the old agent local cache file, and then restart the WEM Agent Host Service (Norskale Agent Host service). [WEM-3281]
- On the Security tab of the administration console, if you create an AppLocker rule for a file with an .exe or a .dll extension using a file hash condition, the rule does not work. This issue occurs because WEM calculates the hash code of that file incorrectly. [WEM-3580]
- On the Security tab of the administration console, if you create an AppLocker rule for a file using a publisher condition, the rule does not work. This issue occurs because WEM resolves the file name incorrectly. [WEM-3582]
- If you click **Add OU** on the administration console, WEM might not display anything on the **Organizational Units** window. The issue occurs when a forest (current or trusted) contains many OUs. As a workaround, you might need to click **Cancel** and then click **Add OU** multiple times. [WEM-3818, UCOHELP-1211]
- The Application Security feature does not work on Windows servers that use non-English Windows operating systems. This issue occurs because WEM fails to start the Application Identity service in non-English language environments. [WEM-3957, LD1185]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1812.0.0.1

- Instances of Adobe Reader installed on Windows Server 2012 R2 prevent Workspace Environment Management from associating PDF files with other PDF reader applications. Users are forced to select the PDF reader application each time they open a PDF. [WEM-33]
- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]

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

- On the **Active Directory Objects** tab of the administration console, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary because the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]
- In Transformer (kiosk) mode, and with Log Off Screen Redirection enabled, WEM might fail to redirect the user to the logon page after logging off. [WEM-3133]
- When you click Apply Filter or Refresh Report on the **Administration Console > Monitoring > User Trends > Devices Types** tab, you might not be able to view the report. Instead, you are returned to the **Administration Console > Actions > Applications > Application List** tab. [WEM-3254]
- On Windows 10 version 1809 and Windows Server 2019, Workspace Environment Management fails to pin the applications to the task bar. [WEM-3257]
- After WEM upgrades to the latest version, if you still use the earlier versions of the agent, the agent fails to work properly in offline mode. This issue occurs because of the scope changes of the agent local cache file in the latest release. As a workaround, delete the old agent local cache file, and then restart the WEM Agent Host Service (Norskale Agent Host service). [WEM-3281]
- On the Security tab of the administration console, if you create an AppLocker rule for a file with an .exe or a .dll extension using a file hash condition, the rule does not work. This issue occurs because WEM calculates the hash code of that file incorrectly. [WEM-3580]
- On the Security tab of the administration console, if you create an AppLocker rule for a file using a publisher condition, the rule does not work. This issue occurs because WEM resolves the file name incorrectly. [WEM-3582]
- Attempts to map a network drive to users fail if you select the character # as the drive letter for that network drive in the **Assign Filter & Drive Letter** window. This issue occurs because WEM currently does not support assigning a random letter to a network drive by using "#."[WEM-3752, LD1014]
- Attempts to migrate your WEM database into the WEM service can fail. The issue occurs when the entries in the VUEMTasksHistory table of your on-premises WEM database contain special characters. As a workaround, delete those entries from your on-premises WEM database, and then restart the migration process. [WEM-3817, UCOHELP-1567]
- If you click **Add OU** on the administration console, WEM might not display anything on the **Or-**

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

ganizational Units window. The issue occurs when a forest (current or trusted) contains many OUs. As a workaround, you might need to click **Cancel** and then click **Add OU** multiple times. [WEM-3818, UCOHELP-1211]

- The Application Security feature does not work on Windows servers that use non-English Windows operating systems. This issue occurs because WEM fails to start the Application Identity service in non-English language environments. [WEM-3957, LD1185]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1811

Workspace Environment Management service contains the following issues:

- Instances of Adobe Reader installed on Windows Server 2012 R2 prevent Workspace Environment Management from associating PDF files with other PDF reader applications. Users are forced to select the PDF reader application each time they open a PDF. [WEM-33]
- If you open the Workspace Environment Management service administration console using Internet Explorer 11 (IE11) or Microsoft Edge, and open the Developer Tools pane (F12), when you close the Developer Tools pane again the administration console does not redraw to full size. If this happens, refresh the browser window to redraw the administration console correctly. [WEM-1377]
- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- On the **Active Directory Objects** tab of the administration console, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- After you migrate your on-premises WEM database to the WEM service, you must reinstall the WEM service agent even if the latest version is installed on your machine. This is necessary because the agent cache cannot synchronize with the WEM service database unless you reinstall the WEM service agent. [WEM-2396]
- Attempts to access the administration console from the Workspace Environment Management service **Manage** tab fail. As a workaround, refresh your browser window and try again. [WEM-2401]

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

- Attempts to run the UpmConfigCheck script on Windows 7 Service Pack 1, Windows 2008 R2 Service Pack 1, or Windows Server 2008 Service Pack 2 fail. To run the script on those operating systems, you must manually install Windows Management Framework 3.0. If the UpmConfigCheck still does not work after you install Windows Management Framework 3.0, restart your WEM agent host service (Norskale Agent Host Service). [WEM-2717]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

Workspace Environment Management service 1807

Workspace Environment Management service contains the following issues:

- On Windows Server 2012 R2, if Adobe Acrobat Reader is installed, it prevents Workspace Environment Management from associating PDF files with other PDF reader applications. Users are forced to select the PDF reader application each time they open a PDF. [WEM-33]
- On the Security tab, when you clear the option **Process DLL Rules**, the rule count reported next to the "DLL Rules"collection is set to zero, regardless of the actual number in the WEM database. [WEM-425]
- If multiple session support is enabled on a Windows server OS machine, application security rules of previously logged on users are replaced by rules of more recently logged on users. For example, if a rule is assigned to user1 but not to user2, when user2 logs on, the rule is deleted from local AppLocker rules. Thus the rule cannot be enforced for user1 as well. [WEM-1070]
- If you open the Workspace Environment Management service administration console using Internet Explorer 11 (IE11) or Microsoft Edge, and open the Developer Tools pane (F12), when you close the Developer Tools pane again the administration console does not redraw to full size. If this happens, refresh the browser window to redraw the administration console correctly. [WEM-1377]
- Agent host machine names listed on the **Active Directory Objects** tab of the WEM service administration console do not update automatically to reflect changes to machine names. To display the new name of a machine in the Machines list, you must manually delete the machine from the Machines list, and then add the machine again. [WEM-1549]
- The on-premises version of Workspace Environment Management (WEM) allows you to use Active Directory security groups as containers for WEM agents. However, the WEM service does not support using Active Directory security groups as agent containers. The on-premises infrastructure service also supports using direct and indirect OUs as agent containers. However, the WEM service does not support indirect OUs. For example, suppose WEM agent AGENT1 belongs to OU2, and OU2 belongs to OU1 (OU1>OU2>AGENT1). The on-premises infrastructure service

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

recognizes AGENT1 as a member of both OU1 and OU2, but the WEM service only recognizes AGENT1 as a member of OU2. [WEM-1619]

- In the administration console Active Directory Objects tab, using **Add Object** and **Check Name** to search and add objects allows only one object to be added at a time. You must close and then reopen the Select Computers or Groups dialog to add another object. (The on-premises version of Workspace Environment Management allows multiple objects to be identified and added without closing the dialog each time.) [WEM-1620]
- On Windows 10 machines, environment and certain other settings that you configured in the administration console might not work. [WEM-14193]

System requirements

September 29, 2025

Software prerequisites

Citrix Cloud Connector. This component must be installed on at least one machine in every resource location you are using before you install the Workspace Environment Management service agent. See Cloud Connector Installation.

.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™ service 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.
> - Starting with Version 2203, the Microsoft Edge WebView2 Runtime installer is packaged with the agent installer.

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

> - To download and install Microsoft Edge WebView2 Runtime, you must have internet access.

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

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) or Citrix Virtual Apps and Desktops. Any supported version of Citrix Virtual Apps or desktops is required.

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

- 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.

Operating system prerequisites

> **Note:**
>
> The Workspace Environment Management agents are supported only on operating system versions that are supported by their manufacturer. You might need to purchase extended support from your operating system manufacturer.

Agent. The Workspace Environment Management agent is supported on the following 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*
- Windows Server 2016 Standard and Datacenter Editions*

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

> **Note:**
>
> Workspace Environment Management service agents running on multi-session operating sys-

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

> tems cannot operate correctly when Microsoft's Dynamic Fair Share Scheduling (DFSS) is enabled. For information about how to disable DFSS, see CTX127135.

Hardware prerequisites

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).

Connectivity prerequisites

For the WEM service agent to operate, you must configure your firewall and proxy server to allow outbound connections. For more information, see Internet connectivity requirements.

In enterprise networks, the WEM service also requires the Cloud Connector to communicate with the WEM service agent. Therefore, check your firewall settings to ensure that the WEM service agent port is configured correctly. For more information, see Port information.

Service dependencies

Netlogon. The agent service ("Citrix WEM 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

The Workspace Environment Management service agent is installed in the following default folder:

- 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)

On-access scanning must be disabled for the entire "Citrix"installation folder for the Workspace Environment Management agent. When this is not possible, the following processes must be excluded from on-access scanning:

- AgentCacheUtility.exe
- AgentGroupPolicyUtility.exe
- AppInfoViewer.exe
- Agent Log Parser.exe
- AppsMgmtUtil.exe
- Citrix.Wem.Agent.EnrollmentUtility.exe
- Citrix.Wem.Agent.Service.exe

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

- Citrix.Wem.Agent.LogonService.exe
- Citrix.wem.dbsync.client.agent.exe
- PrnsMgmtUtil.exe
- VUEMAppCmd.exe
- VUEMAppCmdDbg.exe
- VUEMAppHide.exe
- VUEMCmdAgent.exe
- VUEMMaintMsg.exe
- VUEMRSAV.exe
- VUEMUIAgent.exe

Limits

September 7, 2025

Workspace Environment Management™ (WEM) service is designed for large-scale enterprise deployments. On the server side, WEM service monitors the communication flow between front-end and back-end components, and scales up or down dynamically based on data in transit.

When evaluating WEM service for sizing and scalability, consider the following limits. The values in this article indicate the limits of a single WEM service instance.

Usage limits

The following table lists the usage limits.

Resource	Limit
Concurrent full administration connections	5
End-user connections for every Citrix Cloud Connector™	10,000 end users (machine specification: 4 vCPUs, 8 GB RAM, and 80 GB of available disk space)
WEM agent connections	100,000

> **Important:**
>
> To ensure high availability, we recommend at least two Cloud Connectors in each resource location. The WEM agent balances the load among Cloud Connectors automatically. If the Citrix

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

> Cloud Connectors in place are not for WEM service only, consider deploying additional Cloud Connectors. For information about Cloud Connectors, see Citrix Cloud Connector.

Get started: Plan and build a deployment

September 7, 2025

If you are not familiar with the components used in a Workspace Environment Management (WEM) service deployment, see Workspace Environment Management service.

If you are migrating from an on-premises WEM deployment, see Migrate to cloud.

How to use this article

To set up your WEM deployment, complete the tasks summarized below. Links are provided to each task's details.

Review the entire process before starting the deployment, so you know what to expect. This article also links to other helpful information sources.

Plan and prepare

See the Citrix Tech Zone documentation articles to help establish goals and define use cases and business objectives, and to get to know configuration considerations.

- To learn how WEM improves the overall experience and enhances the security of the deployment, see Tech Brief: Workspace Environment Management.
- To learn the architecture and deployment considerations for this cloud-based service, see Reference Architecture: Workspace Environment Management.
- To learn how WEM optimizes resource utilization, logon times, and RAM usage, see Tech Insight: Workspace Environment Management. Watch the videos there.

Sign up

Sign up for a Citrix account and request a WEM service trial. The onboarding steps are:

1. Sign up for a Citrix account and request a WEM service trial.
2. Discuss integration requirements with Citrix.
3. Complete settings in the Citrix Cloud™ portal.

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

To sign up for a Citrix account and request a trial, contact your Citrix Sales Representative. When you are ready to proceed, go to https://onboarding.cloud.com.

After you log on, in the WEM service tile, click **Request Trial**. The text changes to **Trial Requested**. You will receive an email when your trial is available.

> **Note:**
>
> While waiting for the trial, you can review the information referenced in *Where to go next*. Although Citrix hosts and delivers your WEM service solution, you manage the machines that deliver applications and desktops, plus the applications and users. You can spend this time setting up the infrastructure to your corporate services, such as Active Directory.

Determine which setup method to use

Each machine that WEM manages must have a WEM agent installed on it. WEM agents connect to the WEM service and enforce settings you configure in the administration console. Before you install the agent, determine a setup method that suits your deployment needs.

There are three setup methods to connect the agent to the WEM service:

- **Cloud Connector**. Use this method if your machines are domain-joined. This method requires that you set up resource locations and install at least one Citrix Cloud Connector™ in each.
  - For high availability, we recommend that you install two Cloud Connectors in each resource location.
  - Resource locations contain infrastructure services (such as Active Directory and Cloud Connectors) and the machines that deliver apps and desktops to users.

  See Resource locations and Cloud Connector installation.

  Video about installing Cloud Connectors:

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



- **Non-domain-joined**. Use this method if you want to manage non-domain-joined machines in Citrix DaaS deployments. This method requires that you select **Skip Configuration** when installing the agent.
- **Enrollment**. Use this method to enroll WEM agents without configuring Cloud Connectors. This method requires that you select **Skip Configuration** when installing the agent.

The following provides general guidance to help you decide which method to use.

- **For machines managed by Citrix DaaS™**. Use the same method to connect the agent to Citrix Cloud as you do for the Virtual Delivery Agent (VDA) —through the Cloud Connector or the non-domain-joined method.
- **For machines not managed by Citrix DaaS**. Use the Cloud Connector or the enrollment method.

Install the agent

Each machine that WEM manages must have a WEM agent installed on it. See Install the agent.

Manage your deployment

After you complete the tasks above that set up your WEM deployment, start the WEM administration console. There are two consoles available:

- Legacy console

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

- Web console

We are in the process of migrating features from the legacy console to the web console. The web console responds faster than the legacy console and provides more functionalities. To see the features available only in the web console, see What's new.

More information

- Limits of a single WEM service instance
- REST APIs

Install agents

October 23, 2025

This article begins with a description of Workspace Environment Management™ (WEM) agents. The remainder of the article describes the steps in the agent installation wizard. Additional information related to agents is provided.

Introduction

Each machine that WEM manages must have a WEM agent installed on it. WEM agents connect to the WEM service and enforce settings you configure in the administration console. All communications are over HTTPS using the Citrix Cloud™ Messaging Service. All agents use local caching, ensuring that they can continue using existing settings if the network connection is interrupted.

WEM supports managing both domain-joined and non-domain-joined machines.

- For domain-joined machines, make sure that agent host machines belong to the same Active Directory domain as the configured Cloud Connectors. Also, make sure that the agent host machines in each resource location are joined correctly.
- The process of installing agents on machines that are non-domain-joined is similar to that of domain-joined machines. However, make sure that you satisfy all requirements and select the correct options throughout the process. For more information, see Manage non-domain-joined machines.

There are three methods to connect the agent to the WEM service:

- Cloud Connector

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

- Non-domain-joined
- Enrollment

For more information about the methods, see Determine which setup method to use.

Install the agent

> **Note:**
>
> To access resources published in Citrix Workspace as application shortcuts from the administration console, ensure that Citrix Workspace app for Windows is installed on the agent machine. For more information, see System requirements.

Use the following sequence to install your WEM agent.

Step 1: Download the agent

Download the WEM agent package (*Citrix-Workspace-Environment-Management-Agent-Setup.zip*) from the WEM service **Utilities** tab and save a copy on each agent host.

Step 2: Configure group policies (optional)

> **Important:**
>
> Skip this step if you choose to use the non-domain-joined or the enrollment method.

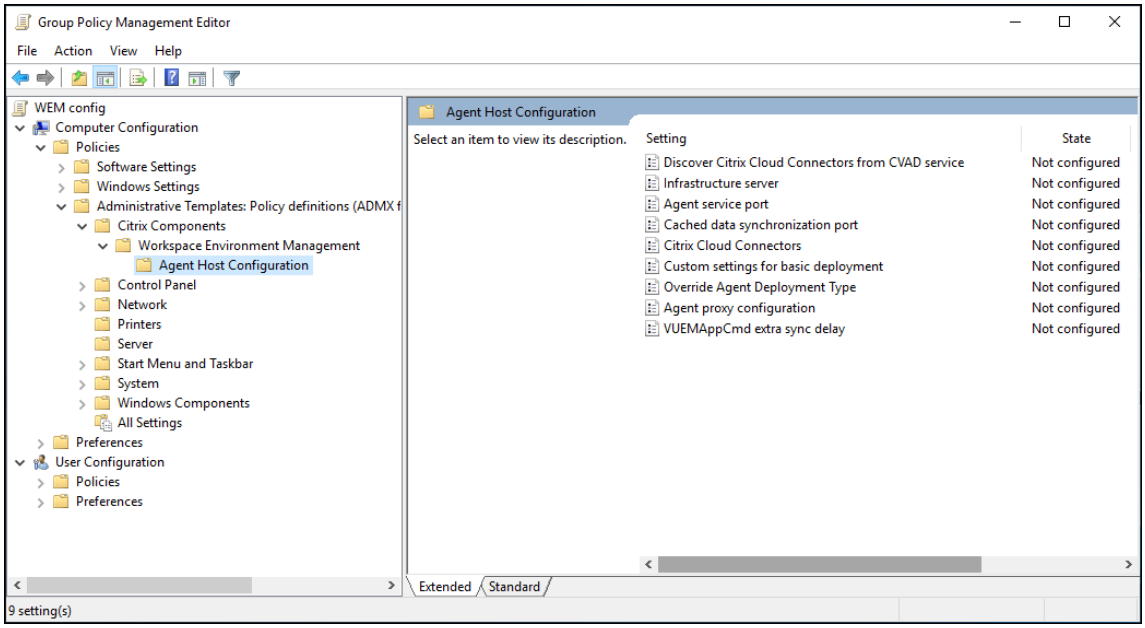
Optionally, you can choose to configure the group policies. The **Agent Group Policies** administrative template, provided in the WEM agent package, adds the Agent Host Configuration policy.

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 **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*).

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

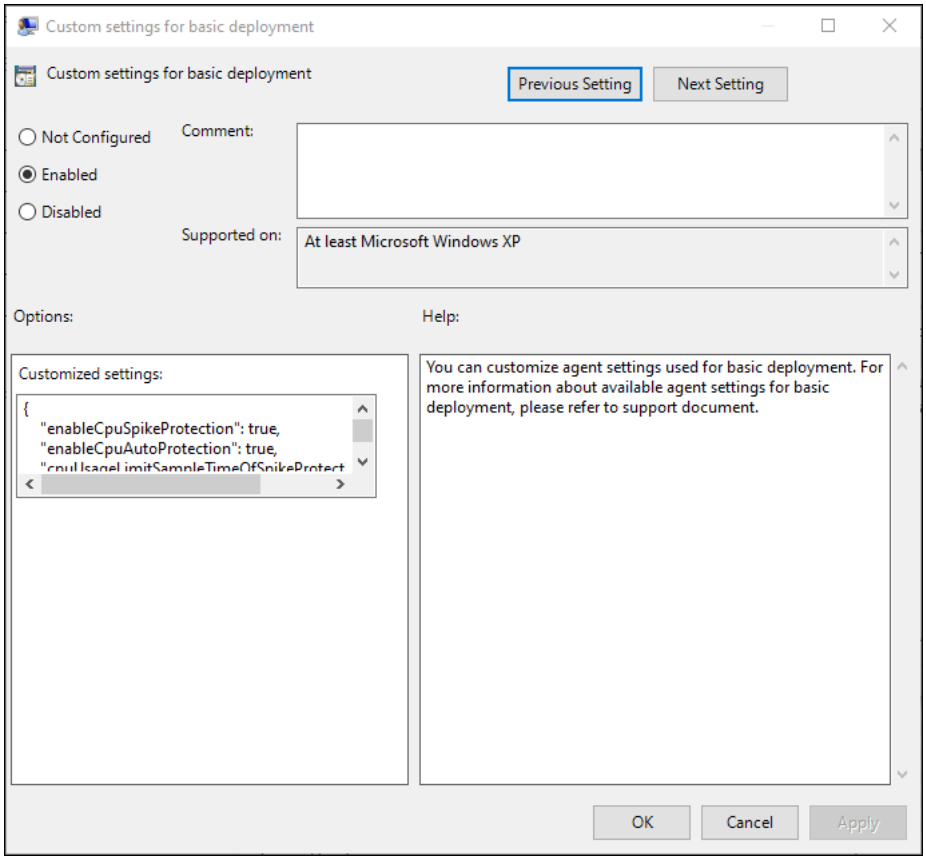
c) Go to the <C:\Windows>\PolicyDefinitions\en-US folder and then paste the files.

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:



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.

Agent proxy configuration. The WEM agent relies on internet connections to connect to the WEM service in Citrix Cloud. The communication between the agent and the service serves the following purposes:

- Uploading statistics and status to the WEM service
- Keeping the agent cache in sync with the WEM service database
- Retrieving the agent settings and the WEM settings specific to the agent's configuration set

Optionally, you can choose to configure an HTTPS proxy to define how the agent communicates with

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

the service. To do so, double-click the **Agent proxy configuration** policy and then type a proxy server address in this format: `http://<FQDN or IP address>:<port number>`. Example: `http://10.108.125.51:8080`.

> **Note:**
>
> WEM service does not support proxy servers that require authentication.

Agent service port. Not required for WEM service. Leave state "Not configured."

Cached data synchronization port. Not required for WEM service. Leave state "Not configured."

Citrix Cloud Connectors. Configure at least one Citrix Cloud Connector. Agent host machines must be in the same AD domain as the configured Cloud Connector machines.

Discover Citrix Cloud Connector from CVAD service. Lets you control whether the agent discovers Cloud Connector information from the relevant Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) deployment if you have not yet configured Cloud Connectors for the agent. The agent then connects to the corresponding Cloud Connector machines.

> **Note:**
>
> - This setting is designed for scenarios where the WEM agent is running in a Citrix DaaS™ deployment.
> - This policy setting does not work if Cloud Connectors are configured during agent installation or the Citrix Cloud Connectors policy setting is enabled.

Infrastructure server. Not required for WEM service. Leave state "Not configured."

VUEMAppCmd extra sync delay. Specifies, in milliseconds, how long the agent application launcher (VUEMAppCmd.exe) waits before 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 3: 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.

The agent setup program *Citrix Workspace™ Environment Management Agent* is provided in the agent download. You can choose to install the agent interactively or using the command line. By default, the agent installs into one of the following folders, depending on your operating system (OS):

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

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

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

To install the agent interactively, complete the following 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**.

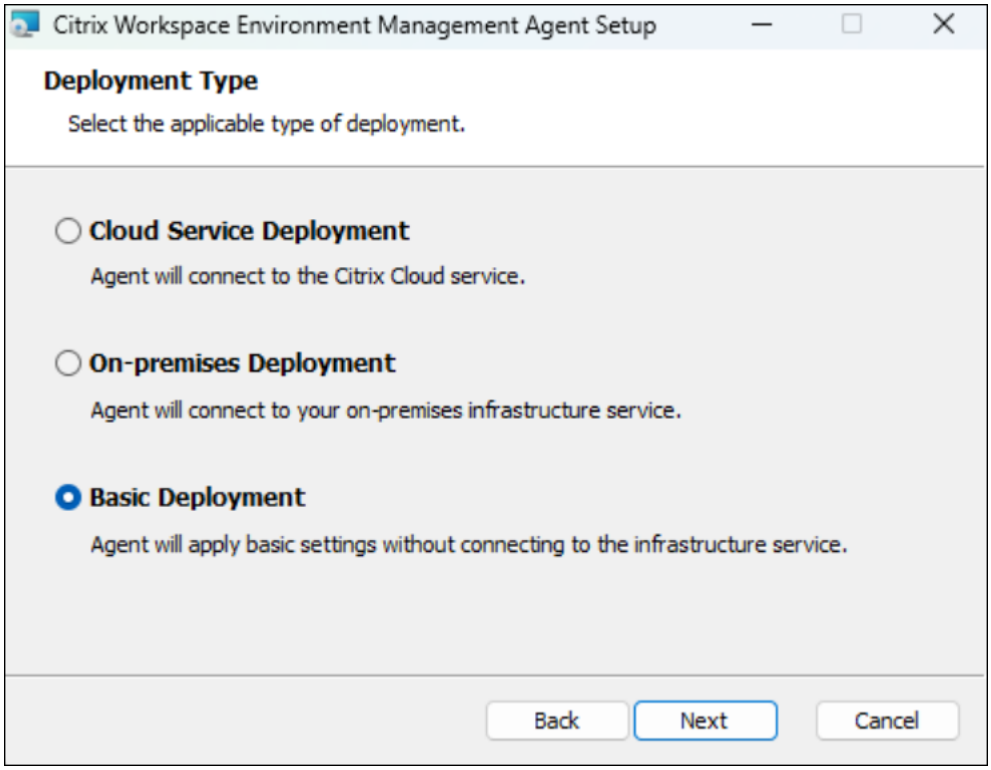
   > **Note:**
   >
   > The Welcome page can take some time to appear. This happens when the required software is missing and is being installed in the background.

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 the WEM agent is already installed, the destination folder field is automatically populated 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 **Cloud Service Deployment**.
6. You can also select the **Basic Deployment** type. When you select the **Basic Deployment** type, the agent turns on the default optimization settings without connecting to the infrastructure service. **Basic deployment** type is the default deployment type for a fresh install.

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

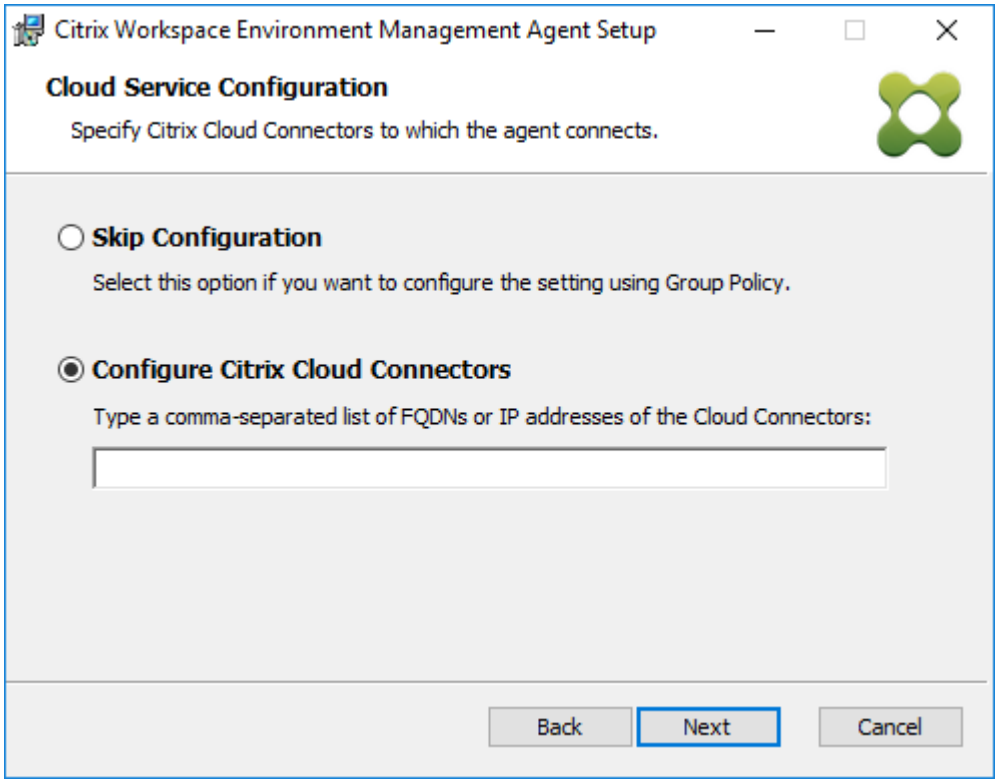


7. On the Cloud Service Configuration page, specify the Citrix Cloud Connectors to which the agent connects and then click **Next**.

   - **Skip Configuration**. Select this option if:
     - You have already configured the setting using Group Policy.
     - The agent machine is a non-domain-joined machine. See Manage non-domain-joined machines.
     - You want to enroll the agent without configuring Cloud Connectors. See Enroll the agent.
   - **Configure Citrix Cloud Connectors**. Configure the Citrix Cloud Connectors to which the agent connects by typing a comma-separated list of FQDNs or IP addresses of the Cloud Connectors.

     > **Note:**
     >
     > - Type the FQDN or IP address of each Citrix Cloud Connector. Make sure to separate the FQDNs or IP addresses with commas (,).
     > - In scenarios where multiple Cloud Connectors are configured, the WEM agent randomly selects from the list a Cloud Connector that is reachable. This design intends to distribute traffic across all Cloud Connectors.

© 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**.

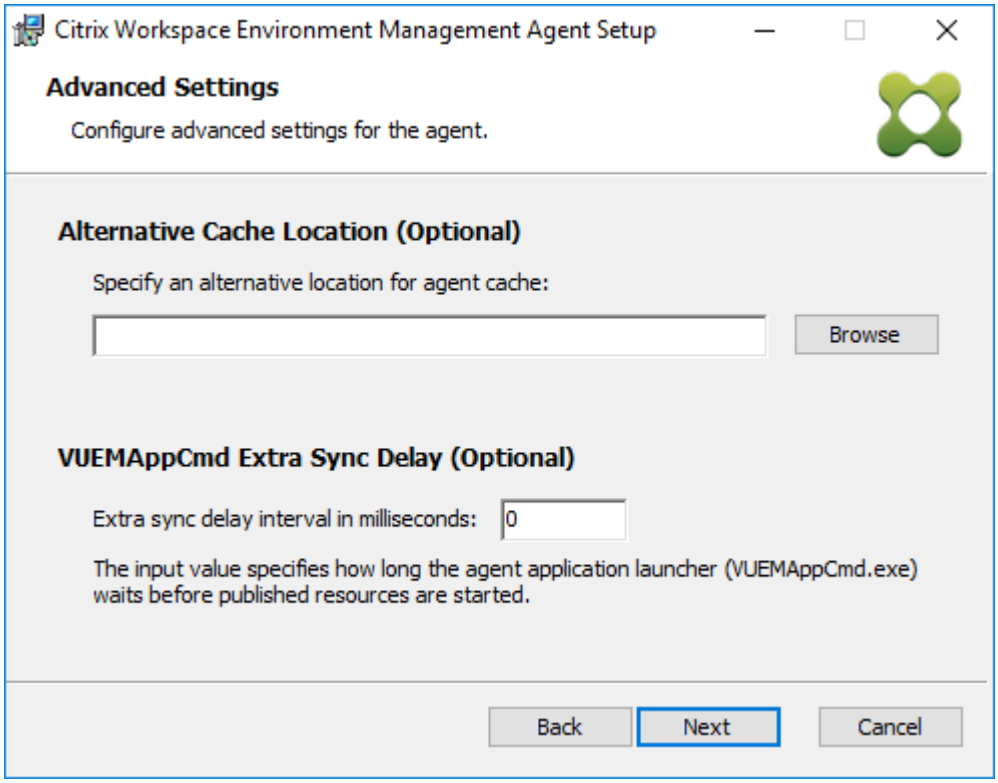
     > **Caution:**
     >
     > Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting

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

> 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 are started. This 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 install wizard.

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

- `Citrix Workspace Environment Management Agent.exe /quiet Cloud=1`

> **Tip:**
>
> - For agents running in a WEM service deployment, enter `Cloud=1`. For agents running in an on-premises WEM deployment, enter `Cloud=0`.

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

> - 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 agent and system settings during the installation process. For more information, see Good to know.

After installation, the agent runs as the following services: **Citrix WEM Agent Host Service** and **Citrix WEM Agent User Logon Service**. The agent runs as `LocalSystem`. Changing this account is not supported. The agent services require the "log on as a local system"permission.

Step 4: Restart the machine to complete the installations

Uninstall the agent

1. On a machine where the agent is installed, open the system's **Control Panel**.
2. Click **Programs and Features**.
3. Select **Citrix Workspace Environment Management Agent** and then click **Uninstall** in the menu.

If you install the agent as an additional component when installing the VDA, use the WEM installer (MSI) available with the VDA installer to uninstall the agent. The WEM installer `citrix_wem_agent_core.msi` is present in `<VDA installer path>\x64\Virtual Desktop Components`. To uninstall the agent that was installed as an additional component with the VDA, complete the following steps:

1. In the folder, right-click `citrix_wem_agent_core.msi`.
2. Select **Uninstall**.

> **Note:**
>
> After uninstalling the agent, you can use the VDA installer or the WEM installer to install it. Starting with Citrix Virtual Apps and Desktops 2209, the WEM agent is no longer included as an additional component in the VDA installation. To install it, use the full-product installer on the Citrix Virtual Apps and Desktops product ISO. For more information, see Install core components.

Where to go next

If you want to migrate your existing on-premises WEM database into the WEM service, see Migrate to cloud.

To directly get started with the WEM service, start the administration console and configure settings there as needed. There are two consoles available:

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

- Legacy console
- Web console

We are in the process of migrating features from the legacy console to the web console. The web console responds faster than the legacy console and provides more functionalities. To see the features available only in the web console, see What's new.

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.
- If you are using Citrix Virtual Apps and Desktops, the WEM agent can automatically detect the persistent system location, eliminating the need for manual configuration.

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 Net Logon 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.

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

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 Net Logon 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.

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 is currently obsolete and is available only for agent versions before 2401.1.0.1.
- `-RefreshSettings` or `-S`: Refreshes agent host settings including the agent cache for agent versions 2401.1.0.1 or higher.
- `-Reinitialize` or `-I`: Reinitializes the agent cache on the agent, where the agent requests an immediate agent cache sync to get the latest settings from the WEM database directly without any delay.

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

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`

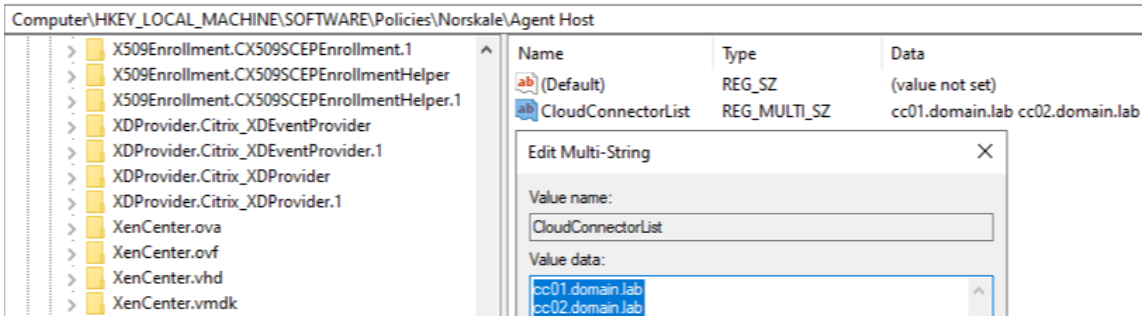
Good to know

The agent executable accepts custom arguments as described below.

Agent settings

See below for the WEM agent settings.

- **AgentLocation**. Lets you specify the agent installation location. Specify a valid folder path.
- **CloudConnectorList**. Lets you specify the FQDN or IP address of each Citrix Cloud Connector. Make sure to separate FQDNs or IP addresses with commas (,).



- **VUEMAppCmdDelay**. Lets you specify how long the agent application launcher (VUEMAppCmd.exe) waits before Citrix Virtual Apps and Desktops published resources are started. 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.
- **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.

Consider the following:

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

- If the settings are configured through the command line, the WEM agent installer uses the configured settings.
- If the settings are not configured through the command line and there are previously configured settings, the installer uses the settings that were previously configured.
- If the settings are not configured through the command line and there are no previously configured settings, the installer uses the default settings.

System settings

See below for the system settings associated with the agent host machine.

- **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.

  > **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.

All the preceding three keys are created under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** during installation. The keys serve to 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, this might result in extra

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

processing time before the logon screen appears. Citrix recommends 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 the preceding settings are not configured using the command line, they are not processed by the WEM agent installer during installation.

Examples

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

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

For example:

- Specify the agent installation location and Citrix Cloud Connectors
  - `"Citrix Workspace Environment Management Agent.exe"/quiet AgentLocation="L:\WEM Agent"Cloud=1 CloudConnectorList=cc1.qa.local,cc2.qa.local`
- Set **user logon network wait time** to 60 seconds
  - `"Citrix Workspace Environment Management Agent.exe"WaitForNetwork=60`

Enroll agents

October 8, 2026

Introduction

You can enroll Workspace Environment Management™ (WEM) agents without configuring Citrix Cloud Connectors. Before doing so, consider the following:

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

- The enrollment applies to both domain-joined and non-domain-joined machines.
- For Citrix DaaS managed VMs, we recommend using the same method to connect the agent to Citrix Cloud as you do for the VDA —through the Cloud Connector or the non-domain-joined method. See Determine which setup method to use.
- To ensure that persistent VMs enroll properly:
  - Remove machine-specific information by generalizing a VM before creating an image. For information about using Sysprep to generalize a VM, see the Microsoft product documentation: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/sysprep--generalize--a-windows-installation?view=windows-11.

This feature requires that you select **Skip Configuration** when installing the agent and that you do not enable the **Discover Citrix Cloud Connector from CVAD service** policy.

Enroll agents

You have the flexibility to determine how to enroll your WEM agents. There are two ways:

- Enroll by invitation. This requires the web console. Users can be invited to participate in the enrollment process.
- Enroll with the bearer token or API secure client. This doesn't require the console and doesn't require users to participate in the enrollment process.

Enroll by invitation

To manage user devices remotely and securely, you enroll user devices in WEM.

A general workflow to enroll by invitation is as follows:

1. In **Manage > Web Console > Enrollment > Invitation**, enable **Enroll by invitation** and then generate an enrollment key.
2. On the agent machine, install the enrollment key using the enrollment tool.
   a) Open the command prompt as the administrator.
   b) Run the following command.(Replace <enrollment key> with the actual key.)
      - `Citrix.Wem.Agent.EnrollmentUtility.exe configenrollmentkey -k <enrollment key>`

> **Tip:**
>
> - The enrollment tool, **Citrix.Wem.Agent.EnrollmentUtility.exe**, is available in the agent installation folder. For more information, see Enrollment tool.

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

> - When preparing a master image, you can install the agent on the master image. Then, you use the master image as a template for creating machines for your users. This way, you don't need to install the enrollment key for each agent.

3. In **Manage > Web Console > Enrollment > Invitation**, send an enrollment invitation to users.

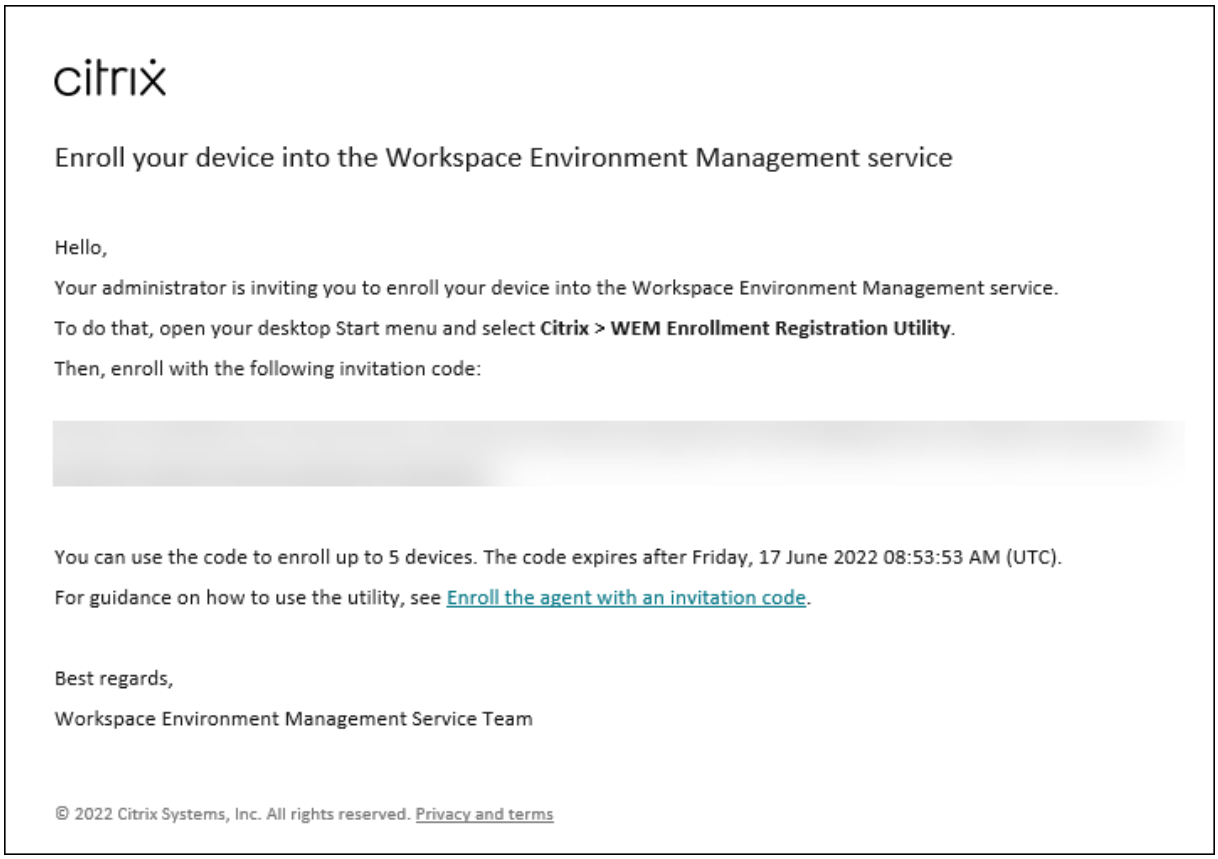
After users receive the invitation, they can enroll their devices using the invitation code. See Enroll the agent with an invitation code.

After a device enrolls, it becomes managed and appears in **Manage > Web Console > Enrollment > Enrolled Agents**. You can add it to a desired configuration set for precise management. See Manage the enrolled agent.

Enroll the agent with an invitation code

> **Important:**
>
> Enrolling an agent requires *local administrator permissions*.

As users, you receive the following invitation email:



citrix

Enroll your device into the Workspace Environment Management service

Hello,

Your administrator is inviting you to enroll your device into the Workspace Environment Management service.

To do that, open your desktop Start menu and select **Citrix > WEM Enrollment Registration Utility**.

Then, enroll with the following invitation code:

You can use the code to enroll up to 5 devices. The code expires after Friday, 17 June 2022 08:53:53 AM (UTC).

For guidance on how to use the utility, see Enroll the agent with an invitation code.

Best regards,

Workspace Environment Management Service Team

© 2022 Citrix Systems, Inc. All rights reserved. Privacy and terms

Enroll your device using the invitation code as follows:

1. Open your desktop Start menu and select **Citrix® > WEM Enrollment Registration Utility**.

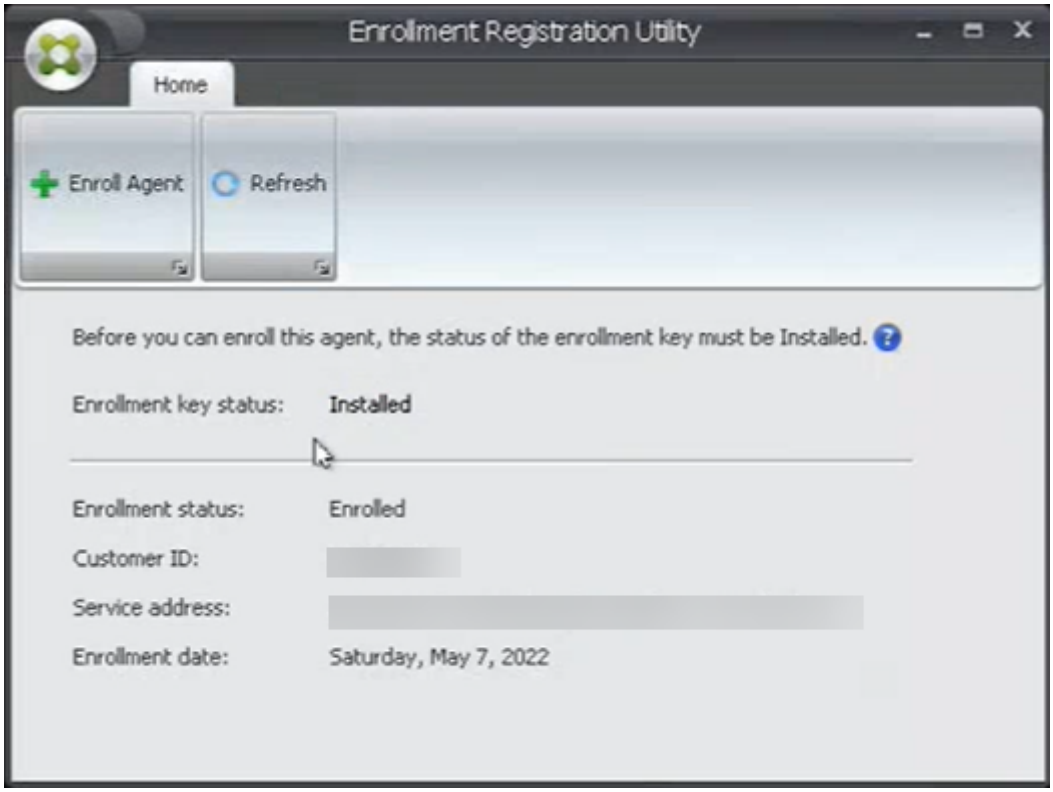
> **Tip:**
>
> If the utility is not available in the Start menu, go to the WEM agent installation folder and open **Citrix.Wem.Agent.Enrollment.RegUtility.exe**.

2. In **Enrollment Registration Utility**, verify that the status of the enrollment key is **Installed** and click **Enroll Agent**.

   > **Note:**
   >
   > If the status of the enrollment key is not **Installed**, contact your administrator.

3. In the **Enroll Agent** window, paste the invitation code (copied from the invitation email) and click **Start Enrolling**.

If the agent enrolls successfully, you see the following message: **The agent was enrolled successfully**. You can click **Close** to return to **Enrollment Registration Utility**, which shows the following information:



> **Note:**
>
> Enrolling with the bearer token or API secure client does not require the participation of the enrollment key. If you use the **Enrollment Registration Utility** to check the enrollment status on

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

> an agent machine enrolled with the bearer token or API secure client, the **Enrollment key status** field appears as **Not installed** and the **Enrollment status** field appears as **Enrolled**.

Enroll with the bearer token or API secure client

To enroll an agent machine, perform the following steps:

1. Sign in to Citrix Cloud and get a bearer token or an API secure client for authentication to the Citrix API service. For information about how to generate an API secure client and a bearer token, see Get started with Citrix Cloud APIs.
2. Log on to the machine that has the agent installed.
3. Open a command prompt window.
    - To enroll the agent with the bearer token, type the following command:
        - `Citrix.Wem.Agent.EnrollmentUtility.exe enroll --customer "customerid"--bearer "bearertoken"--url "api.wem.cloud.com"`

        > **Tip:**
        >
        > When using a bearer token, be aware that the base URL is unique for each region. For more information, see Base URLs. If unspecified, the URL for the US region (api.wem.cloud.com) is used.

    - To enroll the agent with the API secure client, type the following command:
        - `Citrix.Wem.Agent.EnrollmentUtility.exe enroll --customer "customerid"--clientid "clientid"--clientsecret "clientsecret"--authurl "api-us.cloud.com"--url "api.wem.cloud.com"`

        > **Tip:**
        >
        > - When using a secure client, be aware that there are two URLs.
        > - The first URL is the authentication URL, which is unique for each region. For more information, see Get started with Citrix Cloud APIs. If unspecified, the URL for the US region (api-us.cloud.com) is used.
        > - The second URL is the base URL, which is also unique for each region. For more information, see Base URLs. If unspecified, the URL for the US region (api.wem.cloud.com) is used.

Alternatively, in Step 3, create a configuration file in JSON format and use the file with the following command:

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

- `Citrix.Wem.Agent.EnrollmentUtility.exe enroll --config "configfilepath"`

> **Note:**
>
> We recommend that you delete the configuration file after the enrollment because the file contains sensitive information.

The format of the configuration file is as follows:

> **Tip:**
>
> When using a bearer token or secure client, you can leave the corresponding fields empty.

```
{


"CustomerId": The Citrix Cloud customer ID,

"ClientId": The secure client ID of the Citrix Cloud API client,

"ClientSecret": The secure client secret of the Citrix Cloud API
   client,

"AuthUrl": The base URL of the Citrix Cloud API used to get the
   bearer
token,

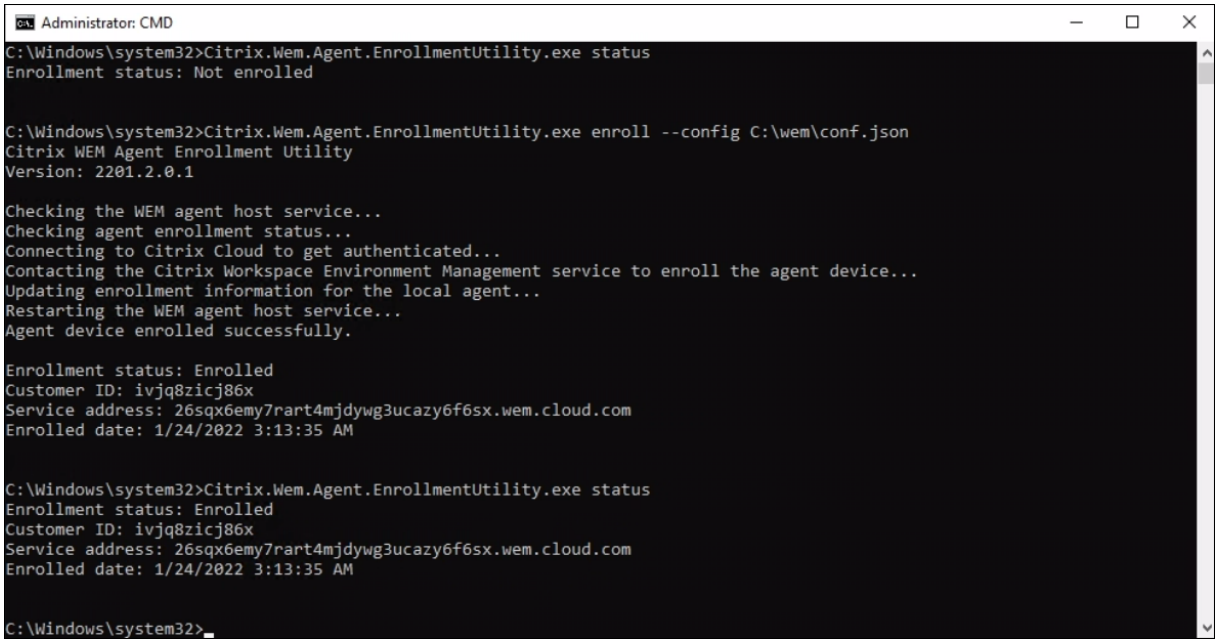
"BearerToken": The Citrix Cloud bearer token,

"BaseUrl": The base URL of the WEM RESTful APIs

 }
```

Example output:

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



Manage the enrolled agent

After enrolling an agent, use the management console to bind it to a desired configuration set for precise management.

- In the web console, go to **Directory Objects** and then add the agent machine to a configuration set. See Directory Objects.
- In the legacy console, go to **Active Directory Objects > Machines** and then add the agent machine to a configuration set. See Active Directory Objects.
- For information about adding non-domain-joined machines, see Manage non-domain-joined machines.

> **Note:**
>
> - After you add an enrolled non-domain-joined machine, the agent first registers with the **Default Site** configuration set or the **Unbound Agents** configuration set (if enabled). After the agent is registered, you can add the machine to other configuration sets.

Key creation and rotation

A service key is created in the cloud when an agent enrolls into WEM successfully. Consider the following rules:

- The key expires in 90 days. After it expires, the agent must connect to the WEM service to rotate the key. By default, the agent automatically connects to rotate the key 14 days before the

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

expiration.
- The expired key is kept for 180 days. The agent must rotate the key within 180 days. After that, the key will be deleted.
- If the key is deleted, the agent using the key can no longer connect to the WEM service. The agent must be reenrolled.

> **Note:**
>
> An identity change can cause a mismatch between the service key and the agent identity. An identity change can occur, for example, when an agent machine joins or leaves a domain. In that case, you must let the agent connect to the WEM service when the key is still valid so that the agent can rotate the key.

Enrollment tool

The agent enrollment tool, **Citrix.Wem.Agent.EnrollmentUtility.exe**, is available in the WEM agent installation folder. By default, the agent is installed in the following default folder.

- `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)

Command-line options with the enrollment tool

The tool has the following options:

Parameter	Description
status	Displays the current enrollment status of the agent machine.
enroll	Enrolls the agent machine with the Citrix Workspace™ Environment Management service.
configenrollmentkey	Configures the enrollment key.
help	Displays more information on a specific command.
version	Displays version information for the tool.

For example, to display agent enrollment status, type the following command:

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

- `Citrix.Wem.Agent.EnrollmentUtility.exe status`

The tool provides the following options for enrollment:

Parameter	Description
–config	Reads configurations from a configuration file in JSON format.
-c, –customer	The Citrix Cloud customer ID.
-b, –bearer	The Citrix Cloud bearer token.
–clientid	The secure client ID of the Citrix Cloud API client.
–clientsecret	The secure client secret of the Citrix Cloud API client.
–authurl	The base URL of the Citrix Cloud API used to get the bearer token. Default: `api-us.cloud.com`.
-u, –url	The base URL of the WEM RESTful APIs. Default: `api.wem.cloud.com`.
-f, –force	Enrolls the agent machine regardless of its current enrollment status. Default: false.
-k, –key	Sets the enrollment key.
-f, –file	Reads the enrollment key from a file and sets the enrollment key.
-s, –status	Shows the current status of the enrollment key.
–help	Displays cmdlet help.
–version	Displays version information for the tool.

Return codes

The tool can return the following codes:

Code	Description
0	No error
1	Invalid arguments
2	Insufficient permissions
3	Agent host service not ready

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

Code	Description
4	Error while calling remote APIs
100	Unhandled exception
1000	Agent not enrolled
1001	Agent currently enrolled. When enrolling the agent, the operation is skipped unless the `–force` option is specified.
2000	Enrollment key not installed
2001	Enrollment key installed

Unenroll the agent

To unenroll the agent, use the agent installer when uninstalling the agent, with the following command:

- `citrix_wem_agent_bundle.exe /uninstall Disenroll=1`

After uninstalling the agent, the following registry key is removed:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\WEM\Agent\Enrollment`

Upgrade

September 7, 2025

> **Note:**
>
> Starting with WEM agent 2211.1.0.1, agents download configuration data only when needed. This enhancement can reduce bandwidth consumption by up to 50%. See What's new. We recommend that you upgrade your agents to 2211.1.0.1 or later so that you can reap the benefit.

Citrix® maintains all Workspace Environment Management™ (WEM) service components in your deployment except WEM service agents.

You can upgrade WEM service agents to a newer version without losing any of their existing configurations. This is called an in-place upgrade.

By default, when new versions of the WEM service agent are released, you receive email notifications. You can choose to unsubscribe if you do not want to receive such emails in the future. To do that, go

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

to the WEM service **Utilities** tab and then click **Unsubscribe** in the **Notifications about new agent versions** section.

> **Important:**
>
> - Before upgrading a WEM service agent, ensure that no users are logged on. Doing that ensures that files on agent machines can be changed during the upgrade process.
> - We recommend that you upgrade the agent to the latest version so that you can use the most recent features.

Upgrade the agent

1. Download the latest WEM service agent package from the WEM service **Utilities** tab.
2. Deploy the new WEM service agent on each target machine as described in Install and configure.

Automatic agent upgrade

> **Note:**
>
> If you use the automatic agent upgrade feature to roll out agent upgrades to non-persistent machines, the upgrades are reverted after the restart of the machines.

You can use the automatic agent upgrade feature to schedule automatic upgrades for the WEM agent. The feature facilitates regular agent upgrades without the need to roll out agent upgrades manually. The feature also provides flexibility in upgrading your WEM agents:

- You can specify a time period for which you want WEM to automatically roll out the upgrade to all agent machines in a configuration set.
- Alternatively, you can choose to enable users to upgrade the agent manually.

For more information, see Create a WEM Agent upgrade task.

Upgrade the agent on demand

You can upgrade your agents from the console on demand. The option is available in both the legacy console and the web console. To use the feature:

- In the legacy console, go to **Administration > Agents**, right-click an agent, and then select **Upgrade agent to latest version**. For more information, see Administration.
- In the web console, go to **Monitoring > Administration > Agents**, select one or more agents, click **More**, and then select **Upgrade agent to latest version**. For more information, see Administration.

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

Migrate

September 7, 2025

> **Important:**
>
> - If you intend to migrate your existing on-premises WEM database into the WEM service, make sure that you use the latest version of the migration tool.
> - To ensure that the migration tool works as expected, you might must upgrade the .NET Framework. If you use WEM 1909 or earlier, upgrade to .NET Framework 4.7.1 or later on the machine where you run the tool.
> - We recommend that you run the migration tool on the machine where the infrastructure service is installed. Doing so ensures that the infrastructure service can connect to the WEM database and that the machine on which the infrastructure service is running has the necessary components.

We provide you with a toolkit to migrate your existing on-premises Workspace Environment Management™ (WEM) database into the WEM service. The toolkit includes a wizard to generate an SQL file containing the contents of your WEM database, and a simple way to upload the SQL file to the WEM service Azure database. This article describes how to complete your on-premises database migration. Review the entire sequence before starting the migration process so that you know what to expect.

Before you migrate your WEM database, keep the following in mind:

- After your migration completes successfully, all data associated with your current WEM service database will be lost.
- You can migrate your WEM database only after your WEM service is successfully provisioned.
- Before starting the migration process, Citrix® recommends that you back up your on-premises WEM database.
- Before starting the migration process, Citrix recommends that you configure your database maintenance on the **Database Maintenance** tab. Doing so reduces the size of your WEM database so that you have a better migration experience. For more information on database maintenance, see Configure the infrastructure service.
- If you attempt to migrate your WEM database while the WEM service is upgrading, the following error message appears in the notifications area in the top-right corner of the Citrix Cloud™ user interface: "The Workspace Environment Management database migration has failed because the Workspace Environment Management service is upgrading. Please try again later."When this happens, try uploading the SQL file after your WEM service is upgraded successfully. Service upgrades are also notified in the top-right corner of the Citrix Cloud user interface.

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

System requirements

The toolkit supports the migration from WEM 4.7 and later. To migrate from an earlier version, upgrade WEM 4.x to WEM 4.7 or later, and then migrate the database to the WEM service. For more information on upgrading, see Upgrade a deployment.

Get started

Log on to your Citrix Cloud account. For more information, see What is a Citrix Cloud account.

Migrate your on-premises database

Step 1: Download the migration tool

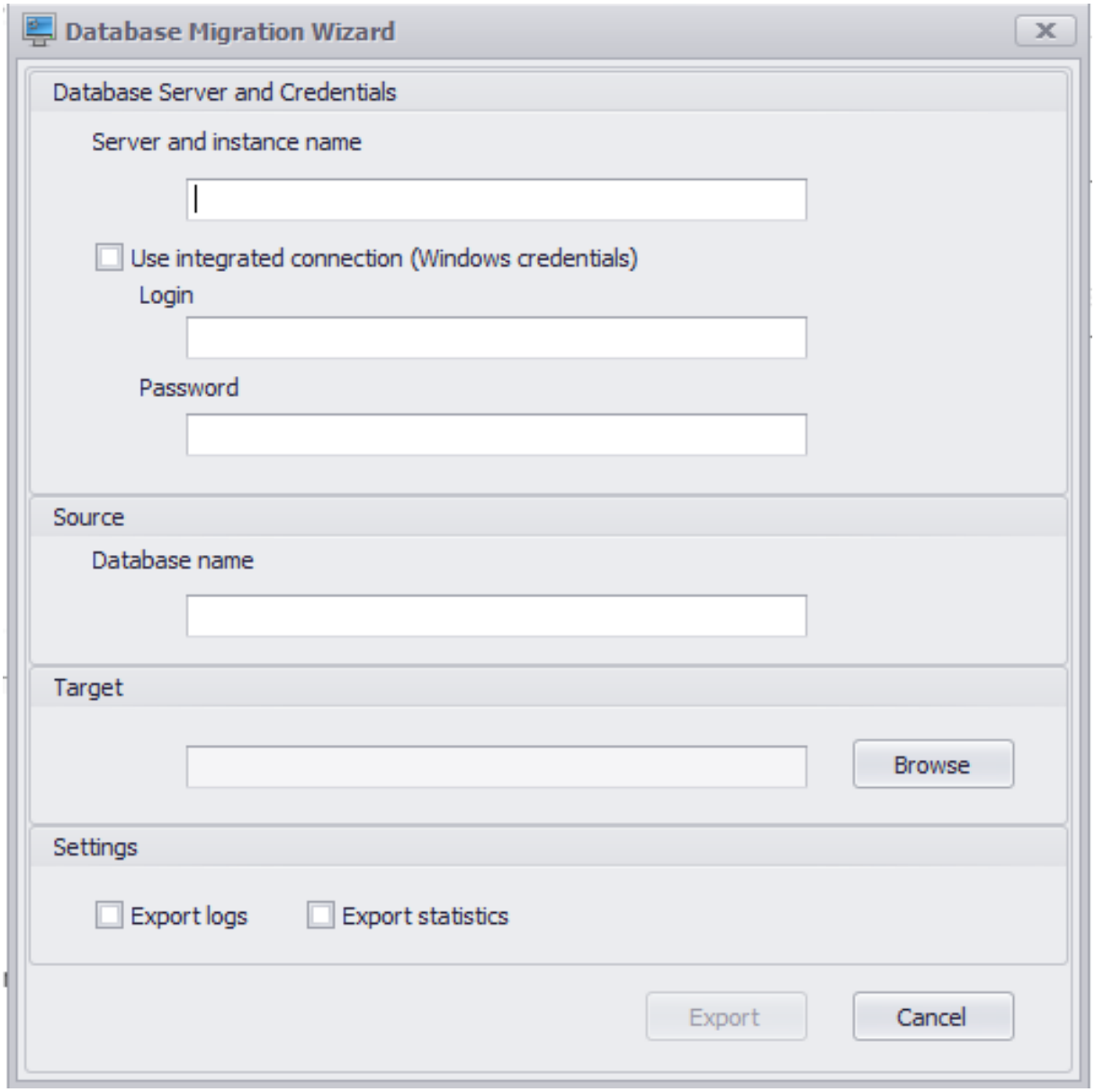
Download the migration tool (WEM-migration-tool.zip) from the WEM service **Utilities** tab. Extract the zip file to a convenient folder.

> **Note:**
>
> Citrix recommends that you run the migration tool on the machine where the infrastructure service is installed. Doing so ensures that the infrastructure service can connect to the WEM database and the machine on which the infrastructure service is running has the necessary components.

Step 2: Export the database data to an SQL file

Run the **Citrix WEM Migration Tool.exe** contained in the zip file.

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



Enter the following data in the wizard:

Server and instance name. Address of the SQL server instance that hosts the database. It must be reachable from the infrastructure server exactly as typed here.

Use integrated connection (Windows credentials). If selected, allows the **Database Migration Wizard** to use the Windows account of the identity it is running under to connect to the SQL server, and then generate the SQL file containing the contents of your on-premises WEM database. If this Windows account does not have sufficient permissions, run the **Citrix WEM Migration Tool.exe** using a Windows account with sufficient privileges, or clear this option and provide an SQL account with sufficient privileges instead.

Database name. Name of the database to be migrated.

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

Target. The desired folder for saving the SQL file containing the contents of your on-premises WEM database. Use the **Browse** button to navigate to the folder where you want to save the SQL file.

Export logs. Controls whether to export logs. The logs contain changes made to your WEM agents. If enabled, the database file to be exported contains the logs. To speed up your migration, we recommend that you do not enable this option.

Export statistics. Controls whether to export agent and user statistics. If enabled, the database file to be exported contains the statistics. By default, this option is disabled. To speed up your migration, we recommend that you do not enable this option.

> **Note:**
>
> When saving as a file, your WEM database file is automatically renamed to "Your database name_upload.7z."

Click **Export** to start the database export process or click **Cancel** to exit the **Database Migration Wizard**.

During the export process, the **Database Migration Status** window appears.

After the export process finishes, click **Finish** to close the window and to return to the **Database Migration Wizard**.

> **Note:**
>
> - Depending on your database size, the export process can take from a few seconds to a few minutes or even a few hours.
> - If you close the **Database Migration Status** window when the database export is in progress, you return to the **Database Migration Wizard**, but the **Export** button is disabled because the database export process continues in the background. To stop the export process completely, click **Cancel**.

If there are errors during export, check the **Citrix WEM Migration Tool Debug Log** file in the migration tool folder that contains the **Citrix WEM Migration Tool.exe**.

Step 3: Upload the SQL file into your WEM service database

> **Important:**
>
> Do not close the Workspace Environment Management service page before the upload finishes. Otherwise, your SQL file cannot be uploaded successfully.

1. On the WEM service **Utilities** tab, click **Upload** to start the upload process.
2. Click **Choose File** on the Upload SQL file page and then select the SQL file to be uploaded.

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

3. Click **OK** to start the upload and to return to the WEM service **Utilities** tab.

After you return to the WEM service **Utilities** tab, the progress message appears under **Upload**, which updates as the upload progresses. After your SQL file is uploaded successfully, the migration process starts automatically.

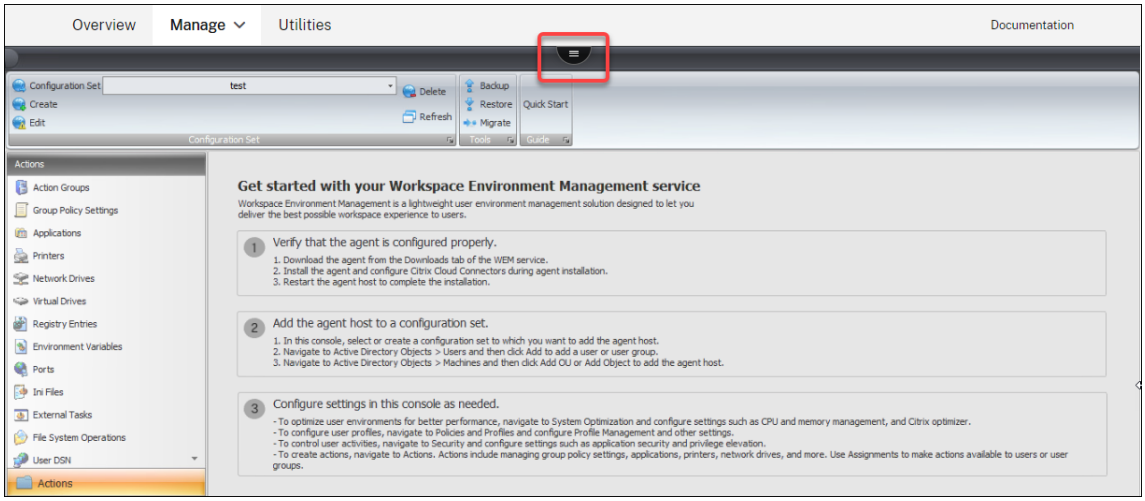
> **Note:**
>
> After your SQL file is uploaded successfully, you must wait 10 minutes before you can upload again.

After migration

You receive a notification message a few hours later, communicating the result of the migration to you. See notifications in the top-right corner of the Citrix Cloud user interface. After the migration completes successfully, perform the following steps on the **Manage** tab to view the data migrated from your on-premises WEM database.

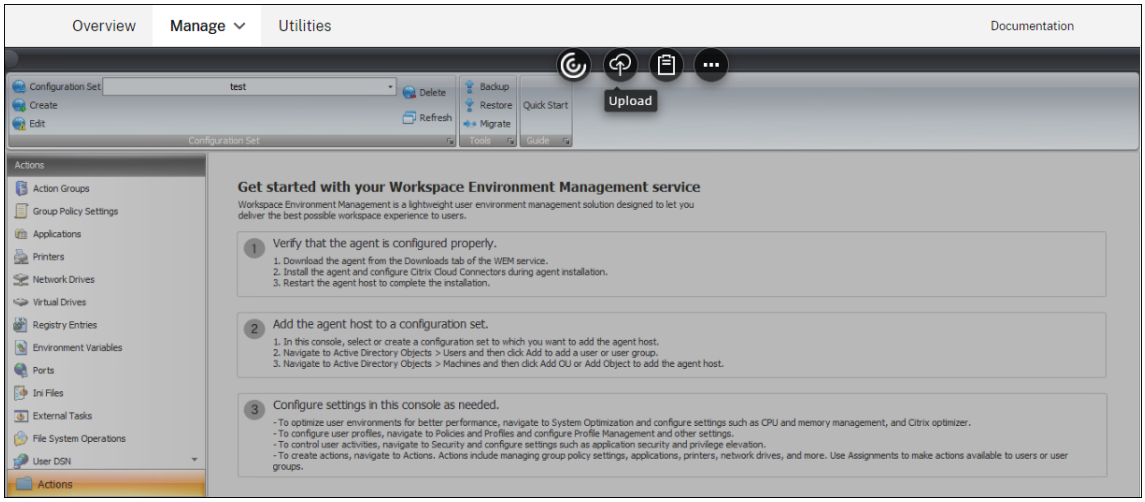
Step 1: Load the migrated data into the WEM service console

1. In **Manage > Legacy Console**, hover over the hamburger menu.



2. Click the Citrix Workspace™ icon.

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



3. Click the ellipsis icon to expand additional options.
4. Click **Log Off** to disconnect from the WEM service.
5. Refresh your browser window to reconnect to the WEM service and to view the data migrated from your on-premises WEM database.

Step 2: Switch to service agent mode

Use the agent switch feature to switch from on-premises to service agent mode. For information about the agent switch, see Agent Switch.

> **Important:**
>
> The agent switch feature is available in Workspace Environment Management 1909 and later. For earlier versions, you must reinstall the agent or upgrade it to version 1909 or later before using the agent switch.

Alternatively, you can download the agent from the service's **Utilities** tab and then manually reinstall the agent.

Manage (legacy console)

September 7, 2025

Start the administration console

1. Log on to your Citrix Cloud™ account.

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

2. In the Workspace Environment Management™ (WEM) service tile, click **Manage**.
3. In **Overview**, click **Manage Service** or click the **Manage** tab.

Configure your deployment

Use the **Manage** tab to configure WEM settings.

- Click items in the lower-left-hand pane to display their subsections.
- Click subsection items to populate the main window area with appropriate content.
- Change configuration as needed. For information about settings you can use, see user interface description (legacy console)

Get started with your WEM service

1. Verify that the agent is configured properly.

    a) Download the agent from the **Utilities** tab of the WEM service.
    b) Install the agent and configure Citrix Cloud Connectors during agent installation.
    c) Restart the agent host to complete the installation.

2. Add the agent host to a configuration set.

    a) In this console, select or create a configuration set to which you want to add the agent host.
    b) Navigate to **Active Directory Objects > Users** and then click **Add** to add a user or user group.
    c) Navigate to **Active Directory Objects > Machines** and then click **Add OU** or **Add Object** to add the agent host.

3. Configure settings in this console as needed.

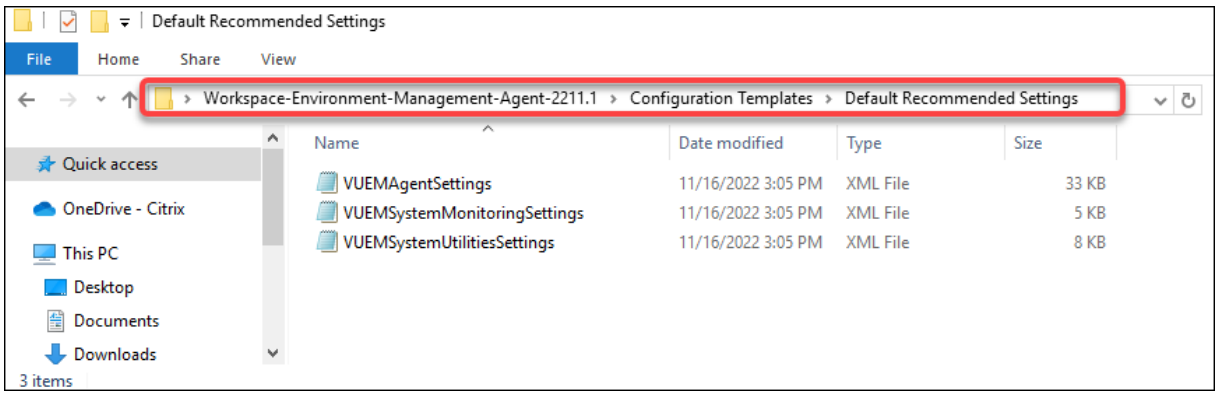
    - To optimize user environments for better performance, navigate to **System Optimization** and configure settings such as CPU and memory management, and Citrix® optimizer.
    - To configure user profiles, navigate to **Policies and Profiles** and configure Profile Management and other settings.
    - To control user activities, navigate to **Security** and configure settings such as application security and privilege elevation.
    - To create actions, navigate to **Actions**. Actions include managing group policy settings, applications, printers, network drives, and more. Use **Assignments** to make actions available to users or user groups.

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

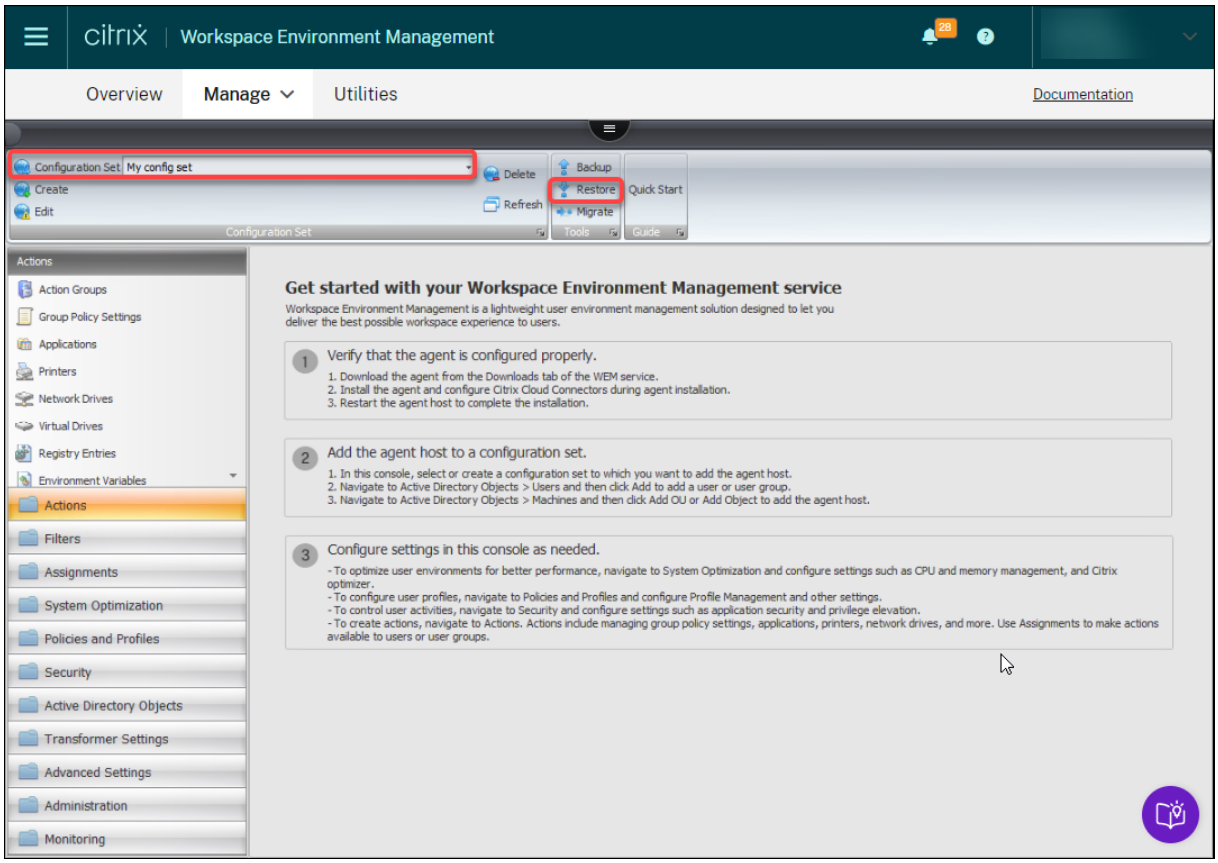
Import recommended settings

> **Note:**
>
> If you have multiple configuration sets, you need to import recommended settings for each.

You can import Citrix-recommended settings into your configuration set and then adjust and apply them as needed. The recommended settings are provided with the WEM agent package. To download the package, go to **Citrix Cloud > WEM service > Utilities**.

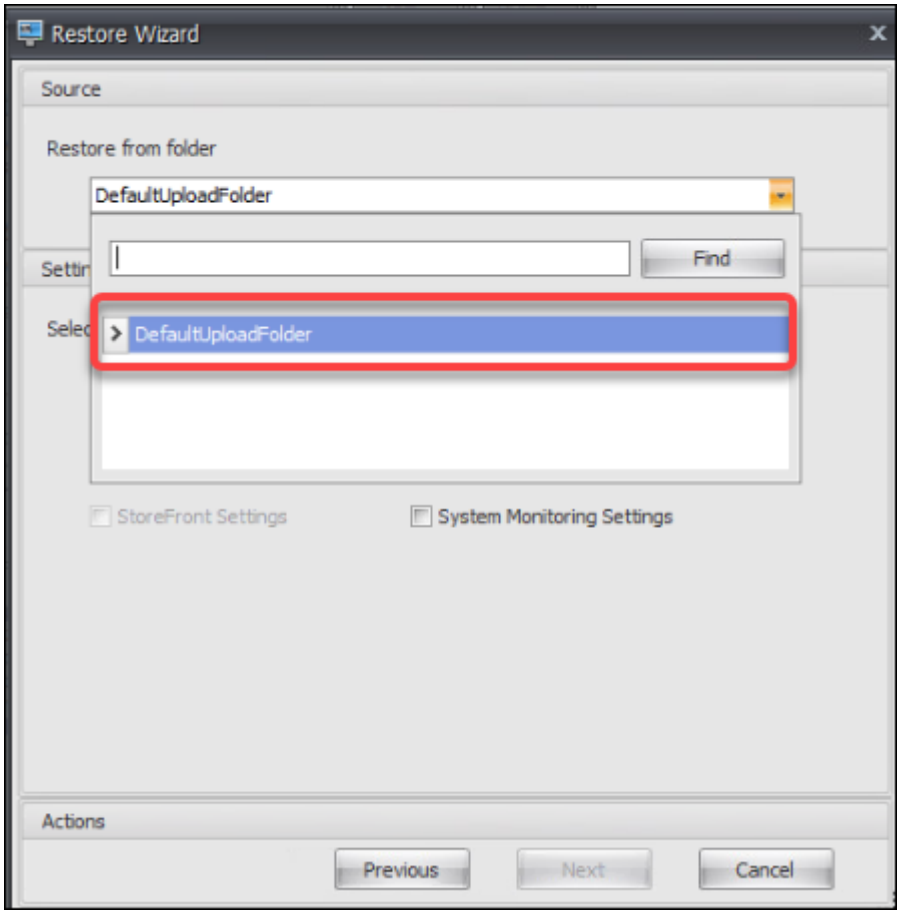


To import recommended settings, use Restore, available in the ribbon of the console. Before you start, first upload default recommended settings into WEM. See Upload files.



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

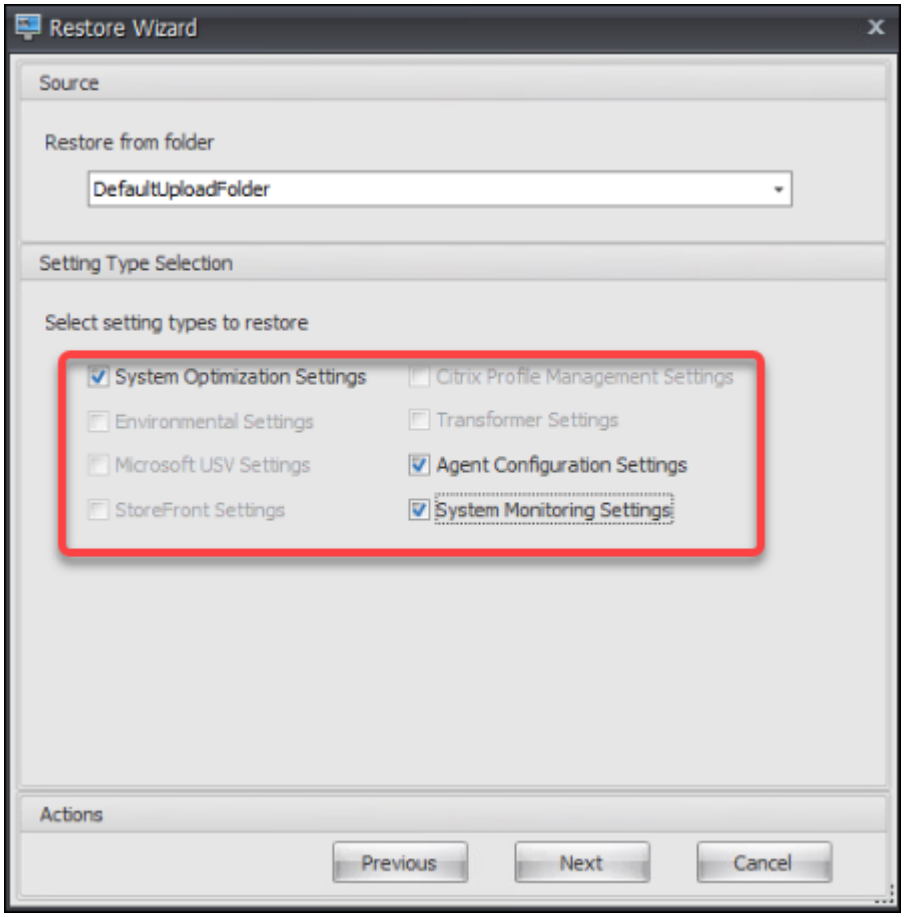
1. Under the target configuration set, click **Restore**. The Restore wizard appears.
2. On the **Select what to restore** page, select **Settings** and then click **Next**.
3. On the **Restore settings** page, click **Next**.
4. On the **Source** page, select `DefaultUploadFolder` to restore the settings from.



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

> **Note:**
>
> The three options let you import all Citrix-recommended settings. For example, the **System Optimization Settings** option lets you apply basic system optimization settings to the configuration set. Basic settings include CPU spike protection, auto-preventing CPU spikes, and intelligent CPU optimization.

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

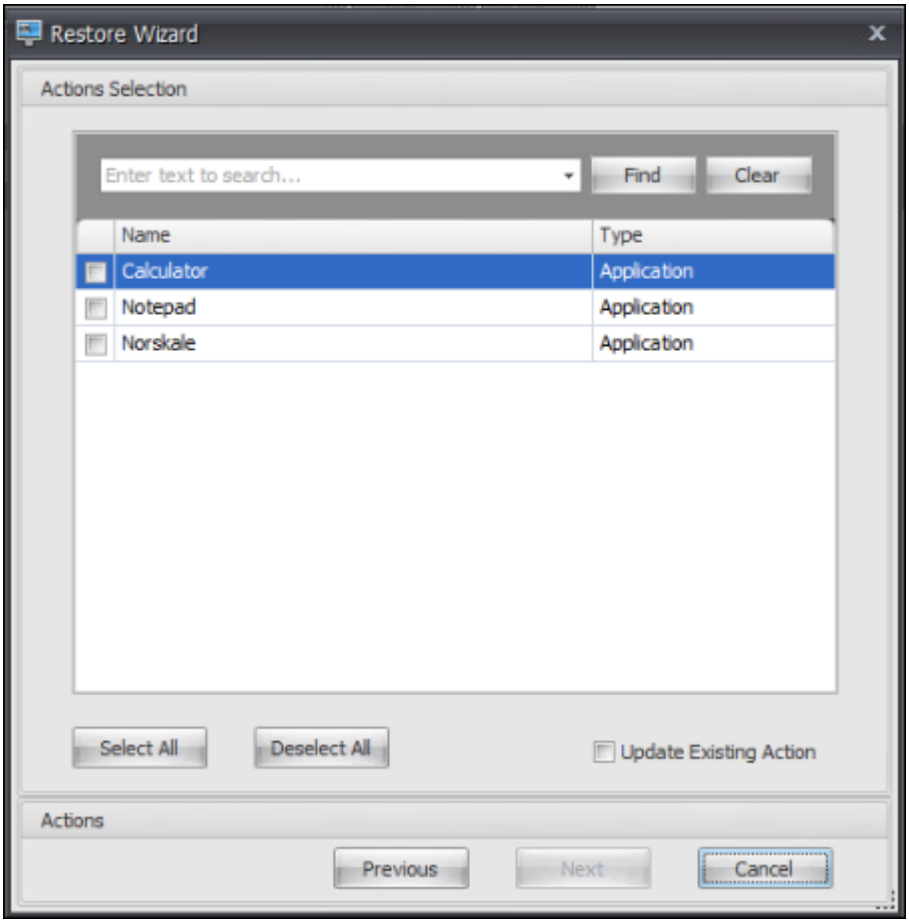


6. On the **Restore settings processing** page, click **Restore Settings** to start the import.
7. Click **Yes** to confirm the action.
8. Click **Finish**.

In addition to recommended settings, the WEM agent package also includes the following settings:

- **Environment Lockdown Sample > VUEMEnvironmentalSettings**. Use this file to import environment settings. To do so, repeat the steps above, minding the following:
  - On the **Source** page, select **Environmental Settings**.
- **Sample Applications > VUEMApplications**. Use this file to import sample applications. To do so, repeat the steps above, minding the following:
  - On the **Select what to restore** page, select **Actions** and then click **Next**.
  - On the **Source** page, select **Applications**.
  - On the **Actions Selection** page, select the actions you want to import.

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



- On the **Restore actions processing** page, click **Restore Actions** to start the import.

> **Note:**
>
> The following are the configuration template files for the WEM.
>
> - **VUEMAgentSettings.xml:** This file includes some agent settings, you can view them in the **Advanced Settings - Configuration and UI Agent personalization** panel after importing the file.
> - **VUEMSystemMonitoringSettings.xml:** This file includes some system monitoring configuration settings, you can view them in the **Monitoring - Configuration** panel after importing the file.
> - **VUEMSystemUtilitiesSettings.xml:** This file includes some system optimization settings, you can view them in **System Optimization** - **CPU Management** and **Memory Management** after importing the file.
> - **VUEMEnvironmentalSettings.xml:** This file includes some environmental settings. You can view them in **Policies and Profiles** - **Environmental Settings** after importing the file.
> - **Sample Applications:** This file includes two WEM actions - Notepad and Calculator. You can view them in the **Actions** panel - **Actions > Applications** after importing the file.

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

Ribbon

September 7, 2025

The ribbon contains the following controls:

Configuration set. Switches from one Workspace Environment Management™ (WEM) site (configuration set) to another.

Create. Opens the **Create configuration set** window.

Name. Site name as it appears in the site list in the Ribbon.

Description. Site description as it appears in the site edition window.

Site State. Toggles whether the site is Enabled or Disabled. When Disabled, WEM agents cannot connect to the site.

Edit. Opens the **Edit configuration set** window, with similar options to the **Create configuration set** window.

Delete. Deletes the site. You cannot delete "Default site"because WEM relies on it to function. You can, however, rename it.

Refresh. Refreshes the site list. The list does not refresh automatically 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:
    - **AppLocker Rule Settings**
    - **Privilege Elevation Settings**
    - **Process Hierarchy Control 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:

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

- Users. Single users and user groups
- Machines. Single machines, machine groups, and OUs

> **Note:**
>
> You can name your backup copy, but you cannot specify the location where the backup copy is saved. The backup copy is automatically saved to a default folder in Citrix Cloud.

- **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
  - Scripted task settings
  - 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 backup copy from the drop-down list. Select a Citrix Cloud folder containing the backup. You can also restore settings from a backup file.

- **Actions**. Restores selected WEM actions.
- **Settings**. Restores selected WEM settings.
- **Security Settings**. Restores all settings present on the Security tab. The settings in 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**
    - **Overwrite Existing Settings**. Controls whether to overwrite existing privilege elevation settings when there are conflicts.
  - **Process Hierarchy Control Settings**

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

- **Overwrite Existing Settings**. Controls whether to overwrite existing process hierarchy control 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. However, user store credentials are *added* to or *replace* existing user store credentials.
> - Restored AD objects are *added* to or *replace* existing site AD objects, depending on whether you select **Overwrite mode** in the AD objects page of the **Restore** wizard.
> - If you select **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.

> **Important:**
>
> - The **Migrate** wizard migrates only the settings (GPOs) that WEM supports.
> - Citrix® recommends that you back up your existing settings before you start the migration process.

Citrix recommends that you perform the following steps to back up your GPOs:

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

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, 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. After that completes successfully, click **Migrate**. On the **File to Migrate** page, select the applicable file from the list. You can also type the name of the file and then click **Find** to locate it.

- **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.

Quick Start. Opens the quick-start page that provides information necessary for you to get started with the WEM service. Follow the on-screen instructions to start configuring your WEM deployment.

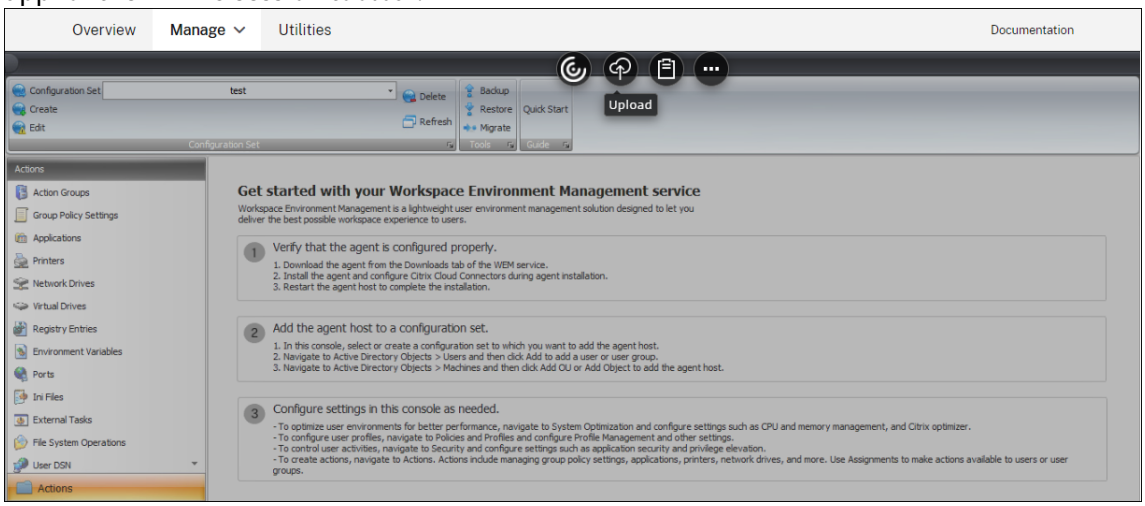
Restore settings from a backup file

> **Warning:**
>
> When you restore settings, the current settings in your Workspace Environment Management service are overwritten.

The on-premises Workspace Environment Management Backup wizard backs up the current configuration set to a special XML format file. You can restore (apply) the settings in the file to the current configuration set in your Workspace Environment Management service, using the following steps:

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

1. In the Workspace Environment Management service **Manage** tab, open the Citrix Workspace™ app for the HTML5 session toolbar.



2. Use **Upload** to upload the XML backup file to a Citrix Cloud folder. The default folder is *Default-UploadFolder*.
3. Use the Workspace Environment Management service Restore wizard to restore from the Citrix Cloud folder.

Actions

September 7, 2025

Workspace Environment Management™ service 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 service also provides you with filters to contextualize your assignments.

- Actions include managing:
  - Action Groups
  - Group Policy Settings
  - Applications
  - Printers
  - Network Drives
  - Virtual Drives
  - Registry Entries
  - Environment Variables

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

    - Ports
    - Ini Files
    - External Tasks
    - File System Operations
    - User DSN
    - File Associations
- Filters
- Assignments

Action Groups

November 28, 2024

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.

> **Note:**
>
> - You can now view group actions with the new **assignment group** feature available in the web console, where you can find your existing action groups. The action groups you created and assigned before will still work, but they can no longer be edited or assigned in the legacy console. To avoid assignment conflicts and take advantage of the new enhancements, we recommend that you unassign the action groups in the legacy console and manage them in the web console.
> - 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.

Actions

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

> **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.

> **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.

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

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.

> **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.

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

For more information about how assignments work, see Assignments.

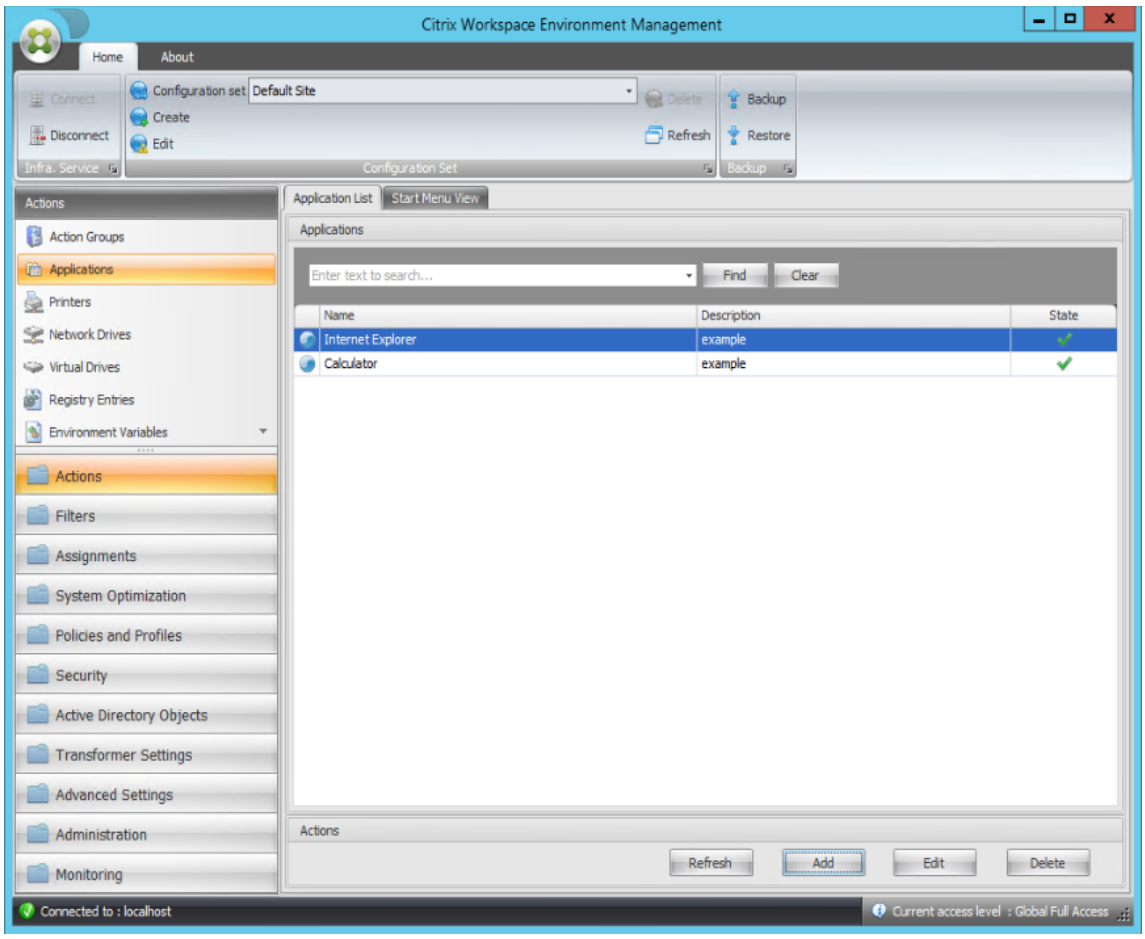
When assigning action groups, there are several scenarios to be aware of:

- 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 were processed earlier, resulting in the actions processed later being unassigned. The other actions remain unchanged.

Example scenario

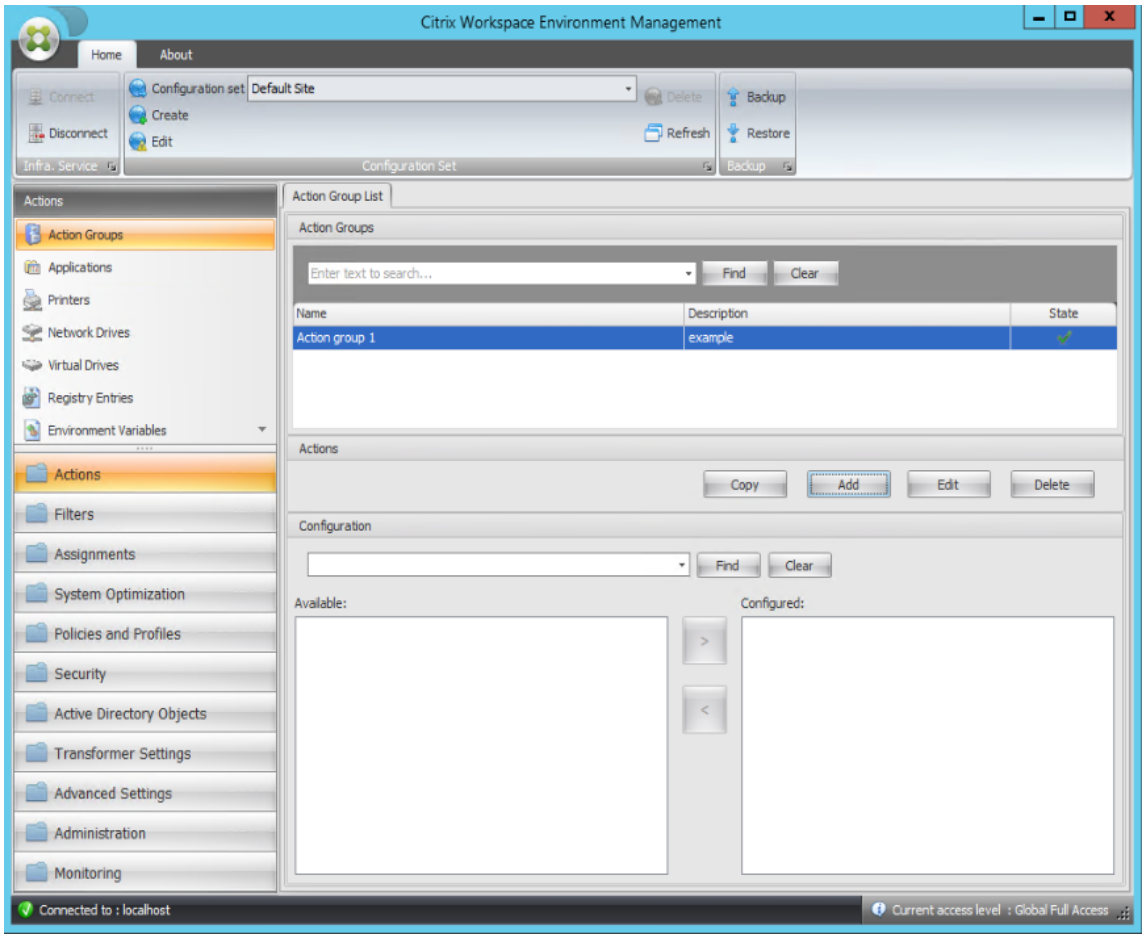
For example, to use the action groups feature to assign two applications (iexplore.exe and calc.exe) to a user at one time, follow the steps below.

1. Go to the **Administration Console > Actions > Applications > Application List** tab and then add the applications (iexplore.exe and calc.exe).



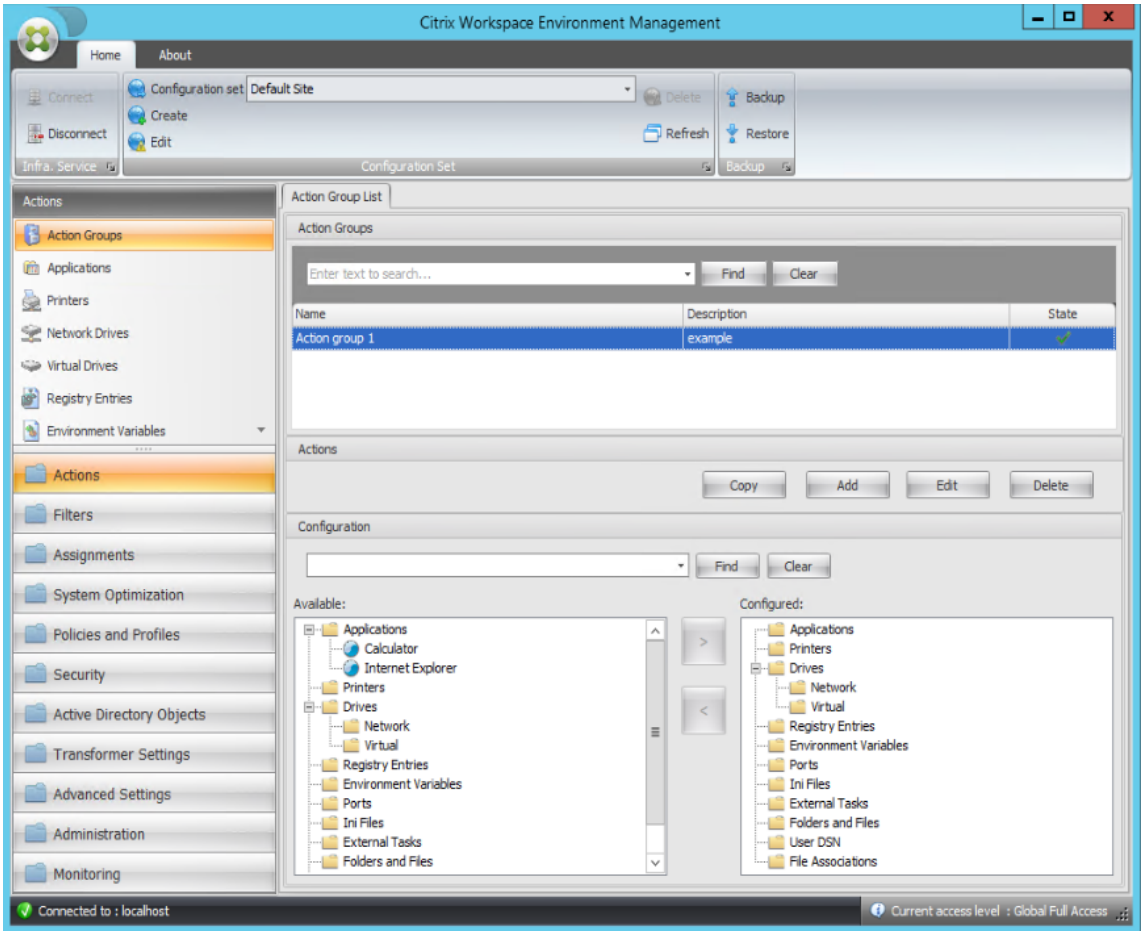
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Go to the **Administration Console > Actions > Action Groups > Action Group List** tab and then click **Add** to create an action group.



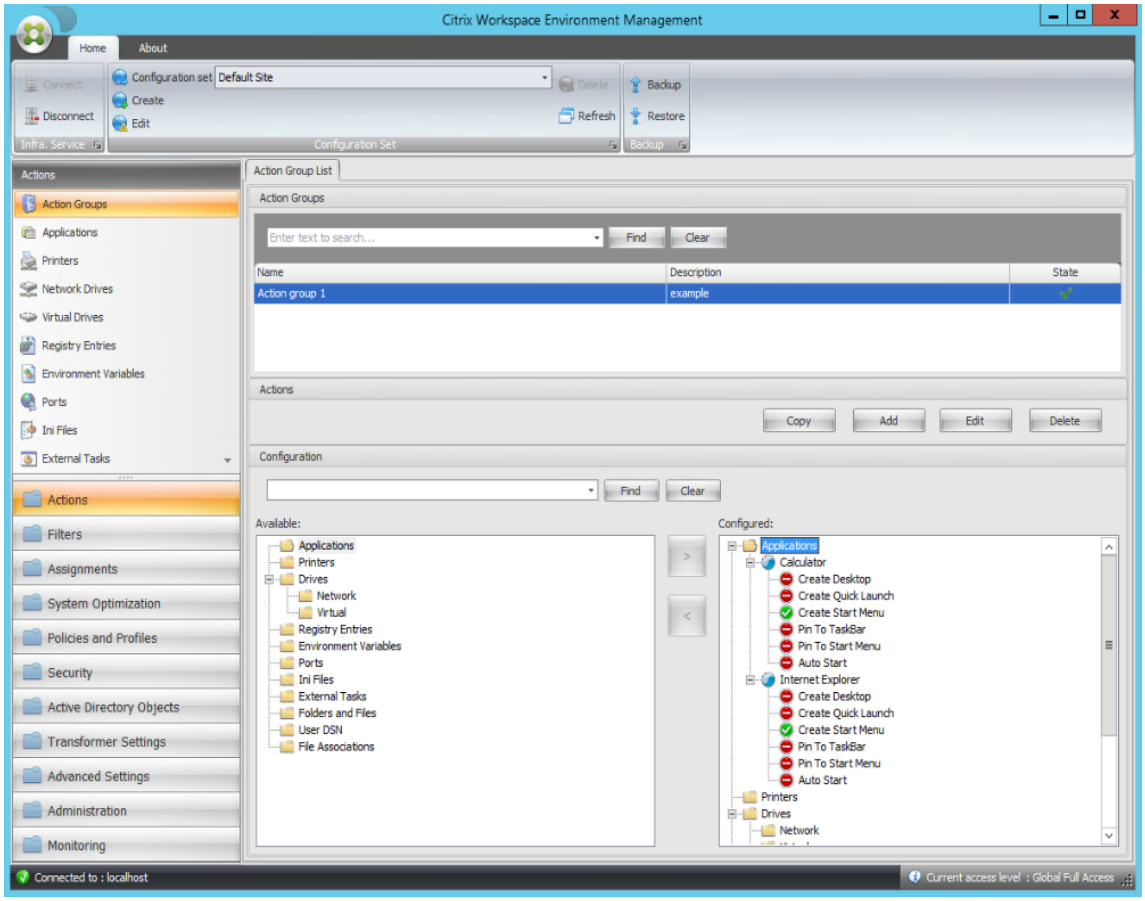
3. On the **Action Group List** tab, double-click the action group you created to display the action list in the **Available** and **Configured** panes.

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



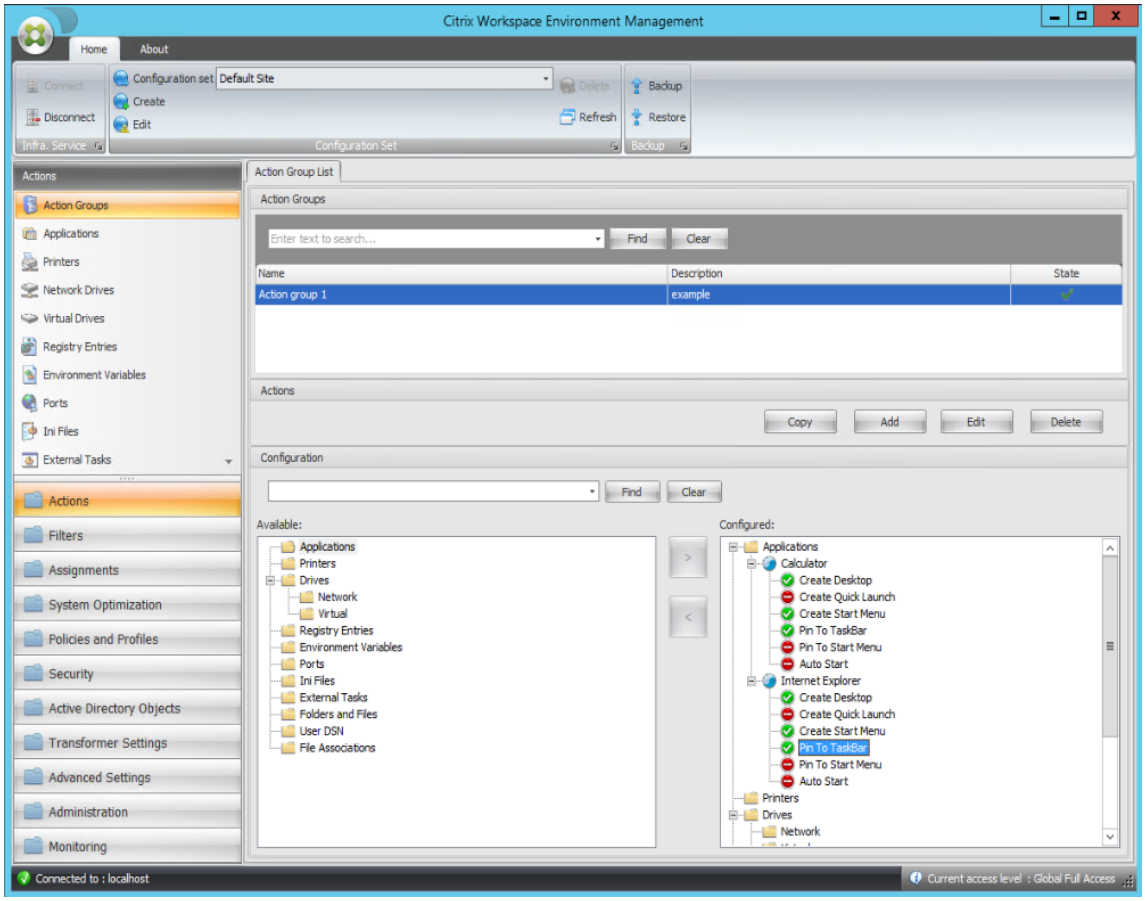
4. In the **Available** pane, double-click each application to move it to the **Configured** pane. You can also do so by selecting the application and then clicking the right arrow.

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



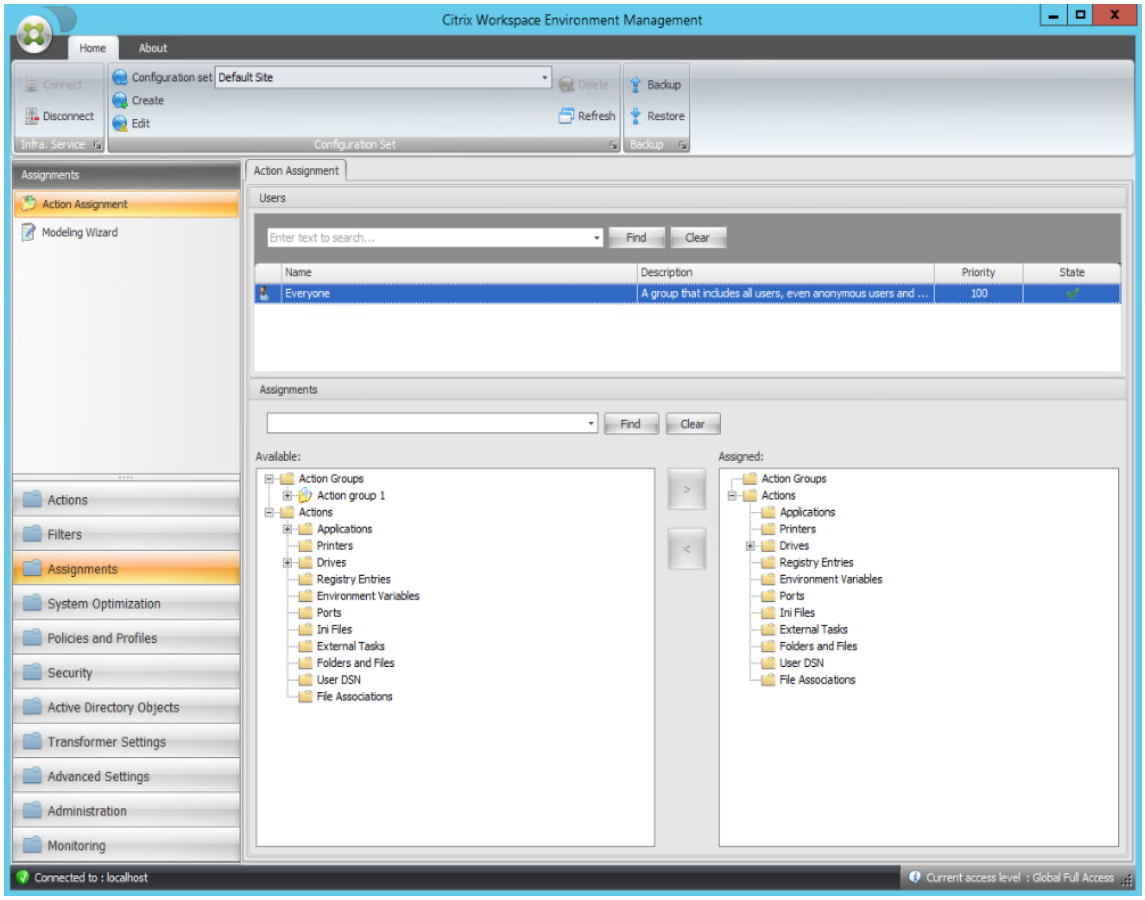
5. In the **Configured** pane, configure the options for each application. In this example, enable **Create Desktop** and **Pin To TaskBar**.

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



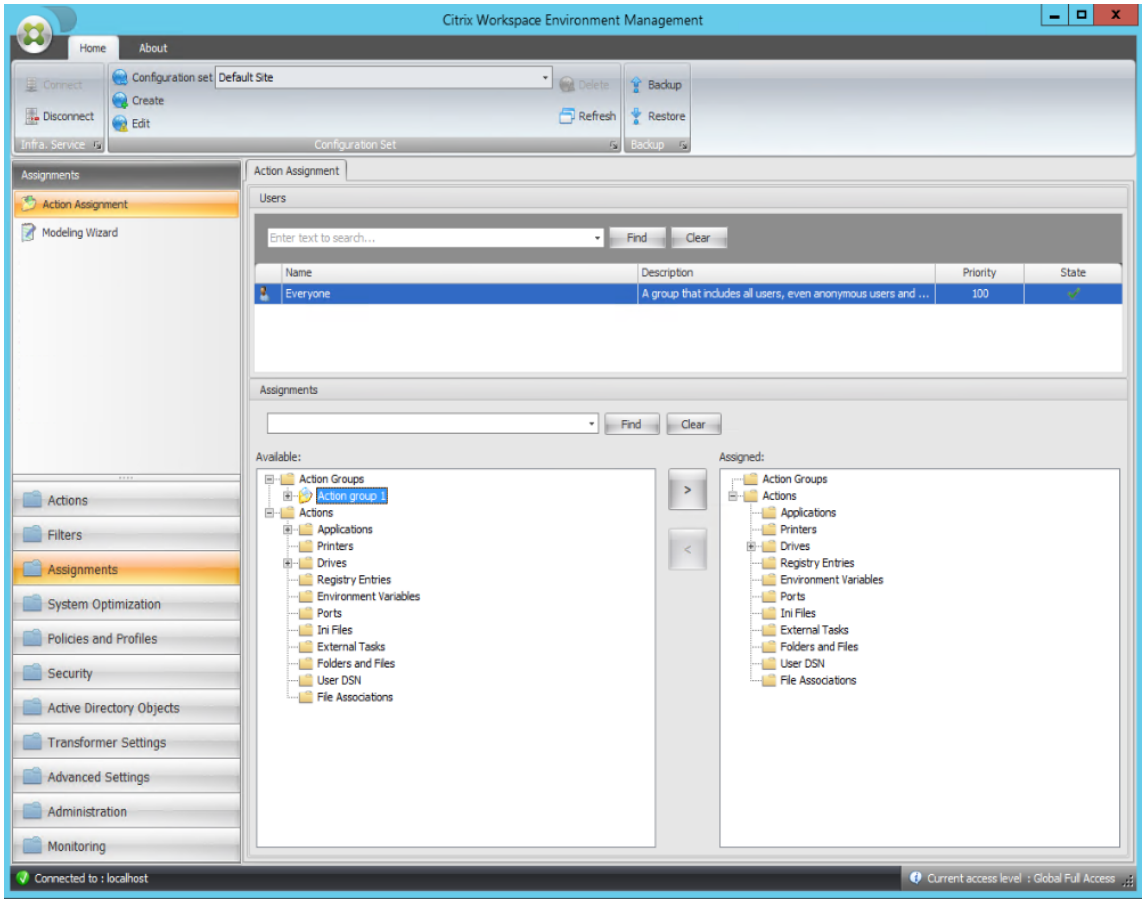
6. Go to the **Administration Console > Assignments > Action Assignment** tab and then double-click the applicable user to display the action group in the **Available** and **Assigned** panes.

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



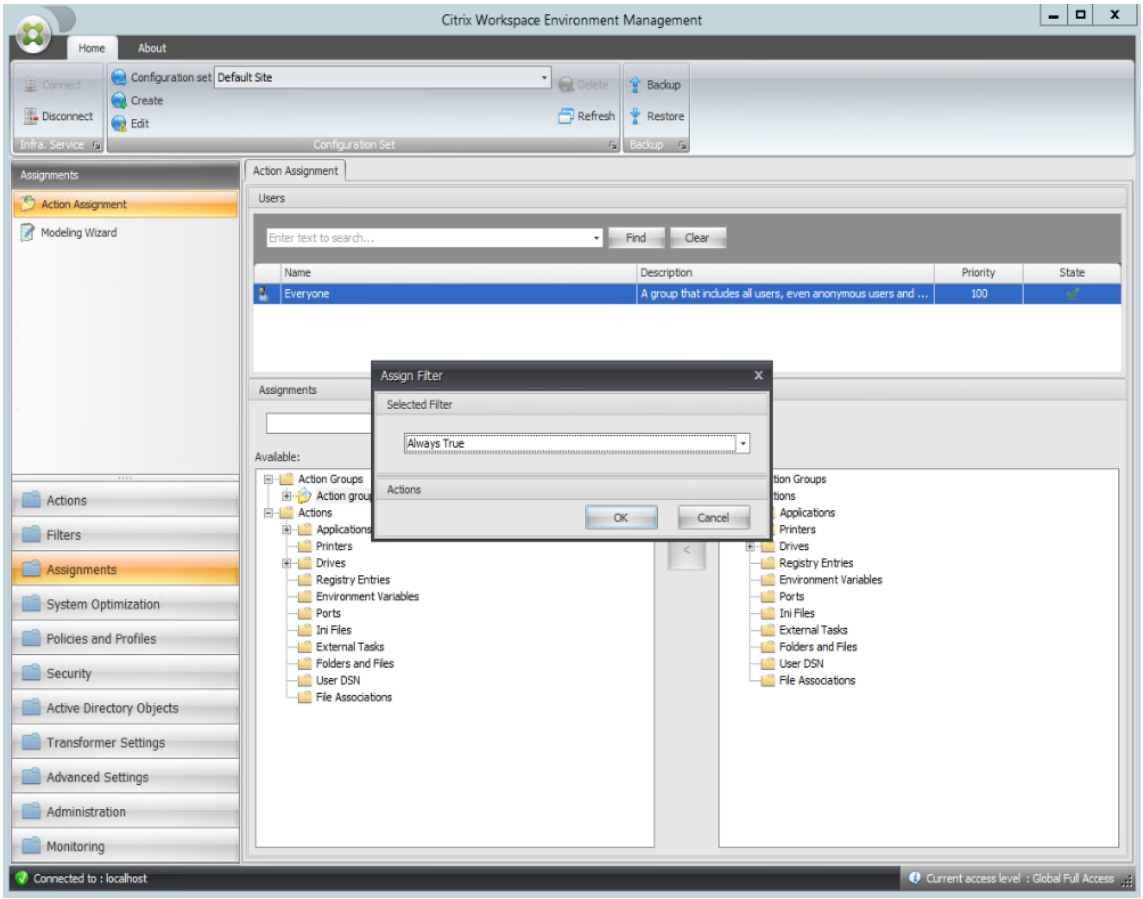
7. In the **Available** pane, double-click the action group you created (in this example, Action group 1) to move it to the **Assigned** pane. You can also do so by selecting the action group and then clicking the right arrow.

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



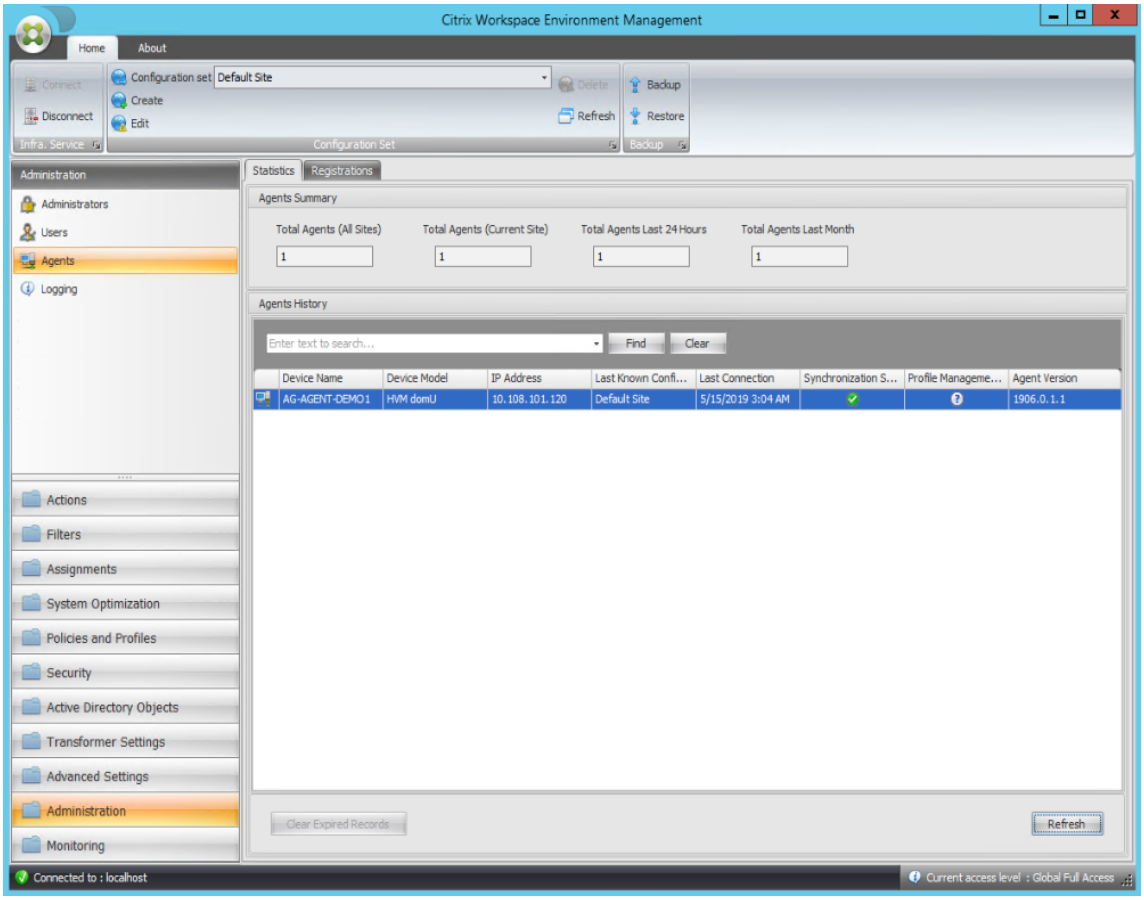
8. In the **Assign Filter** window, select **Always True** and then click **OK**.

© 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

May 8, 2024

> **Important:**
>
> WEM service 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.

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

You can now also import Group Policy settings (registry-based settings) into WEM.

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.

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.

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

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:

- 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.

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

Before you start, be aware of the following:

- Import from a zip file. The zip file can contain one or more registry files. Make sure that the size of the unzipped files 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. Use Upload to upload the zip backup of your registry files to the default folder in Citrix Cloud.
2. Go to **Legacy Console > Actions > Group Policy Settings**, select **Enable Group Policy Settings Processing**, click the down arrow next to **Import**, and select **Import Registry File**.
3. In the wizard that appears, select the file from the list. You can also type the name of the file and then click **Find** to locate it.
    - **Overwrite existing GPOs**. Controls whether to overwrite existing GPOs when conflicts occur.
4. Click **Start Import** to start the import process.
5. 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.

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.

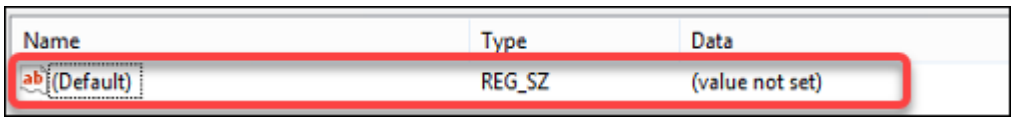
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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.
- **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.

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

  - **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.

- **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.

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.

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

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.
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.

Applications

September 7, 2025

Controls the creation of application shortcuts.

> **Tip:**
>
> - You can use the Full Configuration management interface 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 (formerly Citrix Virtual Apps and Desktops service) 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 use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Application list

Displays a list of your existing application resources. You can use **Find** to filter the list by name or ID.

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

1. Go to the **Administration Console > Actions > Applications > Application List** tab, click **Add**. Alternatively, right-click the blank area and then select **Add** in the context menu. The **New Application** window appears.
    a) On the **General** tab, type the required information and select an application type as needed.
    b) On the **Options** tab, add an icon for the application and configure settings as needed.
    c) On the **Advanced Settings** tab, configure more options for the application.
    d) Click **OK** to save changes and to exit the **New Application** 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 application.
    b) Select the application and click the right arrow (>) to assign it.
    c) In the **Assign Filter** window, select **Always True** and then click **OK**. The application moves from the **Available** pane to the **Assigned** pane.

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

d) In the **Assigned** pane, configure one or more of the following options for the application: **Create Desktop**, **Create Quick Launch**, **Create Start Menu**, **Pin To TaskBar**, **Pin To Start Menu**, and **Auto Start**.

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.

The General tab

Name. The display name of the application shortcut, as it appears in the application list.

Description. Lets you specify additional information about the application.

Application Type. The type of application the shortcut opens. The user interface differs depending on your selection.

- **Installed application**. Lets you create a shortcut that opens an application installed on the user's machine. If selected, prompts you to complete the following:
  - **Command Line**. Type the full path of the application that resides on the user's machine. Click **Browse** to see the listed applications and to understand the file path format.
  - **Working Directory**. 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 **Command Line** field.
  - **Parameters**. Type launch parameters for the application if needed.
- **File/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:
  - **Target**. Type the full path to the target file or folder.

  > **Note:**
  >
  > While using a non-domain-joined agent, **Application Type** such as, **File/Folder** in WEM might not work, if the **Target** is a network share.

- **URL.** Lets you add the URL of an application. If selected, prompts you to complete the following:
  - **Shortcut URL**. Type the URL of an application.

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

- **StoreFront™ store**. Lets you add an application that is based on a StoreFront store. If selected, prompts you to complete the following:
  - **Store URL**. Type the URL of a StoreFront store containing the resource you want to start from the shortcut.
  - **Store Resource**. Add the resource (available from the StoreFront store) that you want to start from the shortcut. Click **Browse** to browse and select the resource.

> **Tip:**
>
> To add an application 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. Lets you specify where to create the application shortcut on the left side of the Start menu. By default, a new shortcut is created in **Programs**. To create a custom folder for a shortcut, perform these steps:

1. Click **Select path** to open the **Start Menu Path Selection** window.
2. In that window, right-click **Programs** and click **Add** from the context menu. The **Create New Start Menu Folder** window appears.
3. In that window, specify a folder name, click **OK**.
4. Click **Select** to exit the **Start Menu Path Selection** window.

The Options tab

Icon File. Lets you add an icon for the application. Click **Select Icon** to type the full path for the icon file you uploaded, select the path from the list, and then click **Load**. For more information, see To select an icon. Icons are stored in the database as strings.

- **High Resolution Icons Only**. Displays only high-definition icons in the list.

Icon Index. This field automatically populates.

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 enabled, prevents users from running the application shortcut. The shortcut icon contains a warning sign to indicate that the shortcut is unavailable. If users click

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

the shortcut, a message appears, notifying them that the application is unavailable. This option lets you proactively manage scenarios where published applications are in maintenance without disabling or deleting those application shortcuts.



Display Name. The name of the shortcut, as it appears in the user environment.

Hotkey. Lets you specify a hotkey for the user to launch the application with. Hotkeys are case sensitive and typed in the following format (for example): `Ctrl + Alt + S`.

Action Type. Describes what type of action this resource is.

The Advanced Settings tab

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. Lets you 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 the user's machine.

Do Not Show in Self-Services. Hides the application from the agent menu (self-service interface) accessible from the user's machine. Users open the agent menu by right-clicking the agent icon in the taskbar when the session agent is running in UI mode. If selected, hides the application from both the **My Applications** menu and the **Manage Applications** dialog.

> **Tip:**
>
> The **Enable Application Shortcuts** option controls whether the **My Applications** option is available in the agent menu. The option is available from the **Administration Console > Advanced Settings > UI Agent Personalization > UI Agent Options** tab. For more information, see UI Agent Personalization.

Create Shortcut in User Favorites Folder. Creates an application shortcut in the user's **Favorites** folder.

Start menu view

Displays a tree view of your application shortcut resource locations in the Start menu.

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

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.

Application launcher

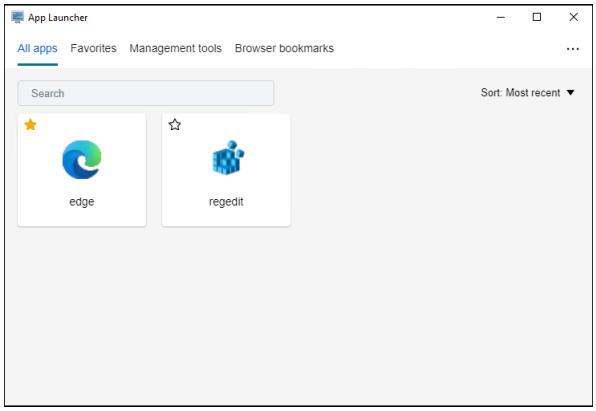
Application launcher aggregates all applications you assigned to your users through the administration console. Using the tool, users can launch all assigned applications in one place.

> **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:



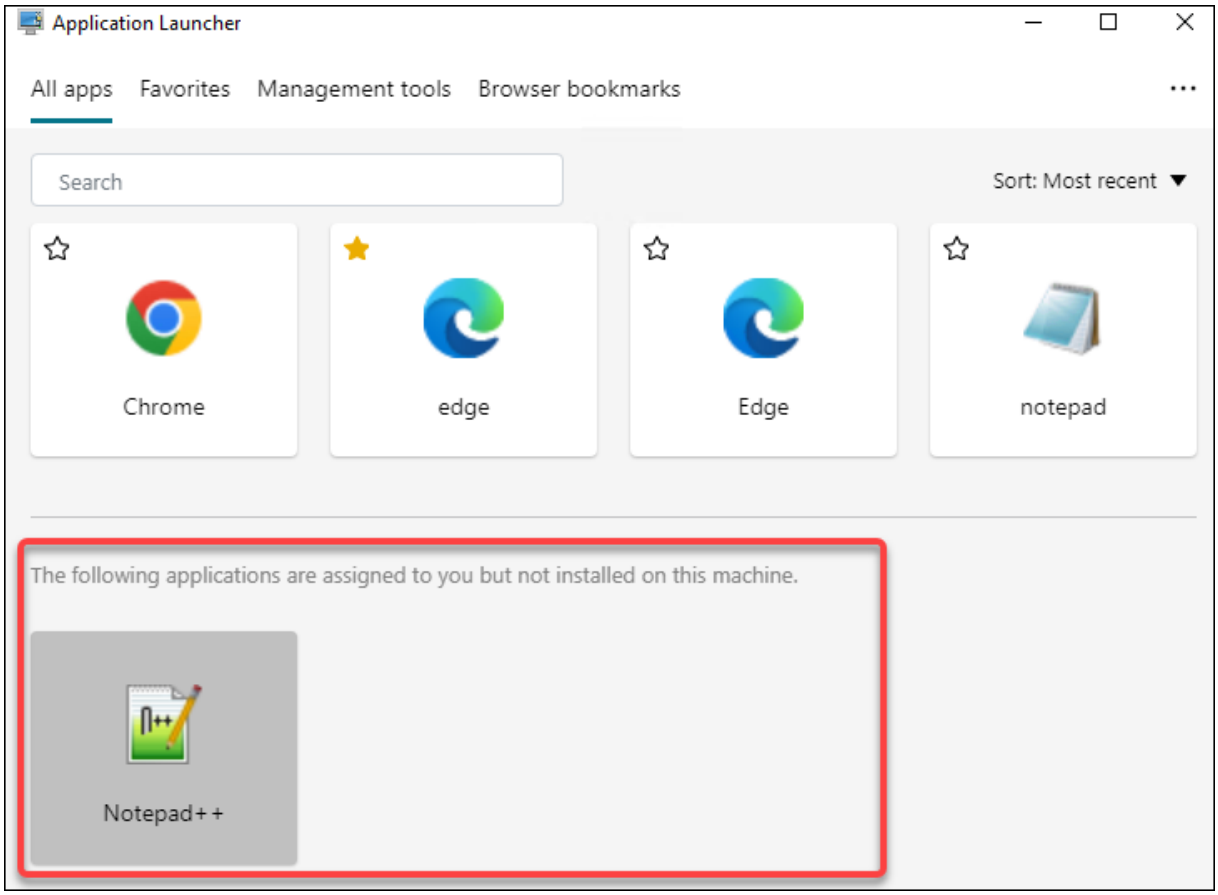
- **All apps**. Shows all assigned applications. Available sorting options: **Most recent**, **A-Z**, and **Z-A**.
- **Favorites**. Shows applications marked as favorites.
- **Management tools**. Shows the following two tools:
  - **Taskmgr**. Opens Task Manager.

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

  - **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.



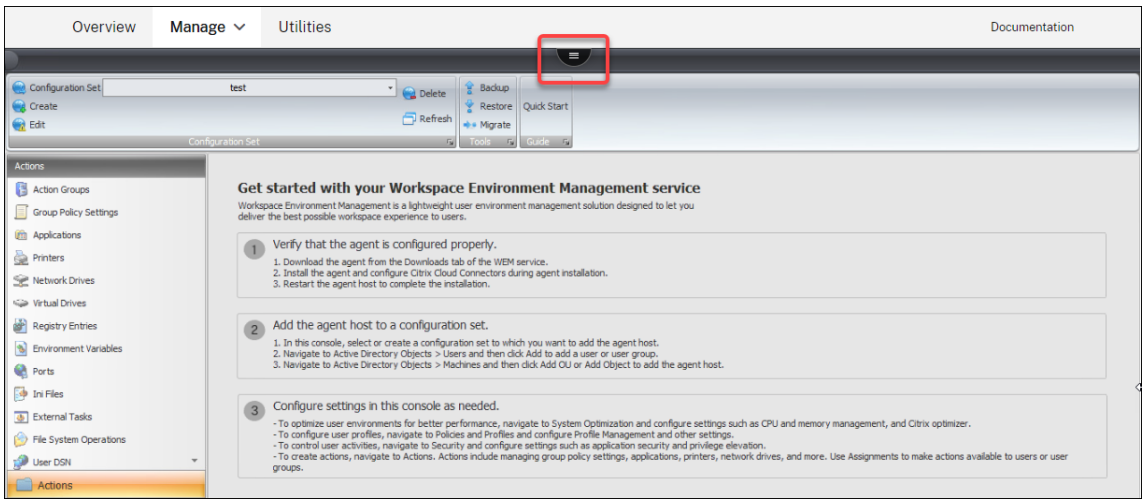
For an example of how to use this feature, see Aggregate assigned applications in one place.

To select an icon

To select an icon, complete the following steps:

1. Hover the mouse cursor over the menu on the **Manage** tab of the WEM service.

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



2. Click the Citrix Workspace icon.
3. Click the upload icon to upload the applicable icon file to a Citrix Cloud™ folder.

> **Note:**
>
> We do not retain the icon file for later use. We might delete the file when the file count limit is reached. If necessary, save a local copy of the file. For more information about the file count limit, see Upload files.

4. On the **Administration Console > Actions > Applications > Application List** tab, click **Add**.
5. In the New Application window, go to the **Options** tab and then click **Select Icon**.
6. In the **Icon Selector** window, type the full file path for the icon file you uploaded, select the path from the drop-down list, and then click **Load**. The default folder path is `C:\DefaultUploadFolder\`. You must type the full file path in the following format: `C:\DefaultUploadFolder\iconname`. For example:

   - `C:\DefaultUploadFolder\iconname.ico`
   - `C:\DefaultUploadFolder\iconname.exe`

7. In the **Icon Selector** window, select the applicable icon and then click **OK**.

Editing application settings using the Full Configuration management interface

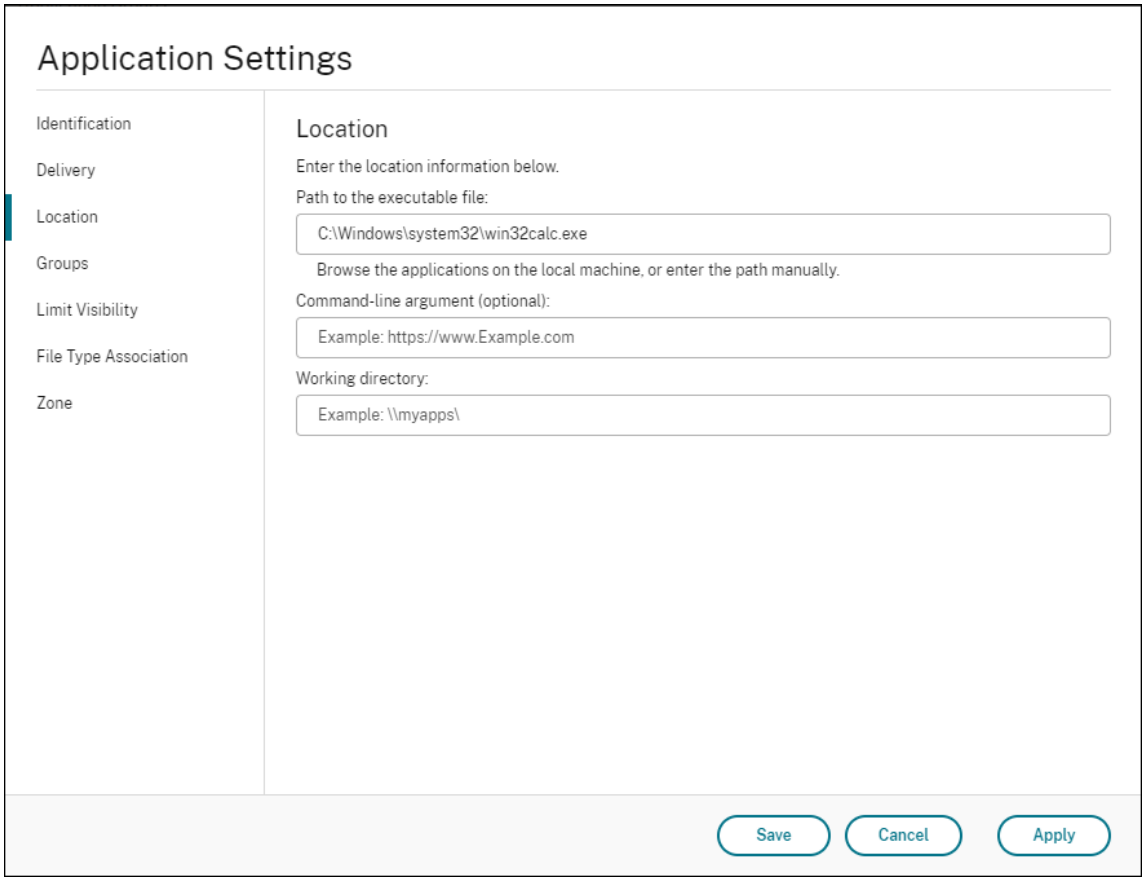
Workspace Environment Management (WEM) provides you with client-side tools to troubleshoot issues you experience. The VUEMAppCMD tool (**VUEMAppCmd.exe**) ensures that the WEM agent finishes processing an environment before published applications are started. It is located in the agent installation folder: `%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 the Full Configuration management interface 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. On the **Application** node, select the application, click **Properties** in the action bar, and then go to the **Location** page.



2. In the **Path to the executable file** field, type the path for `VUEMAppCmd.exe`.
   - Type the following: `%ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMAppCmd.exe`.
3. Type the path for the application to be launched in 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%\Internet Explorer\iexplore.exe"`.

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

Printers

July 5, 2022

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 existing printer resources, with unique IDs. You can use **Find** to filter your printers list by name or ID.

> **Note:**
>
> - The WEM service currently does not support importing printers using **Import Network Print Server** on the ribbon.
> - After Windows Update installs KB5005033 on an agent machine, assigned printers do not work. The issue occurs because the update prevents the automatic start of the Windows Print Spooler service. As a workaround, start the service manually.

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.

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

Self-Healing. Toggles whether the printer is automatically recreated for users when the agent refreshes.

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.

Network Drives

July 5, 2022

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.

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.

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

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

December 5, 2023

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.
    c) In the **Assign Filter & Driver Letter** window, select **Always True**, select a driver letter, and then click **OK**. (Select the asterisk (*) character instead of a specific letter if you want to assign the next available drive letter to the virtual drive.) The virtual drive moves from the **Available** pane to the **Assigned** pane.

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

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.

> **Note:**
>
> While using a non-domain-joined agent, WEM might not work if the **Target Path** is a network share.

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

September 7, 2025

Controls the creation of registry entries.

> **Tip:**
>
> You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

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

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.

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 as it appears 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`.

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

- 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 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. Use Upload to upload the registry file you want to import. The file appears in the default folder in Citrix Cloud.
2. Go to **Legacy Console > Actions > Registry Entries**.
3. In the ribbon, click **Import Registry File**.
4. In the **Import from Registry File** window, select the desired registry file from the list. You can also start typing the file name and then click **Find** to locate it.
5. Click **Scan** to start scanning the registry file. After the scan completes successfully, a list of registry settings appears.
6. Select the registry settings that you want to import and then click **Import Selected** to start the import process.
7. 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 those entries for import. If you want to import the others, rename them.

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

Environment Variables

November 16, 2022

Controls the creation of environment variables.

> **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

January 14, 2022

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

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.

> **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.

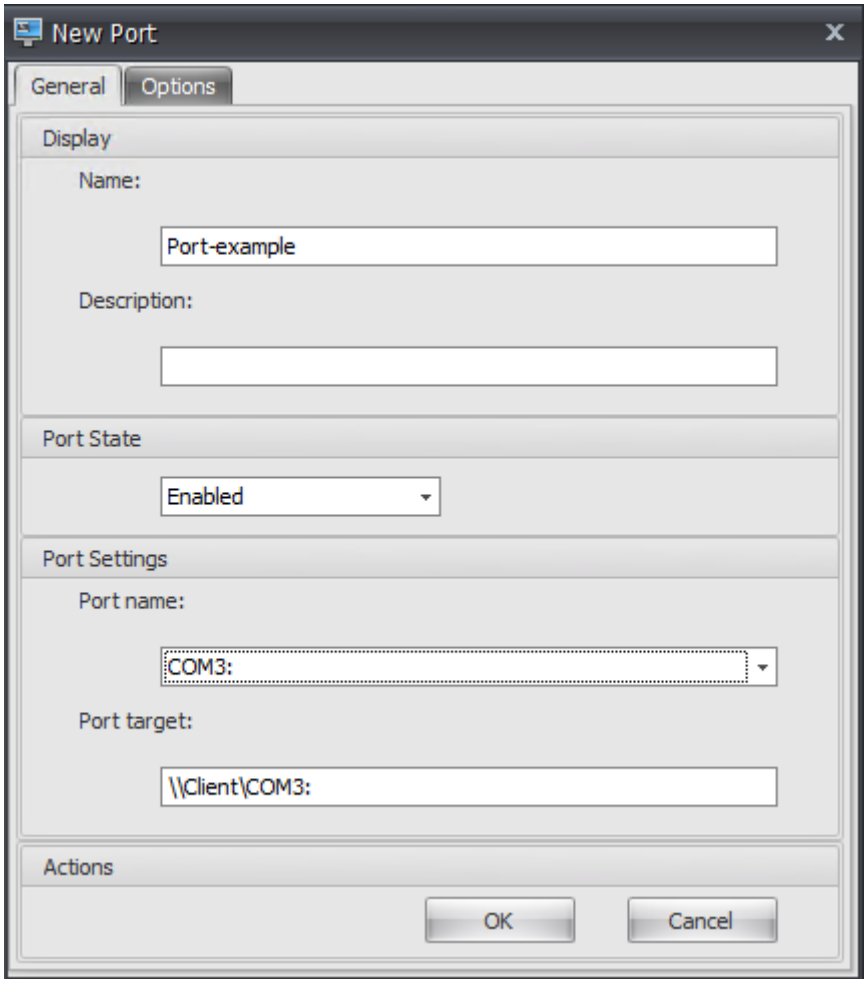
Port Target. The target port.

Options tab **Action Type**. Describes what type of action this resource performs.

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

September 7, 2025

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.

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

To add an .ini file operation

1. Use the context menu **Add** command.
2. Enter details in the **New Ini Files Operation** dialog tab, then 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.

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 perform the operation 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.

External Tasks

December 5, 2023

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.

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

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.

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.
- 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.

> **Note:**
>
> While using a non-domain-joined agent, WEM might not work if network share is used in **Path** or **Arguments**.

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.

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

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.

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.
- **Disconnect**. Controls whether to run the external task when a user disconnects from a machine on which 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 on which 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 on which 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.

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

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.

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.

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

- 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

September 7, 2025

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.

To add a file system operation

1. Use the context menu **Add** command.
2. Enter details in the **New File System Operation** dialog tab, 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.

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

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.

> **Note:**
>
> While using a non-domain-joined agent, WEM might not work if network share is used in **Source Path** or **Target Path**.

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.

User DSN

September 7, 2025

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.

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

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.

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

September 7, 2025

> **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**

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

> **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.

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:

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

- 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.

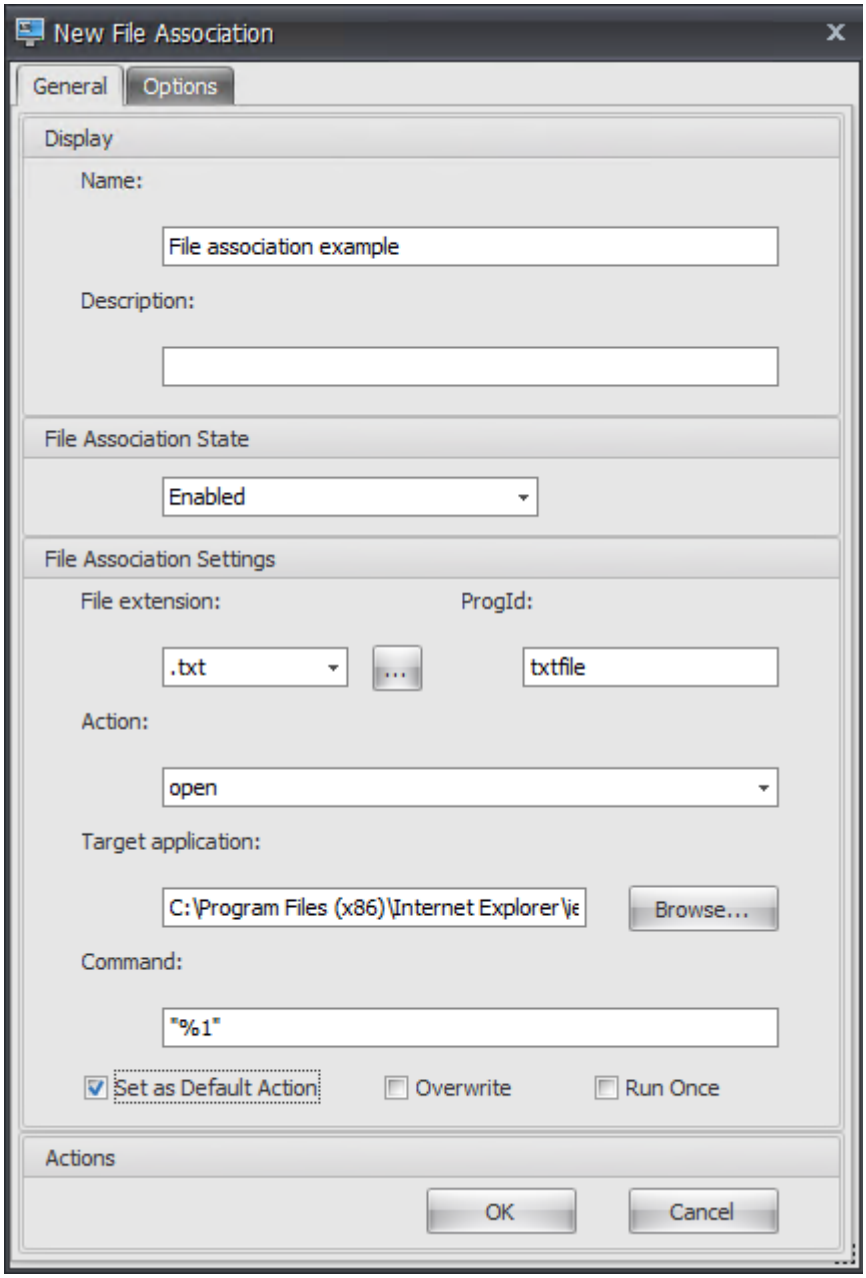
Run Once. By default, Workspace Environment Management™ (WEM) creates a file association every time the agent refreshes. Select this option to create the file association once, rather than on every refresh. This speeds up the agent refresh process, especially if you have many file associations assigned 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.

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**.

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



- **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.
- Select **Set as Default Action**.

3. Go to the **Administration Console > Assignments > Action Assignment** tab.

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

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

> **Note:**
>
> - To ensure that browser association for Google Chrome works, verify that the browser on the agent host is installed by an administrator. Otherwise, log on to the machine as an administrator and reinstall the browser. This is necessary because if the browser is installed by a user (non-administrator) the ProgID is `ChromeHTML.<X>` rather than `ChromeHTML`. "X"denotes the Globally Unique Identifier (GUID) specific to the user, for

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

> example `JLKDKPPE7UYB4JTWJS73YQWTD4`.
> - Browser association for Microsoft Edge works only with the built-in, default instance of Microsoft Edge included in your particular version of the Windows 10 operating system. If you upgrade the browser to a more recent version, the configured association does not take effect. For a workaround, see Knowledge Center article CTX269675.

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.

More information

For an example of how to configure file type associations, see Configure file type associations.

Filters

January 14, 2022

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.

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

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

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 should be included in both ends of the range, e.g.: 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.

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

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.

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 (e.g. **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**.

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

Assignments

November 16, 2022

> **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 Filters.
> - Define filter rules, see Filters.
> - Configure actions, see this article.

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.

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

> **Note:**
>
> WEM supports automatically assigning the next available drive letter to a network drive. When assigning a network drive, select the asterisk (*) character in the **Assign Filter & Drive Letter** window to let WEM automatically assign the next available drive letter (whatever drive letter available) to that network drive.

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**, use the **Enable** and **Disable** context actions to fine-tune the behavior of the assignment.

> **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.

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

System Optimization

September 7, 2025

Workspace Environment Management™ system optimization consists of the following:

- CPU Management
- Memory Management
- I/O Management
- Fast Logoff
- Citrix Optimizer
- Multi-session Optimization

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 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

September 7, 2025

These 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.

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

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 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 **Limit CPU Core Usage** to 4 (half of the VM's logical processors), not to 48 (half of the physical machine's logical processors).

Enable CPU Spike Protection. 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 **Limit Sample Time** field).

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

- **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 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 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 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%.
  - **Limit Sample Time**. 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 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 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.

- **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.

© 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 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, looks for "**Initializing process limitation thread for process**".

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

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

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.

   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**.

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

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).

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.

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

Memory Management

September 7, 2025

These settings let you optimize application memory usage through Workspace Environment Management™ (WEM).

Memory management

If these settings are turned on, 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.

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`

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

- wfshell
- rdpclip
- wmiprvse
- 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

Enable Memory Usage Limit for Specific Processes. Lets you limit the RAM usage of a process by setting an upper limit for the RAM, the process can consume.

> **Warning:**
>
> Applying memory usage limits to certain processes might have unintended effects, including slow system responsiveness.

- **Add**. Allows you to add a process to which you want to apply a memory usage limit.
- **Remove**. Allows you to delete an existing item.
- **Edit**. Allows you to edit an existing item.
- **Dynamic Limit**. Allows you to apply a dynamic limit to the specified process. This setting dynamically limits the amount of RAM allocated to the specified process. If applied, enforces mem-

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

ory usage limits depending on the available memory. Therefore, the RAM that the specified process consumes might exceed the specified amount.

- **Static Limit**. Allows you to apply a static limit to the specified process. This setting always limits the amount of RAM 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 RAM 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**.

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

July 5, 2022

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.

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

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**.

Fast Logoff

September 7, 2025

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.

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

Citrix Optimizer

September 7, 2025

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.

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.

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

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**.
2. In the **New Custom Template** window, complete the following steps:
   a) For **Template Name**, click **Select an XML file** and then select the applicable file from the list.

   > **Note:**
   >
   > The list displays the XML files you uploaded. To upload an XML file, see To upload a custom template.

   b) For **Applicable OSs**, select the applicable OS from the list.
   c) For **Groups**, configure groups that the template contains.
   d) 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**.

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

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**.

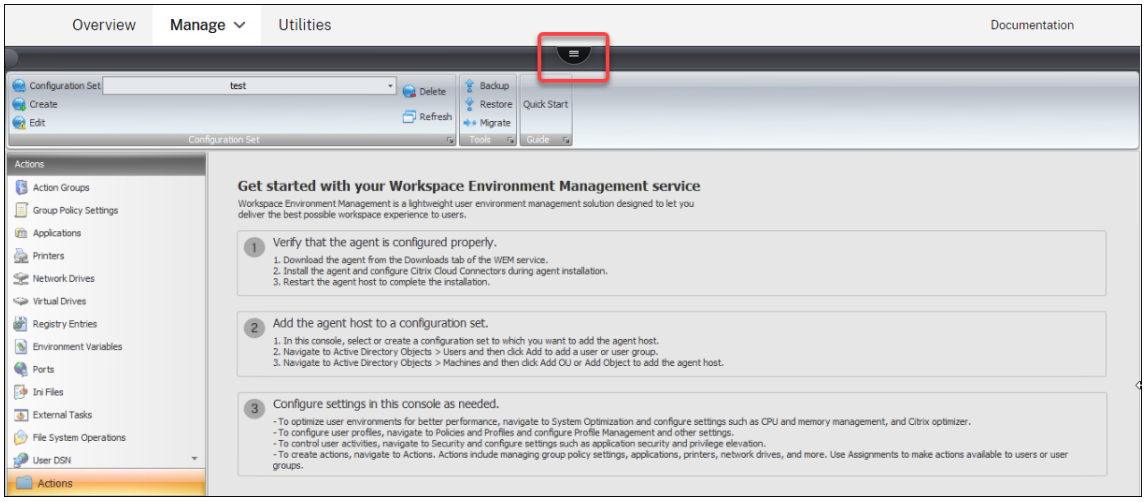
> **Tip:**
>
> New changes might fail to take effect immediately. We recommend that you select **Refresh Agent Host Settings** before you select **Process Citrix Optimizer**.

To upload a custom template

To upload a custom template, complete the following steps:

1. On the **Manage** tab, hover the mouse cursor over the hamburger menu.

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



2. Click the Citrix Workspace™ icon.
3. Click the upload icon to upload the custom template (XML file) to the default folder in Citrix Cloud.

Multi-session Optimization

January 14, 2022

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.

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

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

September 7, 2025

These settings let you replace user GPOs and configure user profiles.

- Environmental Settings
- Microsoft USV Settings
- Citrix Profile Management Settings

Environmental Settings

December 5, 2023

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.

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

> **Note:**
>
> While using a non-domain-joined agent, WEM might not work if you use a network share.

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.

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.

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

SBC/HVD tuning

User Environment: Advanced Tuning. These options allow you to optimize performance in SBC/HVD environments.

Microsoft USV Settings

September 7, 2025

These settings allow you to optimize Microsoft User State Virtualization (USV).

Roaming profiles configuration

These settings allow you to configure the integration of Workspace Environment Management™ 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 that it appears with in the user environment.

Roaming profiles advanced configuration

The following are 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.

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

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.

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.

Citrix Profile Management Settings

October 16, 2025

> **Note:**
>
> Some options work only with specific versions of Profile Management. Consult the Profile Management documentation for details.

Workspace Environment Management™ (WEM) service 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.

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

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.

   > **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.

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

Enable active write back on session lock and disconnection. With both this option and the **Enable active write back** option 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 settings

These options control Profile Management profile container settings.

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 for Profile Container. 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 for Profile Container. 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 File Exclusions for Profile Container. If enabled, Profile Management excludes the listed files from the profile container. Specify at least one file to exclude from the profile container.

Enable File Inclusions for Profile Container. 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 in combination with the **Enable Folder Exclusions for Profile Container** option. Specify at least one file to include in the profile container.

Enable Local Cache for Profile Container. If enabled, each local profile serves as a local cache of its profile container. If profile streaming is in use, locally cached files are created on demand. Otherwise, they are created during user logons. To use this setting, put an entire user profile in its profile container. This setting applies only to Citrix Profile Management profile containers.

> **Tip:**
>
> When adding files or folders, you can use wildcards. For more information, see Wildcard support.

Enable VHD disk compaction. If enabled, VHD disks are automatically compacted on user logoff when certain conditions are met. This option enables you to save the storage space consumed by profile container, OneDrive container, and mirror folder container.

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

Depending on your needs and the resources available, you can adjust the default VHD compaction settings and behavior using the **Set free space ratio to trigger VHD disk compaction**, **Set number of logoffs to trigger VHD disk compaction**, and **Disable defragmentation for VHD disk compaction** options in Advanced settings.

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.

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, 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.

Set number of retries when accessing locked files. Configures the number of times the Agent retries accessing locked files.

Set directory of the MFT cache file. Lets you specify the MFT cache file directory. This option has been *deprecated* and will be *removed* in the future.

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

Enable application profiler. If enabled, defines application-based profile handling. Only the settings defined in the definition file are synchronized. For more information about creating definition files, see Create a definition file.

Process Internet cookie files on logoff. If enabled, stale cookies are deleted at logoff.

Delete redirected folders. If enabled, deletes local copies of redirected folders.

Disable automatic configuration. If enabled, dynamic configuration is disabled.

Log off user if a problem is encountered. If enabled, users are logged off rather than switched to a temporary profile if a problem is encountered.

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).

Enable multi-session write-back for profile containers. If enabled, Profile Management saves changes in multi-session scenarios for both FSLogix Profile Container and Citrix Profile Management profile containers. If the same user launches multiple sessions on different machines, changes made in each session are synchronized and saved to the user's profile container disk.

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.

Disable defragmentation for VHD disk compaction. Applicable when Enable VHD disk compaction is enabled. Lets you specify whether to disable file defragmentation for VHD disk compaction.

When VHD disk compaction is enabled, the VHD disk file is first automatically defragmented using the Windows built-in `defrag` tool, and then compacted. VHD disk defragmentation produces better compaction results while disabling it can save system resources.

Set free space ratio to trigger VHD disk compaction. Applicable when Enable VHD disk compaction is enabled. Lets you specify the free space ratio to trigger VHD disk compaction. When the free space ratio exceeds the specified value on user logoff, disk compaction is triggered.

Free space ratio = (current VHD file size –required minimum VHD file size*) ÷ current VHD file size

* Obtained using the GetSupportedSize method of the `MSFT_Partition` class from the Microsoft Windows operating system.

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

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, disk compaction is triggered again.

Replicate user stores. If enabled, Profile Management replicates a user store to multiple paths on each logon and 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.

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 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 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 need to manually reindex the database when the search index database becomes corrupted.
- **Enable concurrent session support for Outlook search data roaming**. 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.

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.

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

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 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. This setting lets you exclude specific files containing a large amount of data that users do not need as part of their profile. The list is pre-populated with default Windows 7 exclusions, and can be pre-populated with default Windows XP exclusions instead.

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

Enable Folder Exclusions. If enabled, the listed folders are not included in a user's profile. This setting lets you exclude specific folders containing a large amount of data that users do not need as part of their profile. The list is pre-populated with default Windows 7 exclusions, and can be pre-populated with default Windows XP exclusions instead.

> **Tip:**
>
> When adding files or folders, you can use wildcards. For more information, see Wildcard support.

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.

> **Tip:**
>
> When adding files or folders, you can use wildcards. For more information, see Wildcard support.

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 exactly the same as the local versions. See below for more information about how folder mirroring works.

Accelerate folder mirroring. By default, Profile Management copies necessary transactional folders between the user store and local profiles. Mirroring ensures the integrity of those folders. This option eliminates the need to copy them by using a container-based solution, thus accelerating folder mirroring. Profile Management attaches the virtual disk during logons and detaches it during logoffs, eliminating the need to copy the folders between the user store and local profiles. 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.

- **Add folders to mirror**. By default, Profile Management copies necessary transactional folders between the user store and local profiles. A transactional folder is a folder containing interdependent files, where one file references other files. You can add more as needed.

Enable Large File Handling. If enabled, large files are redirected to the user store, thus eliminating the need to synchronize those files over the network.

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

> **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.

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.

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.

Cross-platform settings

These options control cross-platform settings.

Enable cross-platform settings. If disabled, none of the settings in this section are processed.

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.

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

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 option controls user access to files, folders, and registries. A typical use case is to apply rules to control user access to apps installed on machines —whether to make apps visible to relevant users.

Enable app access control. If enabled, Profile Management controls user access to items (such as files, folders, and registries) based on the rules you provide.

There are two ways you can create application rules:

- GUI-based tool - Citrix Environment Tool Hub > Rule Generator for App Access Control
- PowerShell tool –available with the Profile Management installation package

User store credentials

These options control user store credential settings.

Enable credential-based access to user store. If disabled, Profile Management impersonates the current user to access user stores. Therefore, make sure that the current user has permission to directly access the user stores. Disabling this setting prevents all settings on this tab from being processed. If enabled, Profile Management uses the specified user store credentials to access the user stores on behalf of the user. Enabling this setting allows you to put user stores in storage repositories (for example, Azure Files) that the current user has no permission to access.

> **Important:**
>
> Disabling this setting deletes all user store connections that the WEM agent previously established.

- **Add**. Lets you add credentials.
- **Edit**. Lets you edit existing credentials.
- **Remove**. Lets you delete existing credentials.

When adding or editing credentials, complete the following fields:

- **Server share**. Type a UNC path that specifies a server share.
- **User name**. Type the name in the form domain\username.
- **Password**. Type 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.

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.

> **Tip:**
>
> When adding files or folders, you can use wildcards. For more information, see Wildcard support.

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.

Security

September 12, 2025

These settings let you control user activities within Workspace Environment Management™ (WEM).

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

Application security

> **Important:**
>
> To control which applications users can run, use the Windows AppLocker interface or WEM to manage Windows AppLocker rules. You can switch between these approaches at any time. We recommend that you do not use both approaches at the same time.

These settings let you control the applications that users are permitted to run by defining rules. This functionality is similar to Windows AppLocker. When you use WEM to manage Windows AppLocker rules, the agent 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. 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 WEM configuration set. 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:

- **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 convert rules into AppLocker rules. (In this case, AppLocker rules are not updated.)

  > **Note:**
  >
  > This option is not available if the WEM administration console is installed on Windows 7 SP1 or Windows Server 2008 R2 SP1 (or earlier versions).

- **Process DLL Rules**. When selected, the agent converts DLL rules in the current configuration set into AppLocker DLL rules on the agent host. This option is available only 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:**

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

> If you use DLL rules, users might experience sluggish performance. This issue happens because AppLocker checks each DLL that an app loads before the app 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 that include files with the .exe and .com extensions associated with an application.
- **Windows Rules**. Rules that include installer file formats (.msi, .msp, .mst) controlling the installation of files on client computers and servers.
- **Script Rules**. Rules that include files of the following formats: .ps1, .bat, .cmd, .vbs, .js.
- **Packaged Rules**. Rules that 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. WEM supports only publisher rules for packaged apps.
- **DLL Rules**. Rules that include files of the following formats: .dll, .ocx.

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 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.

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

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, 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.
5. In the **Permissions** section, select **Allow** or **Deny**. The selection controls whether to allow or prohibit applications from running.
6. To assign this rule to users or user groups, in the **Assignments** pane, choose users or groups to which you want to assign this rule. 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 WEM Users list.
   > - You can assign rules after the rule is created.

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

7. Click **Next**.
8. Specify the criteria the rule matches, depending on the rule type you choose:
    - **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.
9. Click **Next**.
10. Add any exceptions you require (optional). In **Add exception**, choose an exception type and then click **Add**. (You can edit or remove exceptions if needed.)
11. To save the rule, click **Create**.

To assign rules to users

Select one or more rules in the list and 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 and 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 apply to all users and user groups you select. In other words, existing rule assignments are merged across those rules.

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 and then click **Edit** in the toolbar or context menu. The editor appears, letting you adjust settings that apply to the selection you made.

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

To delete rules

Select one or more rules in the list and 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:
    - **Yes**. Restores rules and reassigns them to the same users and user groups in your current configuration set.
    - **No**. Restores rules and leaves them unassigned.
6. To start restoring, click **Restore Settings**.

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

Process management

These settings let you whitelist or blacklist specific processes.

Process management

Enable Process Management. This option toggles whether process whitelists and blacklists are in effect. If disabled, none of the settings on the **Process BlackList** and **Process WhiteList** tabs take effect.

> **Note:**
>
> This option works only if the agent is running in the user's session. To enable the agent to run in the session, use the **Advanced Settings > configuration > Main Configuration** tab to enable the **Launch Agent** options (**at Logon** / **at Reconnect** / **for Admins**) and set **Agent Type** to **UI**. These options are described in Advanced Settings.

Process blackList

These settings let you blacklist specific processes.

Enable Process Blacklist. This option enables process blacklisting. Add processes by using their executable names (for example, cmd.exe).

Exclude Local Administrators. Excludes local administrator accounts from the process blacklist.

Exclude Specified Groups. Lets you exclude specific user groups from the process blacklist.

Process whiteList

These settings let you whitelist specific processes. Process blacklists and process whitelists are mutually exclusive.

Enable Process Whitelist. This option enables process whitelisting. Add processes by using their executable names (for example, cmd.exe).

> **Note:**
>
> If enabled, **Enable Process Whitelist** automatically blacklists all processes not in the whitelist.

Exclude Local Administrators. Excludes local administrator accounts from the process whitelist (they can run all processes).

Exclude Specified Groups. Lets you exclude specific user groups from the process whitelist (they can run all processes).

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

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 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, 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.
     - **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.

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

> **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.

   > **Important:**
   >
   > WEM provides you with a tool named **AppInfoViewer** to obtain the following information and more from executable files: publisher, path, and hash. For more information, see Tool to obtain information for executable files.

   - **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.

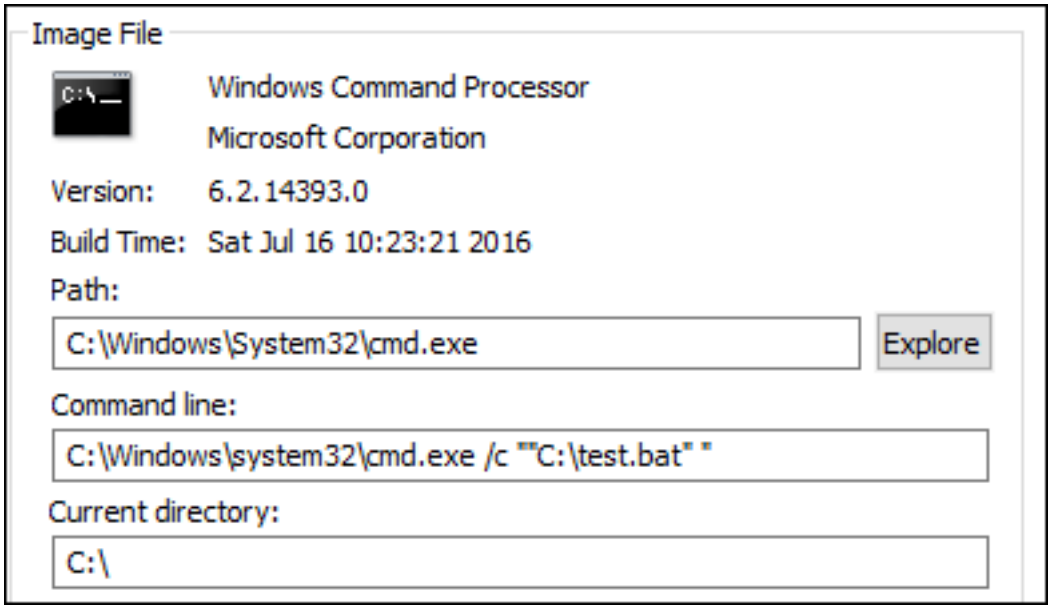
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.



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`

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

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.

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 the 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`.

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

> **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 the 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 the 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:
  - **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.

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

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 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.

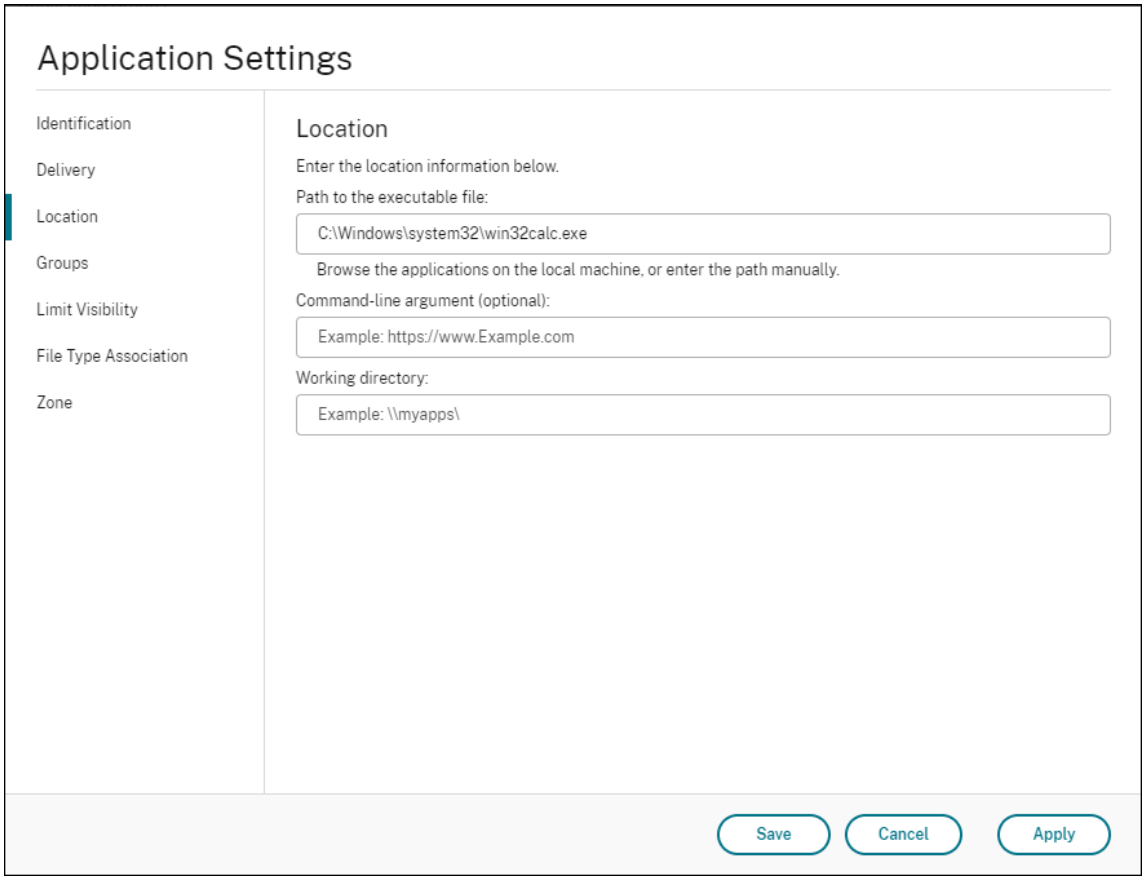
  With the two rules, you cannot open CMD from Notepad by first opening Word and then opening Notepad from Word, regardless of the priority of the rules.

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`.

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:

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

- You must restart the agent machine after upgrading or uninstalling the agent.

  > **Note:**
  >
  > If you upgrade from or uninstall versions **2103.2.0.1** or **2104.1.0.1**, no restart prompt appears.

- The automatic agent upgrade feature does not work on agent version **2105.1.0.1** or later. To use the automatic agent upgrade feature, use the **AppInfoViewer** tool to first disable the process hierarchy control feature.
- If you upgrade from versions **2103.2.0.1** or **2104.1.0.1**, you must restart the agent machine after the automatic agent upgrade completes.

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`

> **Important:**
>
> On versions **2103.2.0.1** and **2104.1.0.1** of the agent, the process hierarchy control feature might be automatically enabled. To verify that the process hierarchy control feature is enabled, open the Registry Editor on the agent machine. If the feature is enabled, you must restart the agent machine manually after upgrading or uninstalling the agent.

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.

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

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.

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.

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

- **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.
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 preceding page.

> **Important:**
>
> WEM provides you with a tool named **AppInfoViewer** to obtain the following information and more from executable files: publisher, path, and hash. For more information, see Tool to obtain information for executable files.

- **Path**. Type the path to the file or folder to which you want to apply the rule for parent processes. The WEM agent applies the rule to an executable according to the executable file path. We do not recommend that you type only asterisk (*) in this field to indicate a path match. Doing that might cause unintended performance issues.
- **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 to parent processes 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.

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

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.
    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

March 4, 2026

Use these pages to specify the users, computers, groups, and organizational units you want Workspace Environment Management™ (WEM) to manage.

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

> **Note:**
>
> Add users, computers, groups, and OUs to WEM so that the agent can manage them.

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 or group

1. Select **Add** from the context menu.
2. Enter a user or group name in the **Select Users or Groups** window and then click **OK**.

After connecting your Citrix Cloud™ account to your Azure Active Directory (AD), you can also add Azure AD users and groups. Complete the following steps:

1. Click the down arrow next to **Add**. The **Add Azure AD User** window appears.
2. In the **Add Azure AD User** window, type information in the search bar and then click **Search** to display matched users or groups.
3. Select applicable users or groups and then click **OK**.

For information about connecting Citrix Cloud to Azure AD, see Connect Azure Active Directory to Citrix Cloud.

Name. The name of the user or group.

Description. Shown only in the **Edit Item** dialog, letting 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 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.

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

Item State. Lets you choose whether a user or group is enabled or disabled. If disabled, you cannot assign actions to it.

Machines

A list of machines that have been added to the current configuration set. Only machines listed here are managed by Workspace Environment Management. You can use **Find** to filter the list by name or ID against a text string.

When agents on these 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 AD 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 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**.

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

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.

* Read-only details reported from Active Directory.

Advanced

Unbound agent site settings

Control whether to apply settings to agents that are not bound to any configuration set.

The following settings apply to your entire WEM deployment. They are not associated with any configuration sets. After you enable them, 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**.
    - **Include unbound non-domain-joined agents**. Lets you control whether to apply the settings to unbound non-domain-joined agents.

AD Settings

Control the following AD-related settings:

- **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.

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

- **Active Directory connection security**. By default, WEM uses *LDAP* for Active Directory queries. To enforce encrypted connections using *LDAPS*, select **Enable LDAPS to encrypt Active Directory connections**.

Transformer Settings

September 7, 2025

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.

Browser support: Use Transformer on the latest version of Microsoft Edge.

General

General settings

These settings control the appearance and basic settings for Transformer.

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 DaaS (formerly Citrix Virtual Apps and Desktops™ service) and Citrix Virtual Apps and 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.

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

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.

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 re-launched.

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).

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

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.

> **Note:**
>
> While configuring the transformer, ignore the Advanced & administration settings.

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.

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.

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

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.

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.

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

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

September 7, 2025

These settings modify how and when the agent processes actions.

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.

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

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.

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:

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

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.

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).

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

> - 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.
> - 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.

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.

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:

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

- 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 a time-intensive process. Select this option only if necessary.

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.

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

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.

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. 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 cache refresh delay times out. For example, you set the value to 30 minutes. The agent selects a random value from this interval: [(30 –30/2), (30 + 30/2)].

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. Type an integer that is equal to or greater than 15 minutes.

Agent Extra Launch Delay. 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.

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

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 service. 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 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. Specify the URL in this form: `http[s]://hostname[:port]`. The host name is the FQDN of the store and the 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.

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

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.

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 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.

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

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.

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.

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

> 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.

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 to

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

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

September 7, 2025

The **Administration** pane consists of the following:

- **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™ (WEM). You can use the logs to:
  - Diagnose and troubleshoot problems after configuration changes are made.
  - Assist change management and track configurations.
  - Report administrative activities.

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

Users

This page displays statistics about your WEM deployment.

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 WEM 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 (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. 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 WEM deployment.

Statistics

This page displays a summary of the WEM agents recorded in the WEM database.

Agents Summary. Displays a count of total agents that have reserved a WEM 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 WEM service.

- 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.

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

- 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 on your deployment.

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). This 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 WEM service 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 WEM service 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.

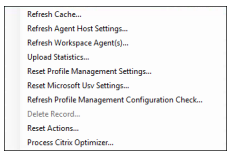
To refresh agents When you refresh an agent it communicates with the infrastructure server. The infrastructure server validates the agent host identity with the WEM database.

1. Click **Refresh** to update the list of agents.
2. In the context menu select **Refresh Workspace Agents**.

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

Options in the context menu When applying the 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 run on the agent side. The more agents you have on the same subnet, the shorter the delay.
- 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.



Currently, applying these options to non-domain-joined and enrolled agents is not supported.

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.

> **Note:**
>
> If the settings are not applied to the agent after configuring **Reset Profile Management Settings**

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

> 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 hosts 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.

The refresh operations described earlier in this section can also be performed on the agent side. However, those operations behave differently depending on actual conditions. For more information, see Agent-side refresh operations.

Upgrade Agent to Latest Version. Lets you upgrade the agent to the last version. The time at which you perform an agent upgrade determines the latest version of the agent. To see the latest agent version, go to the WEM service **Utilities** tab.

Registrations

This page shows the registration status of the WEM 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.

The following information is reported:

Machine Name. Name of computer on which the agent is running.

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).

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

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 WEM 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 WEM 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 login 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.

Agent

This tab lists all changes made to your WEM 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 login XLS format.

Refresh Log. Refreshes the log.

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

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

September 7, 2025

These pages contain detailed user login and machine boot reports.

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.

> **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**.

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

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.

Manage (web console)

September 7, 2025

Start the administration console

1. Log on to your Citrix Cloud™ account.
2. In the Workspace Environment Management™ (WEM) service tile, click **Manage**.
3. In **Overview**, click **Manage Service** or click the **Manage** tab.

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

Configure your deployment

Use **Manage > Web Console** to configure WEM settings. The console consists of two panes:

- The left-hand pane (navigation pane), which displays quick navigation nodes. The following nodes are available:
  - **Home**. Provides an overview of your WEM deployment along with information necessary for you to get to know and get started with WEM quickly.
  - **Configuration Sets**. Displays a list of configuration sets.
  - **Directory objects**. Lets you add machines, groups, OUs, and more, that you want WEM to manage.
  - **Monitoring**. Displays a dashboard to monitor and troubleshoot your WEM deployment and lets you perform administrative tasks. Click the node to display more items.
  - **Files**. Lets you manage all your files on your cloud storage in one place.
  - **Scripted Tasks**. Lets you add scripted tasks that you customize to suit your unique environment management needs. You can then automate those tasks with WEM by configuring them in the applicable configuration set.
- The right-hand pane, which displays details related to the node you are on.

For information about the settings you can use with the web console, see user interface description (web console).

Home page

September 7, 2025

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:

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

- 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.

  > **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.

Highlights

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

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

- 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

August 17, 2026

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
- Edit or delete a configuration set
- Add configuration sets to favorites
- Apply recommended settings
- 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

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

> **Note:**
>
> - Full administrators can perform all these operations.
> - Read-only restricted administrators can only *view* and *refresh* configuration sets within their assigned scopes.

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. (Optional) Select a scope for the configuration set. If you leave this field empty, only full administrators can access it.
5. 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.
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, description or scope. Or, click **Delete configuration set**.

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

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.

Apply recommended settings

Recommended settings are predefined configuration templates that help you standardize configurations across sites and environments and reduce repetitive configuration tasks.

To apply recommended settings to a configuration set, perform the following steps:

1. On the **Configuration sets** node, locate and click the configuration set.
2. In the upper right corner, click **Configuration set options**, and then select **Apply recommended settings**.
3. Click **Save** to apply the recommended settings to the configuration set.

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

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

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:

- **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.

> **Note:**
>
> Only full administrators can upload configuration files and manage automatic backups.

To upload a file, perform the following steps:

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

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.

> **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 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

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

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

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.

Back up Profile Management settings

> **Important:**

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

> 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

August 17, 2026

In Workspace Environment Management™ (WEM), actions are crucial for customizing user environments. They define the configurations and resources applied to users or machines. Using actions can improve logon performance and simplify environment management.

You apply actions to users or machines through assignments and refine them with filters to target specific scenarios. Actions are organized into configuration sets—logical containers that group related settings based on your use cases.

Group Policy settings

Group Policy provides centralized management of user and computer settings on Windows. WEM extends this capability by supporting a wide range of policy configurations and allowing you to migrate existing Group Policy settings from Microsoft Active Directory. Processing Group Policy through WEM can help reduce logon times in Citrix® environments.

You can process Group Policy settings in two ways:

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

- Registry-based settings processing

  You can configure settings directly by specifying their registry locations. This method is fast and flexible.

- Template-based settings processing

  You can configure settings using Administrative Templates (ADM or ADMX files). This method provides structured configuration management.

> **Important:**
>
> WEM currently supports managing Group Policy settings associated with the `HKEY_LOCAL_MACHINE` and the `HKEY_CURRENT_USER` registry hives. To configure Group Policy preferences such as environment variables, go to the corresponding objects in the Actions section.

Before you begin

To enable Group Policy settings processing for a configuration set, go to **Actions > Group Policy settings** and turn on **Process GPOs**.

- When **Process GPOs** is enabled, the WEM agent can process Group Policy settings. The **Enforce processing of GPOs** option also becomes available. When you enable it, the agent reprocesses Group Policy settings on every refresh cycle, even when no changes are detected. This option helps keep policies consistently enforced.
- When **Process GPOs** is disabled, the WEM agent does not process Group Policy settings even if they are already assigned to users or user groups.

Manage registry-based settings

Use the **Registry-based** tab to configure settings for Windows by configuring registry operations.

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

- **Create GPO:** Create a registry-based Group Policy object (GPO).
- **Import:** Import registry-based Group Policy settings into WEM.
- **Refresh:** Update the GPO list.
- **View:** Display the details of a GPO.
- **Edit:** Modify a selected GPO.
- **Manage assignments:** Manage assignments for a GPO.

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

- **Clone:** Clone a GPO.
- **Delete:** Delect 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 use the Import function to migrate configurations from your existing Group Policy infrastructure. You can import settings from a GPO backup or directly from exported registry files.

Before importing settings from registry files, be aware of the following:

- When importing settings, you can upload only .zip files into the WEM console. The .zip 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 by default.

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

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

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

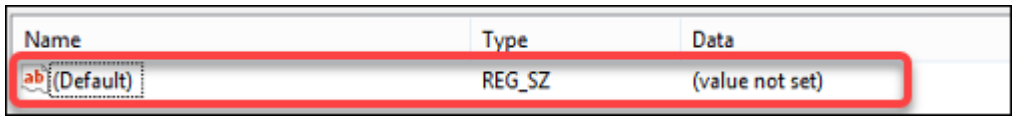
> **Note:**
>
> You can upload only files whose size doesn't exceed 20 MB.

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.
    - **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

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

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

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, 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.

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

- Delete 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 users, Active Directory (AD) groups, or organizational units (OUs). An AD group or OU can contain both users and machines.

- **Machine-level settings** apply when the computer belongs to the assigned group or OU.
- **User-level settings** apply when the signed-in user belongs to the assigned group or OU.

> **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:

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 be-

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

> fore 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.
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.

Manage template-based settings

Use the **Template-based** 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:** Create a template-based Group Policy object (GPO).
- **Manage templates:** Manage Administrative Templates.
- **Import templates:** Import custom Administrative Templates into WEM.
- **Refresh:** Update the GPO list.
- **Edit:** Update a GPO.
- **View:** Update a GPO.
- **Clone:** Clone a GPO.
- **Delete:** Delete a GPO.

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

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 the 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 checkbox, 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 the 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 checkbox, input box (text or number as input), selection, list, or a combination.

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

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

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

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.

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.

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

> **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.
- View an application
- 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.
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

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

> 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:
            - **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.

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

> **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.
     - 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

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

- **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.

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**.

View an application

You can view the WEM applications in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings

To view a application, complete the following steps:

1. Select the application and then click **View** in the action bar.
2. You can view the name, description, and configurations.
3. After you finish, click **Close**.

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:

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

- Create a 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.

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.

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

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.

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, view, 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:

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

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.
    - **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.

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

- **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.

> **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. For more information, see Supportability matrix for triggers.

- Built-in triggers:
  - **Agent refresh**
  - **Reconnect**
  - **Logon**
  - **Logoff**
  - **Disconnect**
  - **Lock**
  - **Unlock**
  - **Machine startup**
  - **Machine shutdown**
- Windows triggers:
  - **event**
- Scheduled 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.

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

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 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**.

View an external task

You can view the WEM external tasks in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings

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

To view a external task, complete the following steps:

1. Select the external task and then click **View** in the action bar.
2. View the name, description, and configurations.
3. After you finish, click **Close**.

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.
    - 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.

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

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**.

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.

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

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:

- Add a printer.
- Add printers from a print server.
- Refresh the printer list.
- Edit a printer.
- View 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.

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

- **Display name**. Specify the name of the printer. The name appears in the user environment.
- **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**.

View a printer

You can view the WEM printers in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings

To view a printer, complete the following steps:

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

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

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.
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

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

- 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.

You can perform the following operations:

- Add a network drive.
- Refresh the network drive list.
- Edit a network drive.
- View 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.

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

- **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.
- **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**.

View a network drive

You can view the WEM network drives in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings

To view a network drive, complete the following steps:

1. Select the network drive and then click **View** in the action bar.
2. View the name, description, and configurations.
3. After you finish, click **Close**.

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.

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

- 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.
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.

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

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.
- View a virtual drive.
- Manage assignments for a virtual drive.
- 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.

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

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**.

View a virtual drive

You can view the WEM virtual drives in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings

To view a virtual drive, complete the following steps:

1. Select the virtual drive and then click **View** in the action bar.
2. View the name, description, and configurations.
3. After you finish, click **Close**.

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

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

> **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.

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:

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

- 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.
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.

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

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.
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.

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

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:

- 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.

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

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.
- View an environment variable.
- Manage assignments for an environment variable.
- Clone an environment variable.
- 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.

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

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.
3. Make changes as needed.
4. After you finish, click **Save**.

View an environment variable

You can view the WEM environment variables in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings

To view an environment variable, complete the following steps:

1. Select the environment variable and then click **View** in the action bar.
2. View the name, description, and configurations.
3. After you finish, click **Close**.

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.

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

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.

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

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

> - 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**.
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.

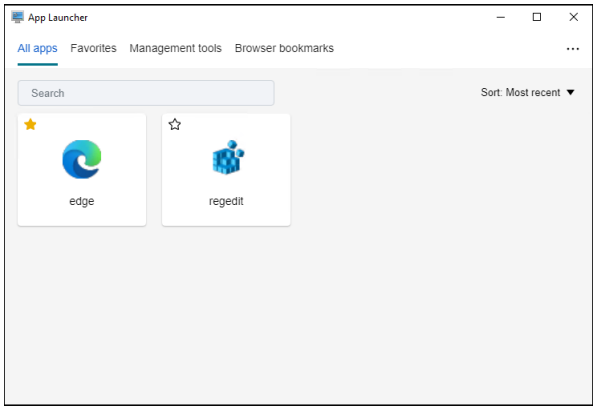
> **Tip:**
>
> We recommend that you publish this tool as a Citrix virtual app.

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.

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

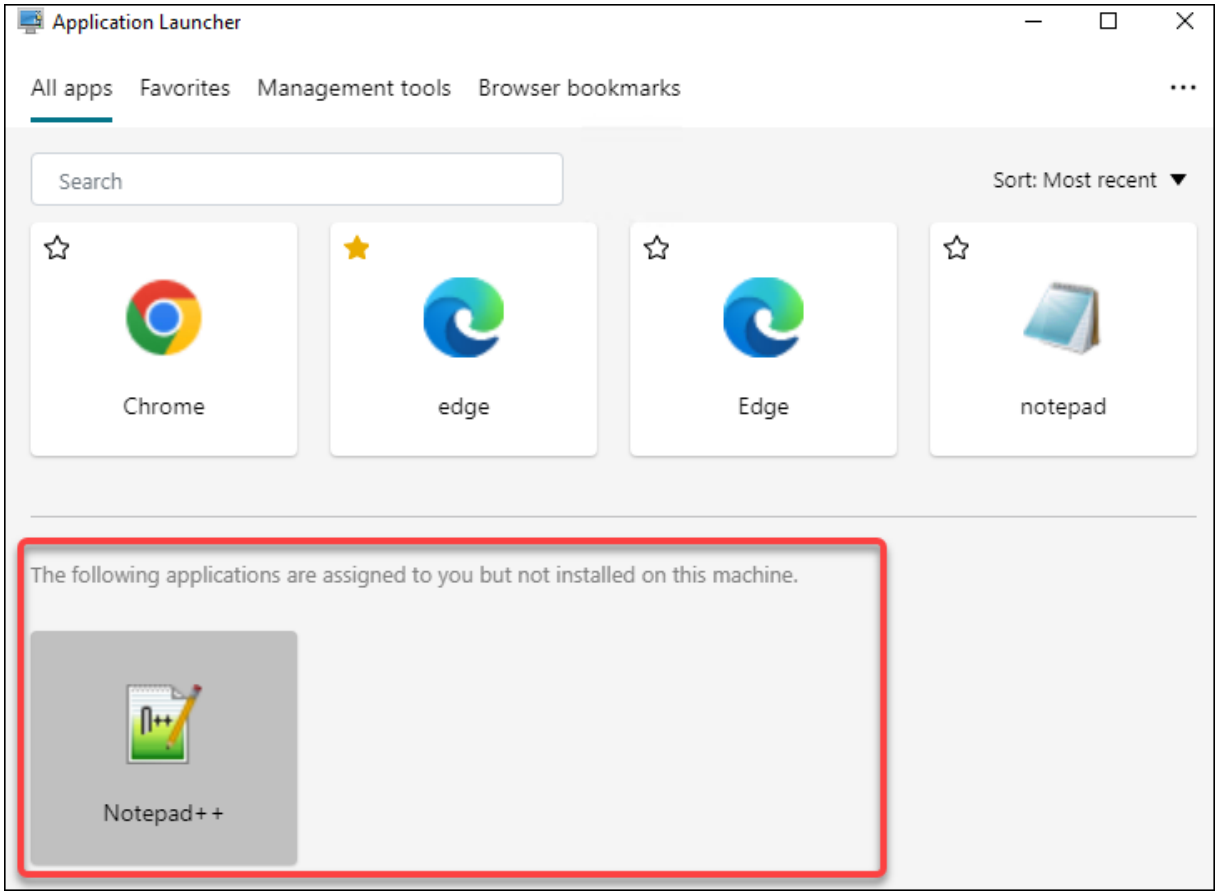
Your users can directly open the application launcher tool (AppLauncherUtil.exe) in their environment. The tool is available in the agent installation folder: `%ProgramFiles%\Citrix\Workspace Environment Management Agent\ AppLauncherUtil.exe`. After opening the tool, users see the following, reflecting the applications assigned to them:



- **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:

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

- 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.

> **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.

© 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:

- Add FTAs
- Refresh FTAs
- Edit FTAs
- View FTAs
- Manage assignments
- Clone FTAs
- Delete FTAs

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

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`

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.

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

> **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**.

View a file type associations You can view the WEM file type associations in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings.

To view a file type association, complete the following steps:

1. Select the file type association and then click **View** in the action bar.
2. View the name, description, and configurations.
3. After you finish, click **Close**.

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.

- 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.

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

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.
- Edit a JSON object.
- View 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:

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

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** and select **Standard**.
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.

   generate-with-template

   - **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.

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

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"],
    "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.
4. Click **Done**.

For more information, see Customize the Start menu layout for Windows 11.

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

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**.

View a JSON object You can view the WEM JSON objects in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings

To view a JSON object, complete the following steps:

1. Select the JSON object and then click **View** in the action bar.
2. View the name, description, and configurations.
3. After you finish, click **Close**.

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.

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.

Target Value. Specifies the value itself.

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

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 perform the operation 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**.

View an INI file You can view the WEM INI files in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings

To view an INI file, complete the following steps:

1. Select the INI file and then click **View** in the action bar.
2. You can view the name, description, and configurations.
3. After you finish, click **Close**.

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.

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

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 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:`

View a port You can view the WEM ports in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings.

To view a port, complete the following steps:

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

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

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.
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**.

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

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. Now, 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.

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.

View a user DSN You can view the WEM user DSNs in read-only mode. This implementation eliminates the risk of misconfiguration when reviewing the existing settings.

To view a user DSN, complete the following steps:

1. Select the user DSN and then click **View** in the action bar.
2. You can view the name, description, and configurations.
3. After you finish, click **Close**.

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.

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

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.

Security

August 6, 2026

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. 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.

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

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 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 **Administration Console > Security > Application Security** tab and select **Import AppLocker rules**.

On the **Import AppLocker rules** page, you get two import mode options:

- **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.

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

> **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 Operating Systems**: 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.
- **Apply to apps in network locations**: Controls whether privilege elevation applies to applications launched from network locations. If selected, privilege elevation rules also process applications hosted on UNC paths (network shares) or mapped drives, in addition to applications on local drives. By default, this option is disabled.

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 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.

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

- **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.
>
> 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

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

- 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:

- 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.

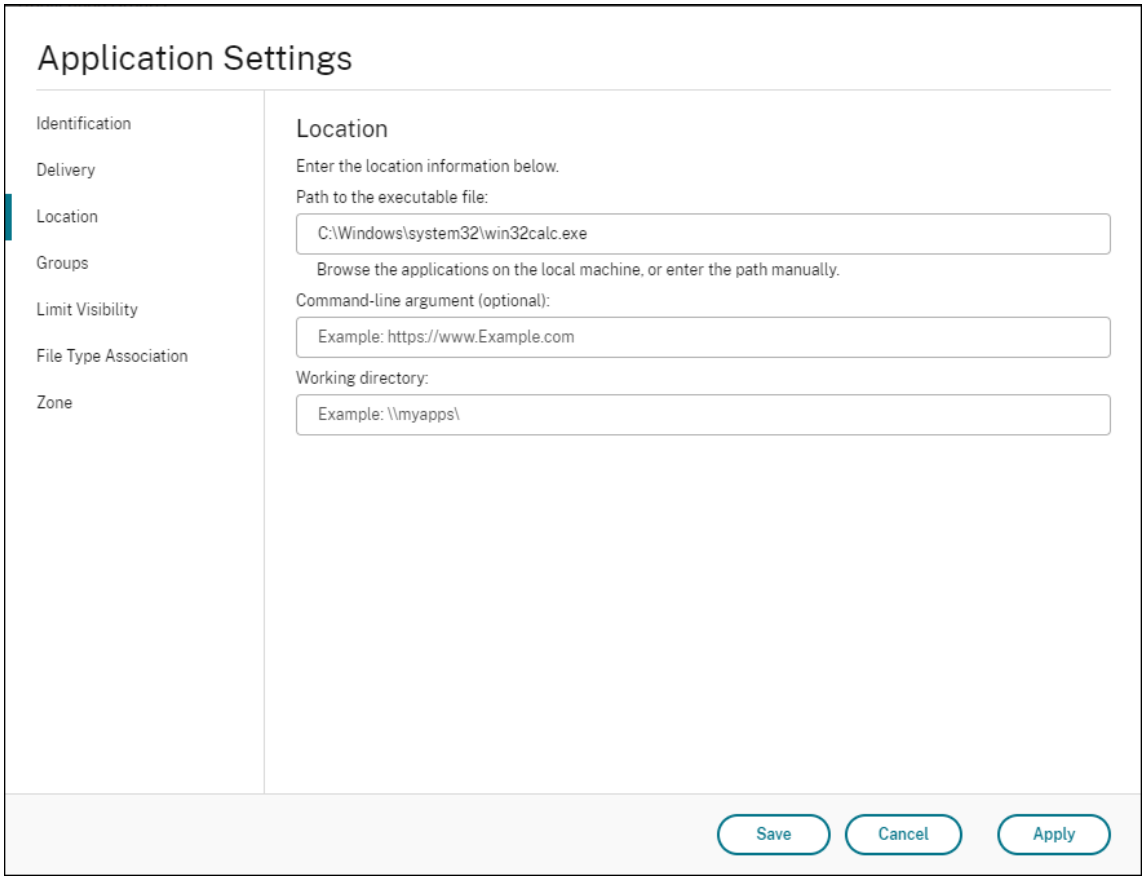
This feature relies on certain process-based parent-child relationships to work. To visualize the parent-child relationships in a scenario, use the process tree feature of the Process Explorer tool. For more information about Process Explorer, see https://docs.microsoft.com/en-us/sysinternals/downloads/procmon.

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

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

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.



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 interface.

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

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.
7. Specify the time period during which the rule is effective.

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

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

June 11, 2026

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:

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

- **Everyone**. A built-in group that contains all users, including anonymous users and guests. Membership is controlled by the operating system.
- **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.
- **Refresh records**. Updates the selected record or the list of records.
- **Requery target names**. Updates the target names.
- **View**. Lets you view details for built-in targets.
- **Manage assignments**. Lets you manage the **Actions** and **Security rules**
- **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.

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

> **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.

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. The location configuration option restricts the OU search scope to a specific location node to find the desired target OU quickly.

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.

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

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**.

> **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).

Modeling wizard

The Modeling Wizard lets you view a user's assigned items, group membership, and OU placement.

To use the Modeling Wizard, perform the following steps:

1. In the identity picker, search for and select an AD or Azure AD user. Only one user can be selected at a time.

   After you select a user, the user's display name and directory path (forest, domain, and name) appear in a summary card.

2. Select **Next** to view the results.

Results

Results are displayed across two tabs:

- Assigned Items
- Groups and OUs

Assigned Items The left panel lists all action categories. Each category shows the count of items assigned to the selected user:

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

Section	Categories
Actions	GPO, Application, Printer, Network Drive, Virtual Drive, Registry Entry, Environment Variable, External Task, File System Operation, File Association, JSON File, INI File Operation, Port, User DSN
Security	Application Security, Privilege Elevation, Process Hierarchy Control

Selecting a category displays the matching assigned items in the right panel, sorted alphabetically. Use the search box to filter by name.

Enable **Show assignment details** to expand each item and display details:

- Filter: The filter condition applied to this assignment, if any.
- Priority: The assignment priority.
- Assignment target: The target this action is assigned to.
- Assignment group: The assignment group that it belongs to.
- (For Printers) Whether the printer is set as the default.
- (For Network or Virtual Drives) The assigned drive letter, **Next available**, or **No letter assigned**.
- (For Applications) Shortcut flags: **Create desktop icon**, **Quick launch**, **Add to Start Menu**, **Auto start**, **Pin to Start Menu**, **Pin to taskbar**.

Groups and OUs The second tab shows the user's directory context resolved during modeling:

- Group membership. Lists all groups that the user belongs to, which determines which assignment targets apply.
- OU placement. Shown for AD users only. Displays the user's innermost OU with its full Distinguished Name.

> **Note:**
>
> - Modeling is performed at query time. Results reflect the current state of WEM assignments and the user's group membership and OU placement.
> - If the user cannot be resolved or assignments cannot be retrieved, an error message is displayed. Go back and reselect the user to retry.

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

Filters

> **Note:**
>
> 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:

- **Create filter**. Lets you create a filter so it is available for use when you assign actions or configure scripted tasks.
- **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**.
- **View Filter**. Lets you view a filter.
- **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.

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. In **Basic information**, configure the following and then click **Next**.
    - **Filter name**. Enter a name for the filter.

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

- **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.

3. 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.

   > **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.

4. 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 sessions run on Citrix Virtual Desktops environments.

> **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.

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

3. (Optional) Enter a description to help identify the filter.
4. Select a template for the filter. See the following table for available templates.

Name	Description	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. **Note:** Time range filters rely on automatic refresh, which and could be delayed until the next refresh.	Session-level filtering

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.
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.

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

Condition type	Description
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**.
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`
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.

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

Condition type	Description
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, 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 (?).

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

Condition type	Description
File version	True or false depending on whether the file version matches the specified values. Enter file versions, separated by semicolons (;).
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. The path must not include any quotes (“). 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**.
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 (?).

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

Condition type	Description
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.
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.

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

The following conditions do not apply to machine settings. If a filter contains any of them, the agent skips them when evaluating the filter.

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

Assignment Groups

This feature allows you to add actions and application security, including GPO and JSON files to a group and select assignment targets for deployment. Assignment details such as filters and options are managed at the individual item level. You can now set a single filter for all assignments associated

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

with a particular target. When you add new items to the group, assignments for those items are generated automatically, letting you review assignment details and make any necessary adjustments.

Create an assignment group

To create an assignment group, complete the following steps.

1. Enter the name and description of the assignment group.
2. Click **Add** and select the desired actions that you need to include in the group on the **Configure group content** page.
3. Choose the assignment targets from the dropdown list.
4. You can either copy, paste, and apply the desired configuration to all the assignments on the tab.

> **Note:**
>
> - If an item in the group is already assigned to a specified target from the dropdown list, the selected target updates the assignment. You can further configure the assignment details for each assignment target in the **Assignment details** page.
> - If a group has been assigned to the organizational units, it cannot contain items other than the Group Policy settings.
> - To add virtual drives, you must select a drive letter manually.

Create an assignment group using security rules You can now create an assignment group using the security rules. Follow the same steps as that of the **Create an assignment group** for this feature. You can also configure the **Privilege Elevation** rule under the **Configure group content** page.

> **Note:**
>
> Default rules cannot be included in the assignment groups and are not displayed in the **Configure group content** page.

Create an assignment group using the exported settings To create an assignment group using the exported settings, import the exported settings into WEM actions and complete the following steps:

1. To begin, upload the ZIP file containing the converted settings.
2. Click **Import** to save the selected settings/items in the current configuration set and create an assignment group with them.
3. Assign the current assignment group to the selected assignment target.
4. Refresh the agent host settings to apply changes immediately.

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

View an assignment group

- To view an assignment group, select it and then click **View** in the action bar.
- You can view the categories of items along with the items listed in the selected category of a table on the **Content** tab.
- On the **Assignments** tab, you can list the assignment targets that the group is assigned to.

Edit an assignment group

- To edit an assignment group, select it and then click **Edit** in the action bar.
- In the **Content** tab, edit the name, description, and content of the assignment group.
- In the **Assignments** tab, you can add or remove the assignment targets. You can also edit the assignment details for each target.

Delete an assignment group

To delete an assignment group, select the assignment and then click **Delete** in the action bar.

Migrate legacy action groups to assignment groups

> **Note:**
>
> This task applies only when an on-premises WEM deployment is migrated to the WEM service. To perform this task, you must have the full **WEM Administrator** role.

After migration, the existing **action groups** from the legacy console appear in **Assignment groups** in the web console as **legacy** items. In the web console, **assignment groups** are the equivalent of legacy action groups. To manage these legacy action groups in the web console, you must migrate them to assignment groups. Afterward, you can edit and manage the migrated assignment groups directly in the web console.

To migrate legacy action groups, follow these steps:

1. In your configuration set, go to **Assignments > Assignment groups**.
2. If legacy action groups exist, an information banner appears below the page title.
3. Click **Migrate legacy assignments** in the banner. The **Migrate legacy assignments** page appears.
4. Review the legacy action groups and their assignments, and then click **Start migration**.
5. Wait for the migration to complete.

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

After the migration completes:

- Legacy action groups are migrated to assignment groups.
- The **Assignment status** changes from **Legacy** to **Assigned**.
- You can edit migrated assignment groups in the web console.
- Some legacy action groups' assignments might contain virtual drives without drive letters. After migration, edit the affected assignments to assign a drive letter for each virtual drive.

Triggers

March 3, 2026

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.

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

> **Note:**
>
> Session triggers let you configure session activities as triggers and are currently available only for external tasks.

- Machine triggers:
  - **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.

> **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:

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

- **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.

- **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:

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

- **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.
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:

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

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.

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

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

	Scripted task	External task
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	

System Optimization

September 7, 2025

Workspace Environment Management™ (WEM) system optimization consists of the following settings:

- CPU management
- Memory management
- I/O management
- 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.

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

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 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

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

> **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). When you select the **Basic Deployment** type, the following optimization features are enabled by default. These settings are stored in the pre-defined agent cache file.

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 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.

© 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 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.

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

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

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.

> **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, looks 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.

> **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:**

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

> - 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 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.

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

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**.

> **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.

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

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.

> **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**.

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

Memory management

These settings let you optimize application memory usage through WEM.

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 the period of releasing excess memory, 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`
- `dllhost`

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

- 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.)
- **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

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

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**.

> **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**.

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

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:

- 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.

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

- 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.

      > **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.

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

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>`

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

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

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.
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**.

Profiles

May 6, 2026

The **Profiles** menu lets you configure Citrix Profile Management, Microsoft User State Virtualization (USV), and user environment settings.

Citrix Profile Management Settings

> **Note:**
>
> Some options work only with specific versions of Profile Management. Consult the Profile Man-

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

> agement 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.

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.

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

> **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.

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**.

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

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).

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.

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

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**.
        - 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.

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

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.

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** 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.

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

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.
- **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.

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

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.

> **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.

Enable BindLink redirection. If enabled, Profile Management uses the Microsoft BindLink API to handle file system redirections within profile containers. This feature is supported only on Windows 11 24H2, Windows Server 2025, or later.

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.

© 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. Specify the type of user profiles to migrate if the user store is empty. Types include:

- 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.

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

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

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.

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

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

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**.
- 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

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

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.
- 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.

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).

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

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.

> **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.

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

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 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.

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

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.

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.

Search Recursivity. Controls how many levels of recursion the user profile search goes through.

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

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.

Environment settings

These settings let you configure user environment settings. You can create, edit, view, clone, and delete environment settings, migrate legacy configuration, and refresh the setting list.

> **Note:**
>
> Deleting an environment setting that is already assigned to users will impact those users.

Create an environment setting

1. In **Environment settings**, click **Add**.
2. Configure the following settings:
   - **Name**. Specify a name to identify the setting.
   - **Filter**. Specify a filter to control when the setting is assigned to **Everyone**. See Filters.
   - **Priority**. Set the priority of the setting for **Everyone**.
   - **Apply this configuration**. Controls whether to assign the setting to **Everyone** based on the filter and priority above.
   - **Settings detail**. Configure the environment setting details.
3. Click **Done** to save and exit.
4. Click **Enable GPO processing** to enable GPO processing for this configuration set. Environment settings take effect only when GPO processing is enabled.

Migrate legacy configuration

If environment settings are already configured in the legacy Administration Console - Policy and Profiles - Environmental Settings, you can migrate them to the web console.

1. Click **Migrate legacy configuration** in the action bar.
2. Preview the configurations to be migrated.
3. Click **Save**.

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

Scripted Tasks

March 4, 2026

> **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**.

> **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.

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

- **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.

> **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.

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

- **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.

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.

© 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

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

March 5, 2025

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

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**.
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.

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

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 `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

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

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.

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 subset 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.

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

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.

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

September 7, 2025

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.

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

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.
- **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.

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

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:

- **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: [(30 –30/2), (30 + 30/2)].

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:

- **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

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

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.
- **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.

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

- **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.

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**

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

- **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**
- **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**

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

- **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**
- **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.

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

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.
- 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.

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

- **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:

- **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.

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

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.
- **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 4 hours. To immediately upload results from the agents, use the **Retrieve statistics from agent** option in Monitoring > Administration > Agents.

  - **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**

  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**

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

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.

  > **Note:**
  >
  > - Results are uploaded every 4 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.

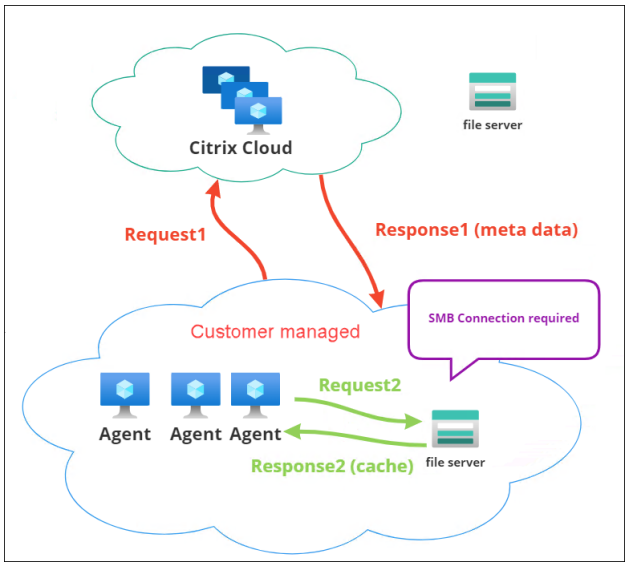
File shares

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

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

on networks and reduces the time to download files to agent machines.

The following graphic provides an overview of how file shares work.



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:
   - **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.

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

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.

Transformer settings

May 22, 2026

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.

Browser support: Use Transformer on the latest version of Microsoft Edge.

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

General

General settings

These settings control the appearance and basic settings for Transformer.

Enable Transformer. If enabled, Agent Hosts connected to this site automatically go 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.

Home page URL. This URL is used as the web front end for the user's virtual desktop. This is the access URL for your Citrix DaaS™ (formerly Citrix Virtual Apps and Desktops™ service) and Citrix Virtual Apps and Desktops environment.

Custom title. If enabled, the Workspace Environment Management™ Agent kiosk window is given a custom title-bar.

Windowed 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.

Show clock. If enabled, displays a clock in the Transformer UI.

12-hour / 24 hour. 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.

Automatically hide application panel. If enabled, the application panel auto-hides itself when not in use.

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.

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

Tool settings

Enable tool list. If enabled, adds a list of tools to the kiosk interface.

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 re-launched.

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 user name for VMware View. If enabled, clears the user name of the previous user on the logon screen when you launch a VMware desktop session.

Monitor remote session status for end-of-session action. If enabled, allows the process launcher to monitor the virtual applications or desktops running on a user's machine and to run **Take action when a remote session ends** when they are all closed. Select from the following options:

- **VMware View session**. Monitors sessions in VMware View mode.
- **Microsoft RDS session**. Monitors sessions in Microsoft Remote Desktop Services (RDS) mode.
- **Citrix session**. Monitors sessions in Citrix mode.

Advanced & administration settings

Run web browser in Internet Explorer compatibility mode. 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.

> **Note:**

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

> While configuring the transformer, ignore the Advanced & administration settings.

Redirect logoff screen to logon. If enabled, automatically redirects the user to the logon page whenever they land on the logoff page.

Suppress web page script errors. If enabled, suppresses any script errors it encounters.

Suppress SSL certificate errors. If enabled, hides SSL warnings entirely.

Hide transformer UI 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 and Start button. If enabled, hides the user's taskbar and start menu. Otherwise, the user is still able to access their desktop.

Prevent task switching (Alt+Tab). If enabled, ignores alt tab commands, preventing the user from switching away from the agent.

Allow sending kiosk UI to background. 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 in full screen. 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 auto-logon** 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.

Hide browser 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.

Pre-launch Citrix Workspace app. If enabled, launches Citrix Workspace app and waits for it to load before bringing up the kiosk mode window.

Allow hotkey to unlock kiosk mode (Ctrl+Alt+U). If enabled, allows users to unlock the kiosk mode by pressing **Ctrl+Alt+U**.

Hide log off 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 shut down option. If enabled, hides **Shutdown** under the shutdown icon in the Transformer UI.

Ignore last-used 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 auto-logon. If enabled, users automatically log on to the desktop environment by the agent, bypassing the Windows logon screen.

Log off from Citrix 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.

Take action when a remote session ends. 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 after idle period. 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.

Directory Objects

March 4, 2026

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

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.

> **Note:**
>
> Converting distinguished names to computer 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.

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
- Non-domain-joined machines

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.

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

> **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**.

Add non-domain-joined machines

> **Note:**
>
> Non-domain-joined machines listed in **Directory Objects** are not shown in the list of machines available to be added to a configuration set.

1. On the **Directory Objects** node, click **Add object**.
2. Select **Non-domain-joined machines** from the object type list.
3. Search for the machines you want to add.
4. Click the plus sign to add. Machines you add are listed in the table under the search box.
5. Select the configuration set to which you want to add them.
6. 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, OUs, or non-domain-joined machines).
    - **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. To change the name and description, use the Full Configuration interface of Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service).

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**.
    - **Include unbound non-domain-joined agents**. Lets you control whether to apply the settings to unbound non-domain-joined agents.

> **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.

Enforce LDAPS to encrypt Active Directory connections

By default, WEM uses *LDAP* for Active Directory queries. To enforce encrypted connections using *LDAPS*, select **Enable LDAPS to encrypt Active Directory connections**.

Non-domain-joined agents

Set up binding rules for unbound non-domain-joined agents. A rule dictates which configuration set to bind the matching agents to. Each agent is evaluated against the rules in the order listed until a match is found. You can add up to 50 rules.

To create a rule, complete the following steps:

1. Click **Create rule**.
2. Configure settings as needed:
    - **Name**. Name the rule.
    - **Criteria**. Add one or more criteria.
        - **Device name**. Enter a regular expression that describes device names to match. For example, if the machines you want to match are named PC-Sales-01, PC-Sales-02, PC-Sales-03, and so on, enter the following expression: `PC-Sales.*`.

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

- **IP address**. Enter an IP address or an IP address range. You can also enter a regular expression that describes IP addresses to match. For example, if the addresses you want to match are 192.168.1.0 through 192.168.1.255, enter the following expression: `192\.168\.1\..*`.
- **MAC address**. Enter a comma-separated list of MAC addresses.

3. Select the configuration set to bind matching machines to.
4. After you finish, click **Done** to save and to exit.

Monitoring

June 2, 2026

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.
  - **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.

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

- Logging. View a record of all changes that administrators make to WEM settings, including who made the change, when, and what was modified.

Administration

March 4, 2026

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.

> **Note:**
>
> Restricted administrators can view statistics only for users in configuration sets within their assigned scopes.

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.

© 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. 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.

> **Note:**
>
> - Restricted administrators cannot clear expired records or delete records.
> - When exporting, you must apply a filter that includes a configuration set condition.

To export data, perform the following steps:

1. Click **Export**. The export wizard appears.
2. Select the export format. Available options: CSV and JSON.
3. Optionally, select **Save a copy of the export to your local machine**. The export is saved to the default download location of your browser.
4. 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.

Agents

This page lets you view agent information and perform administrative tasks such as refreshing the cache, resetting settings, and retrieving agent information. The agent cache sync is centrally managed

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

by the WEM cloud service. The cache sync interval is 30 minutes by default, which is not configurable. Changing the **Agent cache refresh delay** setting in Advanced Settings will NOT take effect.

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.
  > - When you use the **CEM (Citrix Endpoint Management™)** managed configuration set, the callback tasks are not allowed as these agents are read-only records.

- 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.
- 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

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

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.
- **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.
- **Set as Hub Agent**. Lets you set the selected agent as the hub agent.
- **Configure Hub Agent**. Lets you select the configuration sets for which you want to set the agent as the hub agent.
- **Export**. Lets you export the data in each record in CSV or JSON format, which opens in programs such as Microsoft Excel.

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

> **Note:**
>
> - This page displays only agents within configuration sets where you have at least read-only permissions.
> - Only full administrators can clear expired records, set as Hub Agent, and configure Hub Agent.
> - When exporting, you must apply a filter that includes a configuration set condition.

To export data, perform the following steps:

```
1. Click **Export**. The export wizard appears.
1. Select the export format. Available options: CSV and JSON.
1. Optionally, select **Save a copy of the export to your local
   machine**. The export is saved to the default download location of
   your browser.
1. Click **Export** to start the export process.

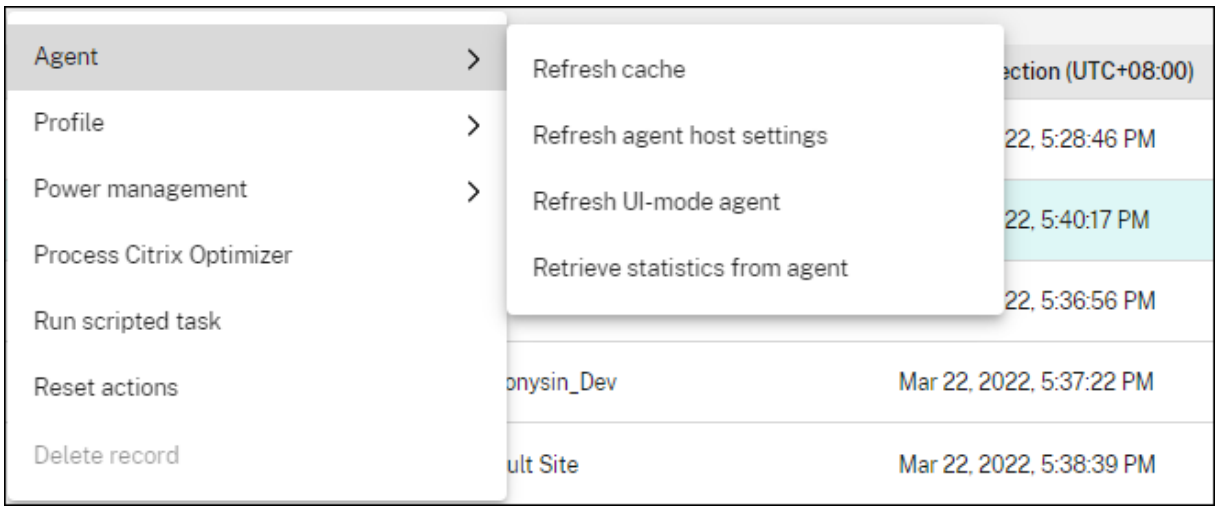
> **Important:**
>    > - You can export up to 50,000 records. When the number of
   records to export exceeds the limit, only the top 50,000 will be
   exported. We recommend that you use filters to reduce the number of
   records to 50,000 or fewer.    > - While an export is in progress,
   you cannot 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](/
   en-us/workspace-environment-management/service/manage/files.html).
```

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.
- 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.

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



Agent:

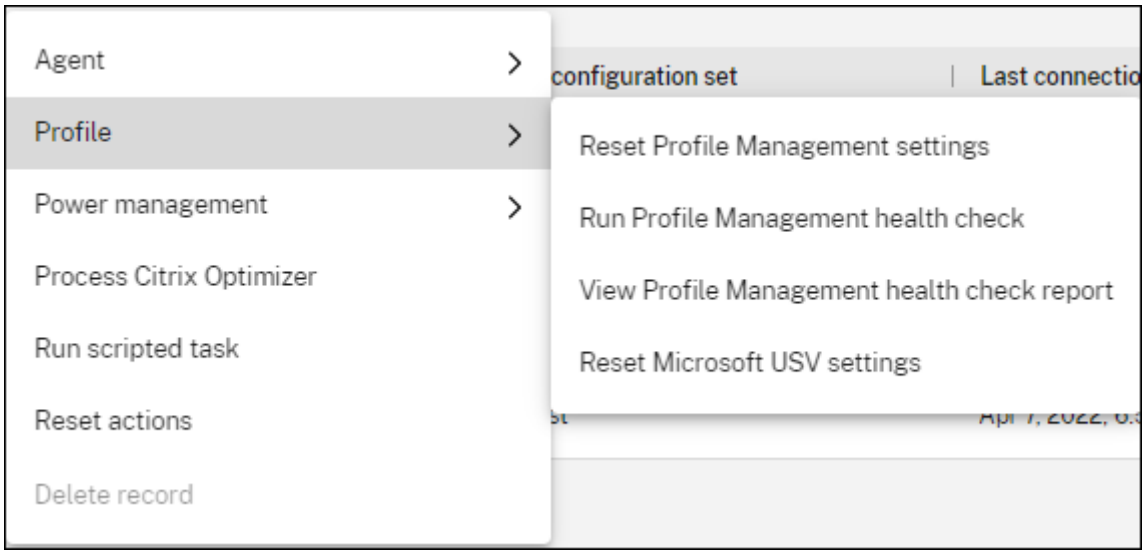
- **Refresh cache**. Triggers a refresh of the local agent cache (an agent-side replica of the WEM configuration database). Refreshing the cache synchronize the local agent cache with the infrastructure services. This option is available to WEM agents only with versions before 2401.1.0.1.
- **Refresh 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. Latest WEM agents with versions 2401.1.0.1 or higher automatically synchronises the agent cache during the agent host settings refresh process. Due to WEM cloud service internal workflow, the agent cache sync may have a maximum delay of (Agent host settings refresh delay x 1.5) + 40 minutes. For example, if the default agent host settings refresh delay (also called SQL settings refresh delay) is 15 minutes, then the maximum agent cache sync delay is 15 minutes x (1.5 + 40 minutes) = 62.5 minutes.
- **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.

  > **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.

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

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:

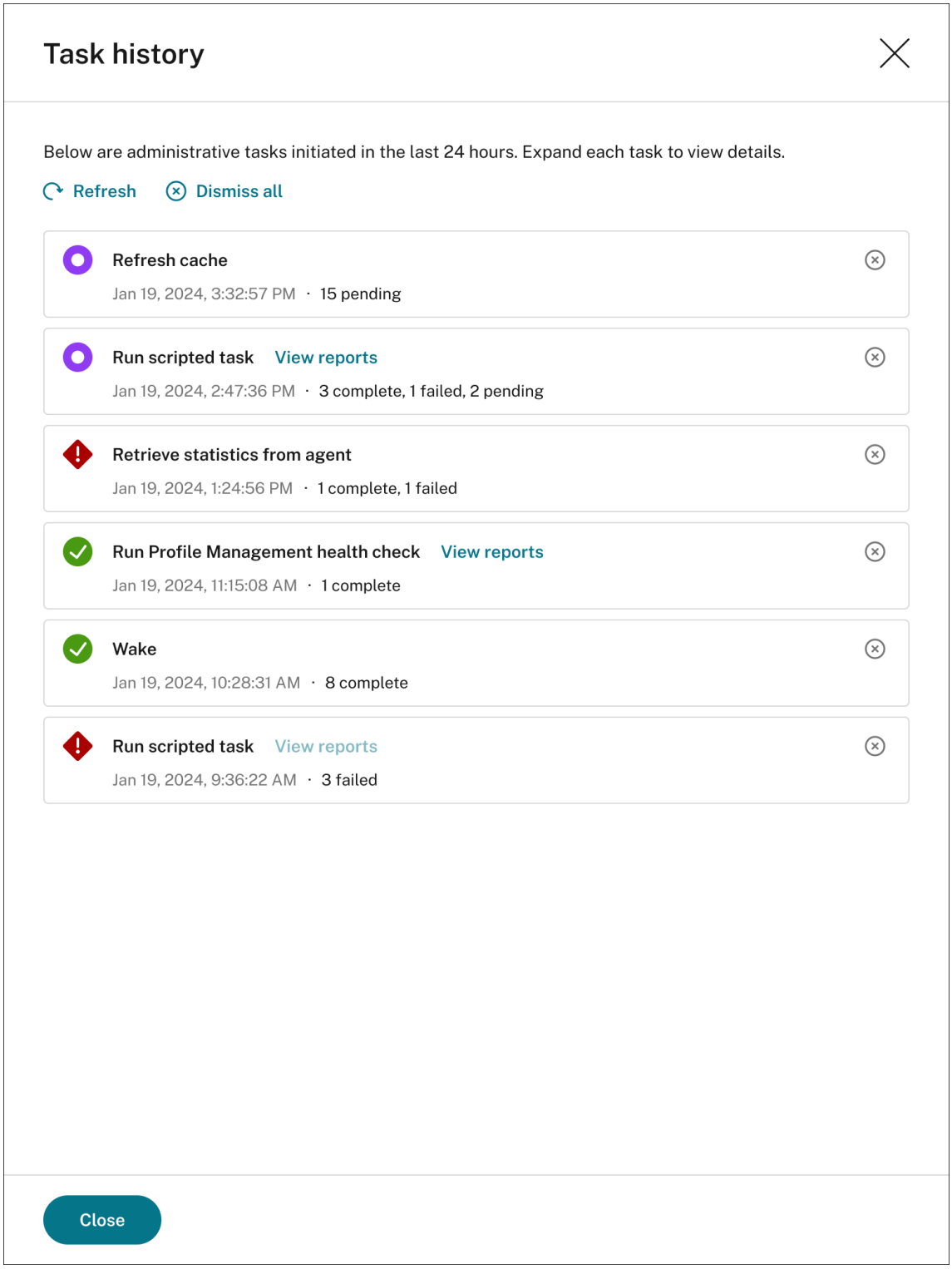
- **Reset Profile Management settings**. Clears the registry cache and updates the associated configuration settings. If Profile Management settings are not applied to your agent, click **Reset Profile Management Settings**. You might need to click **Refresh** for this option to become available.

  > **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.

- **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.
- **Reset Microsoft USV settings**. Clears the registry cache and updates the associated configura-

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

tion 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`.

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.

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

> **Note:**
>
> This option does not apply to non-domain-joined agents.

- **Task**. Select which scripted task you want to run.
- **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.

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.

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

> **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.
  - **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.

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

Hub Agents

Hub agents act as a bridge between the WEM service and your on-premises resources such as SMB shares. With hub agents specified, the WEM service gains access to on-premises sources.

Designate an agent as the hub agent To enable WEM to access your on-premises resources, specify hub agents for your configuration sets.

Follow these steps to assign an agent as the hub agent for multiple configuration sets:

1. Go to **Monitoring** > **Administration** > **Agents**.
2. On the **Statistics** tab, select an agent as needed, and click **Set as hub agent**.
3. On the **Set as hub agent** page that appears, select the configuration sets for which you want to set this agent as the hub agent.
4. Click **Done**.

   The agent appears on the **Hub agents** tab.

> **Note:**
>
> To ensure proper functioning, hub agents must be connected to a network that can access the on-premises resources and the agents in the selected configuration sets.

View and manage hub agents The Hub agent tab displays all hub agents in your deployment along with their details:

- **Status:** Online, Offline, agent not found, or other connection updates.
- Lists of associated configuration sets.

You can manage hub agents as needed:

- To refresh the status of a hub agent, click the Refresh icon next to the status.
- To change the list of configuration sets associated with the hub, click the **Configuration** icon at the end of the agent record.
- To demote the hub agent to a normal agent, click the **Delete** icon at the end of the agent record.

Settings

By default, agents are identified by their MAC address. If your agent machines do not have unique MAC addresses, enable the **Use the alternative agent identifier** option to use the alternative identifier that ensures uniqueness.

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

> **Note:**
>
> - Toggle State Changes: When the state of the toggle is altered, the WEM agent requires a service restart to operate according to the new toggle state. The agent reads the toggle state during service startup.
> - Duplication of Records: After switching to use the unique agent identity, a duplication of agent information and statistics records occurs. Click the button **Clear expired records** after 24 hours to resolve the duplication.
> - Report Aggregation: After transitioning to use the unique agent identity, new reports won't be aggregated with the previous reports generated before the toggle was activated due to a new agent identity.
>
> Hub Agent: The Hub agent must be reconfigured.

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

October 9, 2023

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.

Excluded applications

You can exclude applications from the usage insights (bar chart). To specify an excluded application, complete the following steps.

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

- 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.

> **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.

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

> - 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 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

June 16, 2026

Provides reports that let you analyze your deployments.

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

Introduction

The **Reports** page provides two views: List view and Summary view.

List view

The **List** view on the **Reports** page displays reports in a tabular format. 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.
  - **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.

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

- **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:
    - **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, this type of report is available only for Group Policy settings, external tasks, and JSON files. To enable results collection, see Monitoring preferences.
- **Action processing events**

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

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.

Currently, this type of report is available only for script-based external tasks.

- **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.
- **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**

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

- 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**.

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.

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

- **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.

Summary view

The **Summary** view on the **Reports** page displays four charts that provide statistical results of reports based on **Event type**, **Action processing results**, **Configuration set**, and **Script execution results**. Clicking **Refresh** reloads all four charts with the latest results.

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.

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 using the following methods:

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

- Export reports
- Export to third-party platform

> **Note:**
>
> - Restricted administrators can use only the **Export to CSV** or **Export to JSON** functions.
> - When exporting, you must apply a filter that includes a configuration set condition.

Export reports

To export the data in each report to a CSV or JSON format, perform the following steps:

1. Click **Export > Export to CSV or JSON**. 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 is saved to the default download location of your browser.
2. Click **Export**.

> **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. Citrix® recommends 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 no longer receive notifications about it. Go to **Files** to view the export result later.
> - When exporting reports, 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.

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.

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.

Logging

June 2, 2026

The **Logging** page provides a record of all configuration changes and administrative activities in the Workspace Environment Management™ (WEM) web console. You can use it to audit who changed

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

what, when, and in which configuration set. Administrative logs are retained for 180 days, with a maximum of 100,000 records.

Required permissions

Your role controls access to administrative logs:

- **WEM Full administrators** can view all administrative logs across all configuration sets.
- **WEM Restricted administrators** can view logs for configuration sets they have read access to. For operations not associated with a configuration set, **WEM Restricted administrators** can only view their own activity logs.

Access the Logging page

To access the **Logging** page:

1. Sign in to the WEM web console.
2. In the left navigation, go to **Monitoring** > **Logging**.

View log details

Each log record contains the following information:

Field	Description
Time	The date and time the operation was performed.
Administrator	The display name and user principal of the administrator who performed the operation.
Event type	The category of the event.
Operation	The type of operation performed (for example, Create or Update).
Target	The name and type of the object that was modified.
Configuration set	The configuration set associated with the operation, if applicable.
Status	Whether the operation succeeded or failed.
Details	A description of the change, including before-and-after values where applicable.

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

Filter logs

You can filter the log list by the following criteria:

Filter	Description
Time range	Filter logs by start and end time.
Administrator	Filter logs by the administrator who performed the operation.
Event type	Filter by event category: **Configuration changes**, **Assigned agent tasks**, **Monitoring operations**, **RBAC configurations**, or **Enrollment events**.
Operation type	Filter by operation: **Create**, **Update**, **Delete**, **Assign**, or **Unassign**.
Configuration set	Filter logs by the configuration set they are associated with.

Export logs

You can export logs to a CSV or JSON file.

To export logs:

1. Optionally, apply any filters you want.
2. Click **Export** and select **CSV** or **JSON**.

Scripts for scripted tasks

July 10, 2026

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.

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

- 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:

1. Create script content

   Write a PowerShell script based on your requirements.

2. Validate 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 the **Custom** tab, and then click **Add custom script**.
2. In the **Add custom script** wizard, configure the following settings and then click **Save**.
   - **Script name**. Specify a name for the script.
   - **Description**. Optionally, specify additional information to help you identify the script.
   - **Scope (optional)**. Specify the scope to which this script belongs. Only administrators authorized for that scope can access this script. If you do not specify a scope, only full WEM administrators can access this script.

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

- **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.
- **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 custom 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 Custom Script** page, paste the content directly from the 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.

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

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:

- Edit a script
- Delete a script
- Clone a script
- Configure scripted tasks
- Create an external task 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**.

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

> **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**.

> **Note:**
>
> When cloning a script, you are prompted to change the name to avoid duplicate names.

Configure scripted tasks

To configure and automate scripted tasks, 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.

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

Create an external task from a script

Use this action to create an external task directly from an existing script.

> **Tip:**
>
> Scripted tasks work at a machine level. To run tasks at a user session level, create external tasks instead.

To create an external task 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 **Create external task**.
3. In the **Select configuration set** wizard, choose the configuration set where you want to create the task.
4. Follow the steps in Create an external 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
- Check DNS Settings
- Check RDS License
- Diagnose VDA Unregistration
- Run Profile Management Health Check
- Set Profile Reset Trigger
- Diagnose Citrix AOT issues
- Collect Citrix AOT Failure Logs
- Collect Citrix Diagnostic Logs
- Collect Windows Event Logs
- Collect Citrix Scout Diagnostics

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.

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

name	type	default	mandatory	Note
ForceStart	boolean	true	False	Indicates whether to start the service if it's found to be not running. It does not affect running services. 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

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

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.

Parameters

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

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.
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.

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

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

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 delivery controller federated authentication service provisioning services ctx license universal print server citrix ddc control. exe runs before it automatically stops and exits. session recording administration session recording player citrix workspace app for windows
ctlFilePath	string	null	False	Specifies the file to start the trace with.
RunMinutes	Integer	30	False	Specifies how long

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 directories are deleted if the `FileAgeDays` is less than 1 day.

Collect Citrix AOT Failure Logs

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.

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

Name	Type	Default	Mandatory	Note
LogonTime	[string]	null	False	Specifies the logon time to filter event log searches. Accepts various date and time formats. If not 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.

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

Name	Type	Default	Mandatory	Note
FoldersToRestore	[string]	null	False	Specifies the folders to restore after a 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%.

Diagnose Citrix AOT Issues

This script validates Citrix Always On Tracing (AOT) configuration, diagnoses common issues, and generates an AOT diagnostic report to support troubleshooting. Setting the StructuredOutputOnly parameter to **true** displays results in a structured UI view for easier review.

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

Name	Type	Default	Mandatory	Note
StructuredOutputOnly	[boolean]	false	False	If specified, the script outputs only the raw JSON diagnostic report instead of the human-readable formatted text.

Collect Citrix Diagnostic Logs

This script collects Citrix Always On Tracing (AOT) logs and Windows Event Logs from the VDA and saves them as a timestamped ZIP file.

Name	Type	Default	Mandatory	Note
LogType	[string]	Not Applicable	False	Controls which logs to collect. AOTLog collects only AOT ETL files, EventLog collects only Windows Event Logs. Leave empty to collect both.
RestartTelemetryService	[boolean]	true	False	Whether to stop and restart Citrix-TelemetryService before collecting AOT logs, which releases file locks on ETL files. Accepts **true** or **false**. Defaults to **true**.

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

Name	Type	Default	Mandatory	Note
StartTime	[DateTime]	24 hours ago	False	Specifies the start time for log collection. Defaults to 24 hours ago. Example: 2025-08-01 10:57:15
EndTime	[DateTime]	Current time	False	Specifies the end time for log collection. Defaults to the current time. Must be later than StartTime. Example: 2025-08-14 11:57:15
OutputPath	[string]	C:\ProgramData\Citrix\WEM\CitrixLogs	False	Directory to write the output zip file. Defaults to C:\ProgramData\Citrix\WEM\CitrixLogs.

Collect Windows Event Logs

This script collects Windows event logs from the Virtual Delivery Agent (VDA) and saves them as a timestamped ZIP file.

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

Name	Type	Default	Mandatory	Note
LogChannelPrefixes	[string]	Not Applicable	False	Comma-separated prefixes to match against ETW channel names. When provided, overrides the default four-log collection. Example: Citrix-HostCore, Microsoft-Windows-AppLocker.

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

Name	Type	Default	Mandatory	Note
`ProviderPrefixes`	[string]	Not Applicable	False	Comma-separated prefixes to match event provider/source names. The script automatically discovers which log channels each provider writes to via its LogLinks, so it works with both classic logs (Application, System) and custom ETW channels. When provided, overrides the default four-log collection. Example: `WEM Agent Service`, `Norskale Agent Service`.
`StartTime`	[DateTime]	24 hours ago	False	Specifies the start time for event log collection. Defaults to 24 hours ago. Example: 2025-08-01 10:57:15

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

Name	Type	Default	Mandatory	Note
EndTime	[DateTime]	Current time	False	Specifies the end time for event log collection. Defaults to the current time. Must be later than StartTime. Example: 2025-08-14 11:57:15
OutputPath	[string]	C:\ProgramData\Citrix\WEM\CitrixEventLogs	False	Directory to write the output zip file. Defaults to C:\ProgramData\Citrix\WEM\CitrixEventLogs.

Collect Citrix Scout Diagnostics

This script runs ScoutCLI.exe to collect Citrix diagnostic data from the VDA and saves the output as a timestamped ZIP file. Optionally, you can exclude specific collectors, such as MSI or localdata.

Name	Type	Default	Mandatory	Note
OutputPath	[string]	C:\ProgramData\Citrix\WEM\CitrixScoutCliLogs	False	Directory to write the Scout output zip file. Defaults to C:\ProgramData\Citrix\WEM\CitrixScoutCliLogs.

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

Name	Type	Default	Mandatory	Note
`Exclude`	[string]	Not Applicable	False	Comma-separated list of collectors to exclude from Scout collection. Supported values: `msi`, `localdata`. Leave empty to include all collectors.

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

March 4, 2026

This page lets you manage all your files on your cloud storage in one place. The total size of your storage space is 100 MB. 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.

> **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.

> - You can access only the files within your assigned scopes.

Enrollment

September 7, 2025

The **Enrollment** node lists enrolled agents for you to manage and lets you use the enrollment method to enroll agents.

> **Note:**
>
> Enrollment is available only to full administrators.

The enrollment method is one of the three setup methods you can use to connect the Workspace Environment Management (WEM) agent to the WEM service. For more information, see Enroll agents.

The **Enrollment** node consists of the following items:

- Enrolled Agents. Lists all enrolled agents. You can manage them as needed.
- Invitation. Lets you send enrollment invitations to users. Each invitation includes an invitation code and the steps needed to complete the enrollment.

Enrolled Agents

September 7, 2025

Lists all enrolled Workspace Environment Management™ (WEM) agents. You can manage them as needed.

Introduction

After an agent enrolls, it becomes managed. In Directory Objects, you can bind it to a configuration set as needed. For information about enrollment, see Enroll agents.

There are two ways to enroll an agent:

- Enroll by invitation. This requires the web console. Users can be invited to participate in the enrollment process.

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

- Enroll with the bearer token or API secure client. This doesn't require the web console and doesn't require users to participate in the enrollment process. For more information, see Enroll with the bearer token or API secure client.

On this page, you can perform the following operations:

- **Refresh**. Updates the list of enrolled agents.
- **Unenroll**. Unenrolls an agent.
- **Edit associated user**. Changes the association or removes the associated user.
- **Remove invalid agents**. Removes agents with invalid enrollments.

Unenroll an agent

You can unenroll multiple agents at a time. Unenrolling an agent invalidates its enrollment and removes it from WEM.

To unenroll an agent, perform the following steps:

1. In **Enrollment > Enrolled Agents**, select the agent.
2. In the action bar, select **Unenroll**.

Edit the associated user

When enrolled, non-domain-joined devices are automatically associated with invited users. Associating a user with a non-domain-joined machine lets WEM apply settings to the user on logon.

To change the association for a device, perform the following steps:

1. In **Enrollment > Enrolled Agents**, select the agent.
2. In the action bar, select **Edit associated user**. The **Edit associated user** wizard appears.
3. Select an identity provider.
4. Select the domain of the user that you want to add.
5. In the **Select user** box, enter the name of the user that you want to add.
6. After you have finished, click **Save**.

To remove the associated user for a device, perform the following steps:

1. In **Enrollment > Enrolled Agents**, select the agent.
2. In the action bar, select **Edit associated user**. The **Edit associated user** wizard appears.
3. Select **Remove associated user**.

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

Remove invalid agents

If an enrolled agent has been inactive for 270 days, its enrollment becomes invalid. It will no longer be managed by WEM. The **Remove invalid agents** button appears only when there are invalid agents.

Invitation

September 7, 2025

Lets you send enrollment invitations to users. Each invitation includes an invitation code and the steps needed to complete the enrollment.

Introduction

You have the flexibility to determine how to enroll your Workspace Environment Management™ (WEM) agents. There are two ways:

- Enroll by invitation. This requires the web console. Users can be invited to participate in the enrollment process.
- Enroll with the bearer token or API secure client. This doesn't require the web console and doesn't require users to participate in the enrollment process. For more information, see Enroll with the bearer token or API secure client.

A general workflow to enroll by invitation is as follows:

1. In **Manage > Web Console > Enrollment > Invitation**, enable **Enroll by invitation** and then click **Generate** to generate an enrollment key.
2. On the agent machine, install the enrollment key using the enrollment tool.
   a) Open the command prompt as the administrator.
   b) Run the following command. (Replace <enrollment key> with the actual key.)
      - `Citrix.Wem.Agent.EnrollmentUtility.exe configenrollmentkey -k <enrollment key>`

> **Tip:**
>
> The enrollment tool, **Citrix.Wem.Agent.EnrollmentUtility.exe**, is available in the agent installation folder. For more information, see Enrollment tool.

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

3. In **Manage > Web Console > Enrollment > Invitation**, create an invitation or send enrollment invitations to users.
4. Perform the following steps as needed:

    - If you do not want to send enrollment invitations through WEM, create an invitation and then do either of the following:
        - Go to the agent and enroll it with the invitation code.
        - Share the invitation code with your user. Then, your user logs on to the agent and enrolls it with the invitation code.
    - If you want to send enrollment invitations through WEM, no further action is required on your part. After the users receive the invitation email, they can enroll their agents using the invitation code.

    For information about how to enroll the agent with an invitation code, see Enroll the agent with an invitation code.

After an agent enrolls, it becomes managed and appears in **Enrollment > Enrolled Agents**. You can add it to a desired configuration set for precise management. For more information, see Manage the enrolled agent.

Enroll by invitation

Controls whether to open the invitation-based enrollment.

When enabled, you can generate an enrollment key and send invitations. When disabled, agents can't be enrolled using invitations.

Enrollment key

Lets you generate an enrollment key. You then install the key on the agent, using the enrollment tool, **Citrix.Wem.Agent.EnrollmentUtility.exe**, available in the agent installation folder. Without the key, the agent can't enroll using invitations.

The generated key expires in 180 days. After generating a key, you can perform the following operations:

- **Copy**. Copies the key to the clipboard.
- **Download**. Downloads a .txt file that contains the key.
- **Regenerate**. Regenerates the key.

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

> **Important:**
>
> Regenerating a key automatically invalidates the current one. For unenrolled agents, make sure that the valid key is installed before sending invitations.

Enrollment invitation

Lists all invitations. You can perform the following operations:

- Create an invitation
- Invite users
- Refresh the list
- View the details of an invitation
- Resend an invitation
- Delete an invitation
- Clear expired invitations

Create an invitation

You create an invitation by generating an invitation code. The code supports enrolling up to 5 devices and expires after 48 hours.

With the code, you can do the following as needed:

- Use the code yourself. Go to the agent and enroll it with the code.
- Share the code with your user. Then, your user logs on to the agent and enrolls it with the code.

> **Important:**
>
> WEM audits activities associated with an invitation code on a per code basis, for example, who does the enrollment, when the enrollment occurs, and which device is enrolled. So, we recommend that you do not share the same code with multiple users.

To create an invitation, perform the following steps:

1. In the action bar, select **Create invitation**. The **Create invitation** wizard appears.
2. Select **Generate code**.
3. After the code is generated, select **Copy to clipboard**.

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

Invite users

You can send enrollment invitations to your users. Each invitation includes an invitation code and the steps needed to complete the enrollment.

Consider the following when inviting users:

- You can invite up to 100 users.
- An invitation code is created for each user. The code supports enrolling up to 5 devices and expires after 48 hours.
- Users with a registered email address will receive the invitation code by email. For users without a registered email address, you can share the invitation code with them using other methods.
- Enrolling an agent requires *local administrator permissions*. When enrolled, non-domain-joined devices are automatically associated with invited users.

To invite users, perform the following steps:

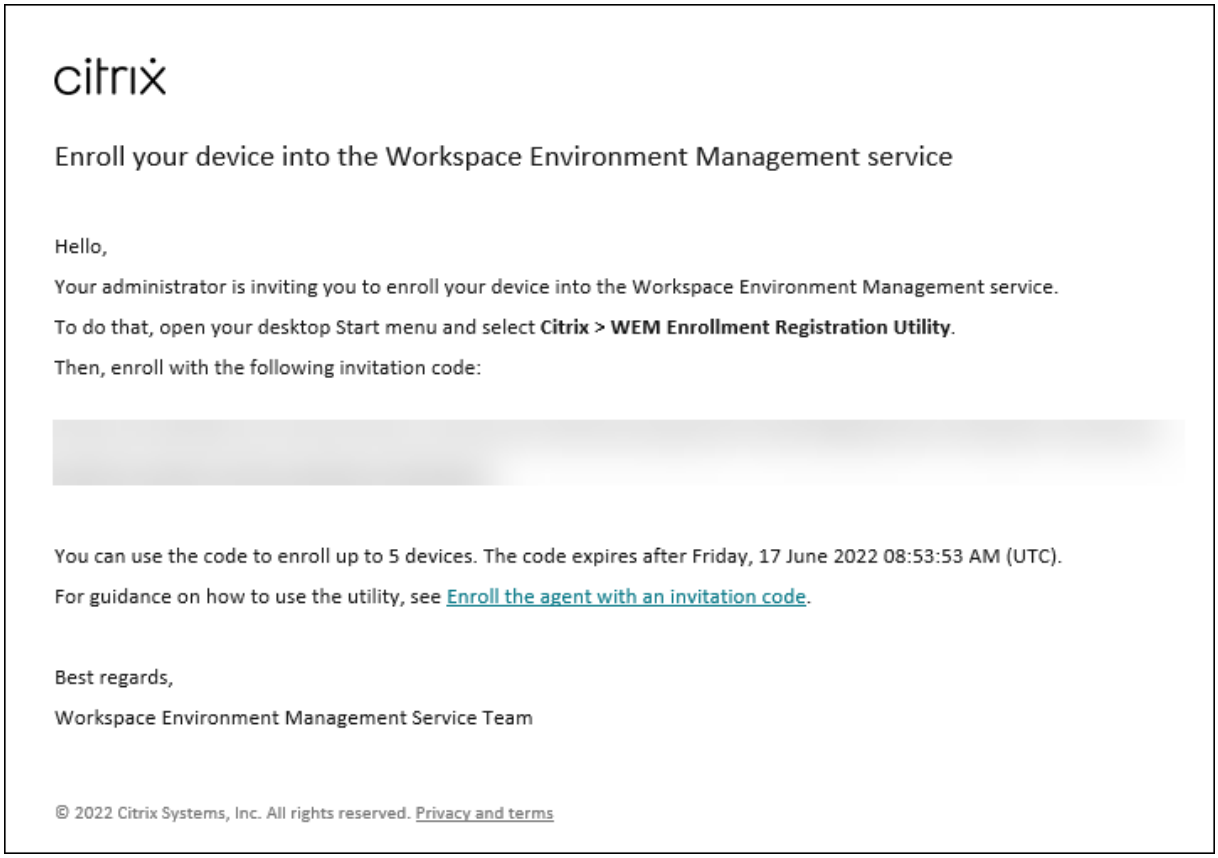
1. In the action bar, select **Invite user**. The **Invite user** wizard appears.
2. Select an identity provider.
3. Select the domain of the users you want to add. Select **Users** and **Security groups** as needed.
4. In the **Select** box, enter the name of the user or the group you want to invite.

   > **Note:**
   >
   > The search returns only the top 50 results. Refine your search if necessary.

5. Select desired users or user groups from the list. Selected users and user groups are shown under **Search**.
6. After you have finished, click **Invite** to send the invitation.

The users will receive the following invitation email:

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



citrix

Enroll your device into the Workspace Environment Management service

Hello,

Your administrator is inviting you to enroll your device into the Workspace Environment Management service.

To do that, open your desktop Start menu and select **Citrix > WEM Enrollment Registration Utility**.

Then, enroll with the following invitation code:

You can use the code to enroll up to 5 devices. The code expires after Friday, 17 June 2022 08:53:53 AM (UTC).

For guidance on how to use the utility, see Enroll the agent with an invitation code.

Best regards,

Workspace Environment Management Service Team

© 2022 Citrix Systems, Inc. All rights reserved. Privacy and terms

If you have installed the enrollment key on the users'agents using the enrollment tool, no further action is required on your part. Your users need to complete the enrollment using the invitation code.

View the details of an invitation

To view details of an invitation, select the invitation and then select **View details** in the action bar. The **View details** window appears, displaying the following information:

- Invitation code
- Time when the invitation was created
- Expiration date
- Recipient —who received the invitation email
- Display name of the recipient
- Email address of the recipient
- Delivery status

  Possible values:

  - **Delivered**. Indicates that the invitation email was delivered to the user successfully.

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

- **Failed**. Indicates that attempts to send the invitation email failed.
- **Pending**. Indicates that the invitation email hasn't yet been delivered.

Resend an invitation

To resend an invitation, select the invitation and then select **Resend email** in the action bar.

This action does not extend the expiration time of the invitation code.

Delete an invitation

To delete an invitation, select the invitation and then select **Delete** in the action bar. You can delete multiple invitations at a time.

Deleting an invitation invalidates the invitation code sent to or shared with users. As a result, those users can't enroll their agents with the code.

Clear expired invitations

To delete all expired invitations, select **Clear expired invitations** in the action bar. The **Clear expired invitations** button appears only when there are expired invitations.

Access control

September 7, 2025

Role-Based Access Control (RBAC) in Workspace Environment Management™ (WEM) provides a structured way to delegate administration.

Setting up RBAC involves three steps:

1. **Designate roles:** In Citrix Cloud, assign each administrator a role —either WEM > Full administrator (unrestricted access) or WEM > Restricted administrator (limited access based on scopes). For more information, see Manage administrator permissions.
2. **Define scopes:** In the **Access control** node of the WEM web console, define scopes for restricted administrators. For more information, see Create a scope.
3. **Assign scopes:** In the **Access control** node of the WEM web console, assign scopes to restricted administrators to apply the associated access policies and permissions. For more information, see Assign scopes to a restricted administrator.

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

About the Access control node

The **Access control** node is where you implement RBAC by defining what restricted administrators can access and how they can interact with WEM resources.

With this node, you can:

- Define and assign **Scopes** to limit which resources (such as configuration sets, scripted tasks, and app packages) restricted administrators can manage.
- Delegate scopes and role types (**Read-only admin** or **Read/write admin**) to restricted administrators while protecting critical resources and reducing operational risk.

> **Note:**
>
> Only administrators who have the **Full administrators** role for WEM can access this node.

View WEM administrators

To view all WEM administrators (full or restricted), follow these steps:

1. Go to **Access control > Administrators**. The Administrators list appears with all WEM administrators (full or restricted).
2. To check an administrator's role type, use the **Search box** to find them by name or email.
3. To sync the list with **Citrix Cloud™ > Identity and Access Management > Administrators**, click **Refresh**.

> **Note:**
>
> To add or remove WEM administrators, or to change a WEM administrator's role type (full or restricted), go to **Citrix Cloud > Identity and Access Management > Administrators** using a user account with **Full Access**:
>
> - To assign a user the WEM **Full administrator** role, select **Custom Access > Workspace Environment Management > Full Administrator**.
> - To assign a user the WEM **Restricted administrator** role, select **Custom Access > Workspace Environment Management > Restricted Administrator**.
>
> For more information, see Manage administrator permissions.

Create and manage scopes

A scope is a collection of WEM resources, including configuration sets, scripted tasks, and app packages. Scopes help you organize resources and control which administrators can access and manage them.

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

The **Scopes** page gives you a centralized view of all scopes in your environment. You can create, edit, view, or delete scopes:

- **Search**: Filter scopes by name or description.
- **Create scope**: Add a resource collection.
- **Refresh**: Update the list of scopes.
- **Administrator** icon: View which administrators are assigned.
- **Menu (…)** icon: View, edit, or delete a scope. (**Shared scopes** can't be edited or deleted.)

WEM provides a built-in **Shared scope** that includes shared resources such as WEM cloud agent packages and built-in scripts. This scope is always available to all restricted administrators in *read-only* mode and can't be edited or deleted.

Create a scope

1. Go to **Access control > Scopes**.
2. Click **Create scope**.
3. On the **Basic information** page, enter a name and (optionally) a description, and click **Next**.
4. On the **Resources** page, select which WEM resources to include from the **Configuration sets**, **Scripted tasks**, and **App packages** lists. Use these filters to narrow a list:
   - **Show all**: Displays all resources.
   - **Show available only**: Displays resources not yet assigned to a scope.
   - **Show selected only**: Displays the resources that you've chosen.
5. Click **Done**.

View or edit a scope

1. In **Scopes**, search for the scope by name or description.
2. Click the **Menu (…)** icon at the end of the row, and select **View** or **Edit**.
3. Review or update the information on the **Basic information** and **Resources** pages.
4. Click **Save**.

Delete a scope

1. In **Scopes**, select the scope.
2. Click the **Menu (…)** icon at the end of the row, click **Delete**.

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

> **Note:**
>
> If the scope is already assigned to restricted administrators, deleting it immediately impacts their access.

Assign scopes to a restricted administrator

To control which collections of WEM resources a restricted administrator can manage, follow these steps:

1. Go to **Access control > Administrators**.
2. Locate a restricted administrator by name or email.
3. Click the **Manage access** icon at the end of the row.
4. On the **Manage administrator access** page that appears, do the following actions:
    - Select one or more existing scopes.
    - Click **Create scope** to define a new collection of resources. For more information, see Create a scope.
5. Select the role type:
    - **Read-only admin**: The administrator can only view resources in the scope.
    - **Read/Write admin**: The administrator can view and manage resources in the scope.
6. Click **Done**.

> **Note:**
>
> Restricted administrators always have read-only access to the built-in **Shared scope**.

Manage non-domain-joined machines

September 7, 2025

You can use Workspace Environment Management (WEM) to manage non-domain-joined machines in Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure) deployments.

This feature enables you to assign policies and settings to non-domain-joined machines as you do with domain-joined machines.

A general workflow to get started with managing non-domain-joined machines is as follows:

1. In Azure, prepare a master image that has a Citrix VDA and a WEM agent.

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

2. Import that image from Azure for use with catalog creation. For more information, see Master images.

   > **Important:**
   >
   > - For this feature to work, you must use WEM agent version 2103.2.0.1 or later. Download the WEM agent from the WEM service's **Utilities** tab.
   > - For this feature to work, you must select **Skip Configuration** when installing the agent.
   > - By design, the agent running on the virtual machine that is used to create the image cannot connect to the WEM service.

3. In Citrix DaaS Standard for Azure, create a non-domain-joined catalog. For more information, see Create catalogs.
4. In the legacy console, add non-domain-joined machines to a WEM configuration set.

   a) Go to the **Administration Console > Active Directory Objects > Machines** tab, click the down arrow next to **Add Object**, and then select **Add Non-Domain-Joined Computers**.

   b) In the **Add-Non-Domain-Joined Computers** window, select one or more non-domain-joined machines that you want to add to the configuration set. The list displays only non-domain-joined machines that have not yet been added to any configuration sets.

   c) Click **Add** to add the selected machines and to exit the **Add-Non-Domain-Joined Computers** window.

5. Optionally, verify that those machines are registered with the WEM service. To do that, navigate to the **Administration Console > Administration > Agents > Statistics** tab, double-click a machine you added and then confirm registration information in the **Agent Information** window.

   > **Important:**
   >
   > Non-domain-joined agent machines automatically register with the WEM service and are added to the default configuration set.

After adding non-domain-joined machines to the WEM service, you can assign policies and settings to those machines as you do with domain-joined machines. However, when you assign policies and settings in the case of non-domain-joined machines, you have only the **Everyone** assignment option.

Manage Basic Deployment agents

May 13, 2026

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

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 back-end components such as broker, database, and consoles.

Configuring the basic deployment agent settings

When the 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 the 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
enableCpuAutoPrevention	boolean	Automatically prevent CPU spikes	true	true	
cpuUsageLimitOfSpikeProtection	int	CPU usage limit (%)	70.0	70.0	
enablePerCoreCpuUsageLimit	boolean	Set limit relative to single CPU core	false	false	
perCoreCpuUsageLimitOfSpikeProtection	int	CPU usage limit relative to single CPU core (%)	80.0	80.0	
cpuUsageLimitSampleTimeOfSpikeProtection	int	CPU usage limit (sec)	30	30	

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

Property	Type	Setting	Default	Example	Note
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	
excludeProcessesFromCpuSpikeProtection	boolean	Exclude processes from CPU spike protection	false	false	
processesExcludedFromCpuSpikeProtection	array of strings	Process names	[]	[“devenv”, “msbuild”]	
disableProcessPriorityInheritance	boolean	Prevent child processes from inheriting CPU priority	false	false	
parentProcessesToDisableProcessPriorityInheritance	array of strings	Process names	[]	[“devenv”, “msbuild”]	
enableMemoryWorkingSetOptimization	boolean	Optimize memory usage for idle processes	false	true	Memory optimization settings
idleSampleTimeOfMemoryWorkingSetOptimization	integer	Idle time (min)	30	30	
idleStateLimitOfMemoryWorkingSetOptimization	integer	Idle state limit (%)	1	1	

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

Property	Type	Setting	Default	Example	Note
enableMemoryOptimization	boolean	Restrict optimization	true	true	
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	false	true	Fast Logoff settings
enableMultiSessionOptimization	boolean	Enable multi-session optimization	false	true	Multi-session optmizations
excludeProcessesFromMultiSessionOptimization	boolean	Exclude processes from multi-session optimization	false	false	
processesExcludedFromMultiSessionOptimization	array of strings	Process names	[]	[“devenv”, “msbuild”]	
agentServiceDebugModeEnabled	boolean	Enable agent service debug mode	false	false	**Advanced settings > Agent settings > Agent service options**

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

Property	Type	Setting	Default	Example	Note
enableLogonDurationAnalysis	boolean	Enable logon duration analysis	true	true	Logon duration analysis
useAlternativeLocalReportLocation	boolean	Use an 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 reports to be kept	30	30	
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	

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

Property	Type	Setting	Default	Example	Note
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	

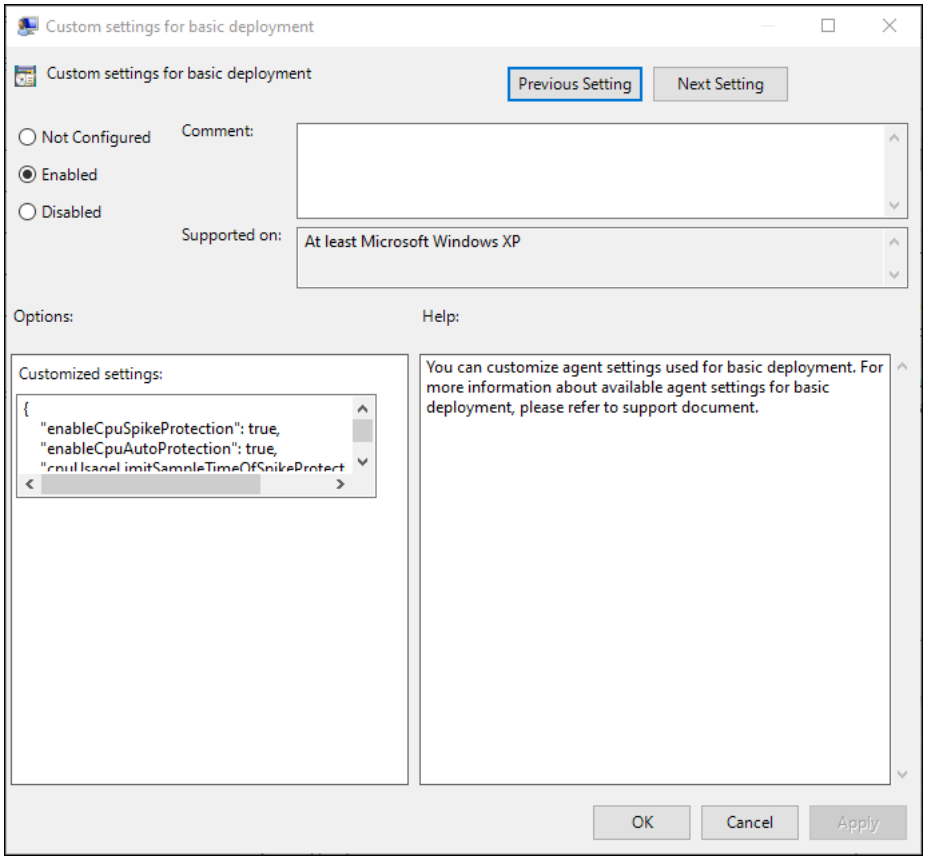
> **Note:**
>
> If the custom settings are not configured or are invalid, the WEM agent uses the default settings.

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.
- You can use Citrix Environment Tool Hub to check the agent-generated report.

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

Upload files

September 7, 2025

> **Note:**
>
> This article applies to uploading files when using the legacy console.

You can use **Upload** to upload files you want to import or add to the Workspace Environment Management™ administration console. The **Upload** option is available in the menu on the WEM service **Manage** tab.

This feature is useful in scenarios where you want to:

- Use the **Restore** wizard to restore your WEM settings to WEM service. Those settings include:
  - Security settings
  - AD objects
  - Configuration set

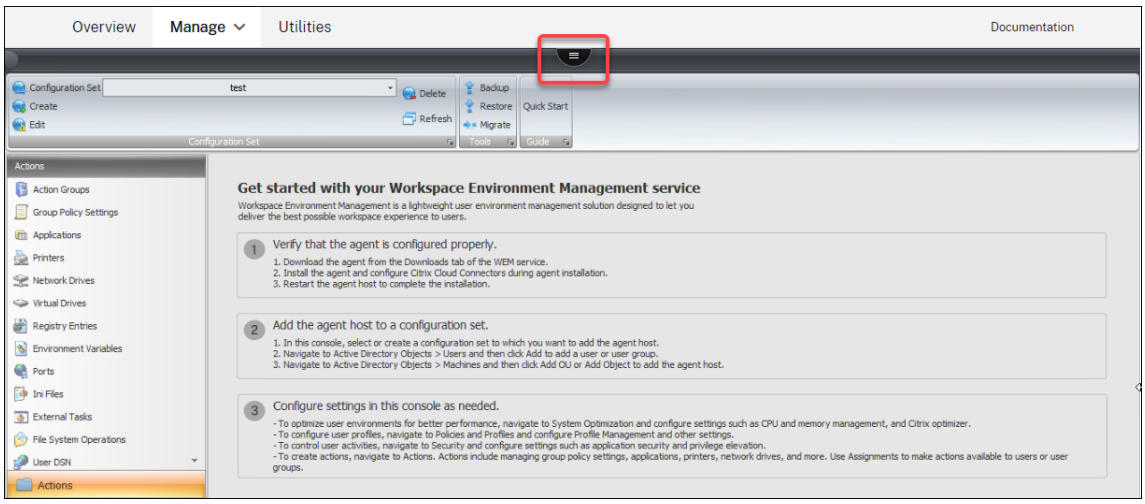
  For more information, see Ribbon.
- Use the **Migrate** wizard to migrate a zip backup of your Group Policy Objects (GPOs) to WEM service. For more information, see Ribbon.
- Import your registry files. For more information, see Registry Entries.
- Add custom icons for your applications. For more information, see Applications.

The files you upload are saved to the default folder (*DefaultUploadFolder*) in Citrix Cloud.

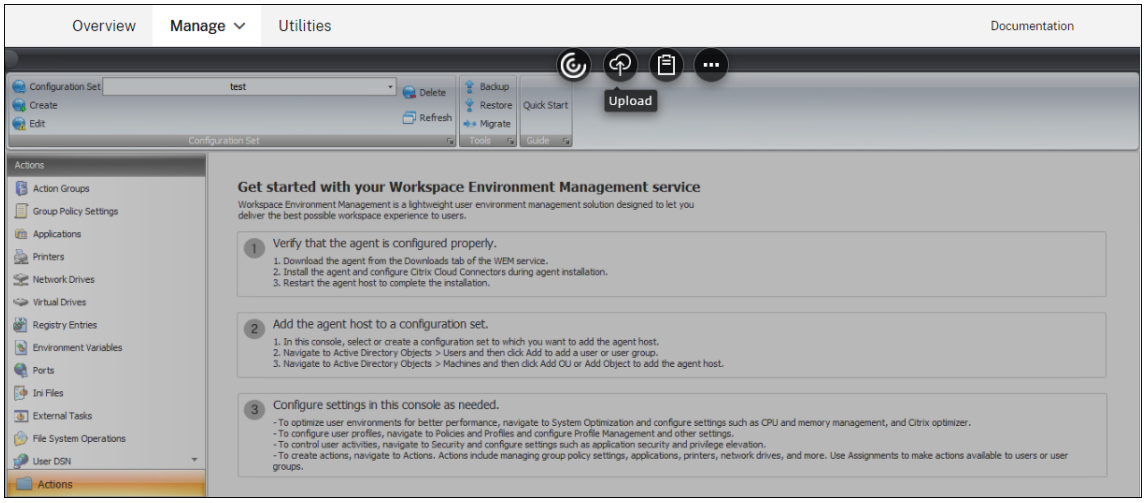
To upload a file, complete the following steps:

1. In **Manage > Legacy Console**, hover over the hamburger menu and then click the Citrix Workspace™ app icon.

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



2. Click **Upload** to upload the file to the default folder in Citrix Cloud.



Keep the following limitations in mind when using this feature to upload your files:

- **File count limit**. This feature supports uploading multiple files at a time. By default, it supports storing up to 10 files *for every account*. Uploaded files are handled on a first-come, first-deleted basis.
- **File size limit**. By default, you can upload only files whose size is smaller than 5 MB.
- **File sync interval**. By default, this feature synchronizes uploaded files to the Azure storage every 30 minutes.

If you want to change the defaults, contact Citrix Technical Support.

When you attempt to add or restore the uploaded files to the administration console for the first time after an upgrade, you might find that they are not available for use. The issue might also occur the first time you use the console. Possible causes:

- Those files have not yet been downloaded from the Azure storage. Downloading them to the

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

administration console can take some time to complete. Exit the administration console and try again later.
- An error might occur while downloading those files. If the problem persists, contact Citrix Technical Support.

REST APIs

August 7, 2026

With the Workspace Environment Management™ (WEM) service REST APIs, you can automate the management of resources within a WEM deployment.

The API service does not require you to sign in to the WEM administration console to call the services.

Currently, the following API categories are supported:

- **Machine AD Object APIs**: a set of APIs for managing your machine-level AD objects within a WEM deployment.
- **Site APIs**: a set of APIs for managing your configuration sets within a WEM deployment.
- **System Optimization APIs:** a set of APIs for managing and optimizing resources (for example, CPU, memory, and I/O) of Windows devices within a WEM deployment.
- **User AD Object APIs:** a set of APIs for managing your user-level AD objects within a WEM deployment.

The WEM service APIs are available at https://developer-docs.citrix.com/en-us/workspace-environment-management/workspace-environment-management-rest-apis/overview. It contains everything you need to configure access to the API service and use those APIs to manage and optimize the resources.

Accelerate logon performance using Citrix Environment Tool Hub and WEM

November 4, 2025

To accelerate slow Windows logon times, you can migrate those time-consuming Group Policy Preferences (GPP) settings to Citrix Workspace Environment Management (WEM). This article guides you

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

through using the Citrix Environment Tool Hub to export these configurations and import them to WEM for optimized performance.

For more information about identifying specific Group Policy settings that cause slow logons, see Troubleshoot Login Time Issues Using Citrix Environment Tool Hub and WEM.

Prerequisites

Before you begin, make sure that you have:

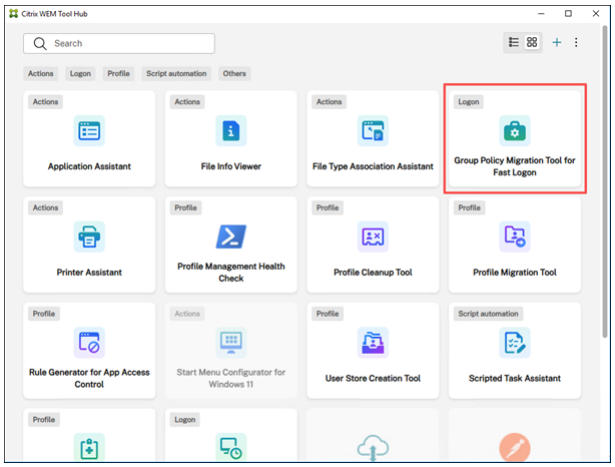
- Administrator privileges on the target Windows machine
- Domain administrator privileges on the Domain Controller (DC)
- Administrator privileges on the WEM Web Console

Migrate time-consuming Group Policy Preferences

To improve logon performance, migrate time-consuming GPP settings from Group Policy to WEM. Complete the following steps in sequence.

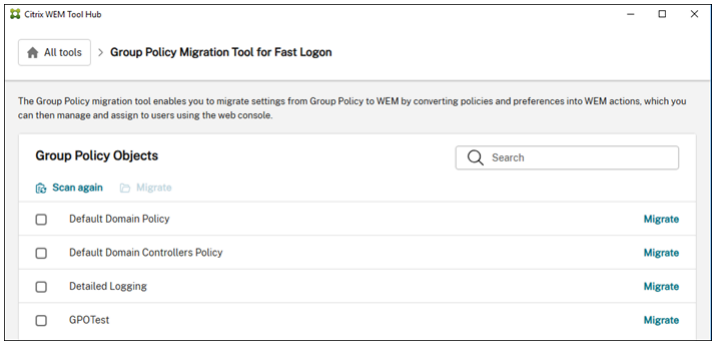
Step 1: Export GPP settings from the target Windows machine

1. Log on to the target Windows machine with administrator privileges.
2. Open **Citrix Environment Tool Hub > Group Policy Migration Tool for Fast Logon**.

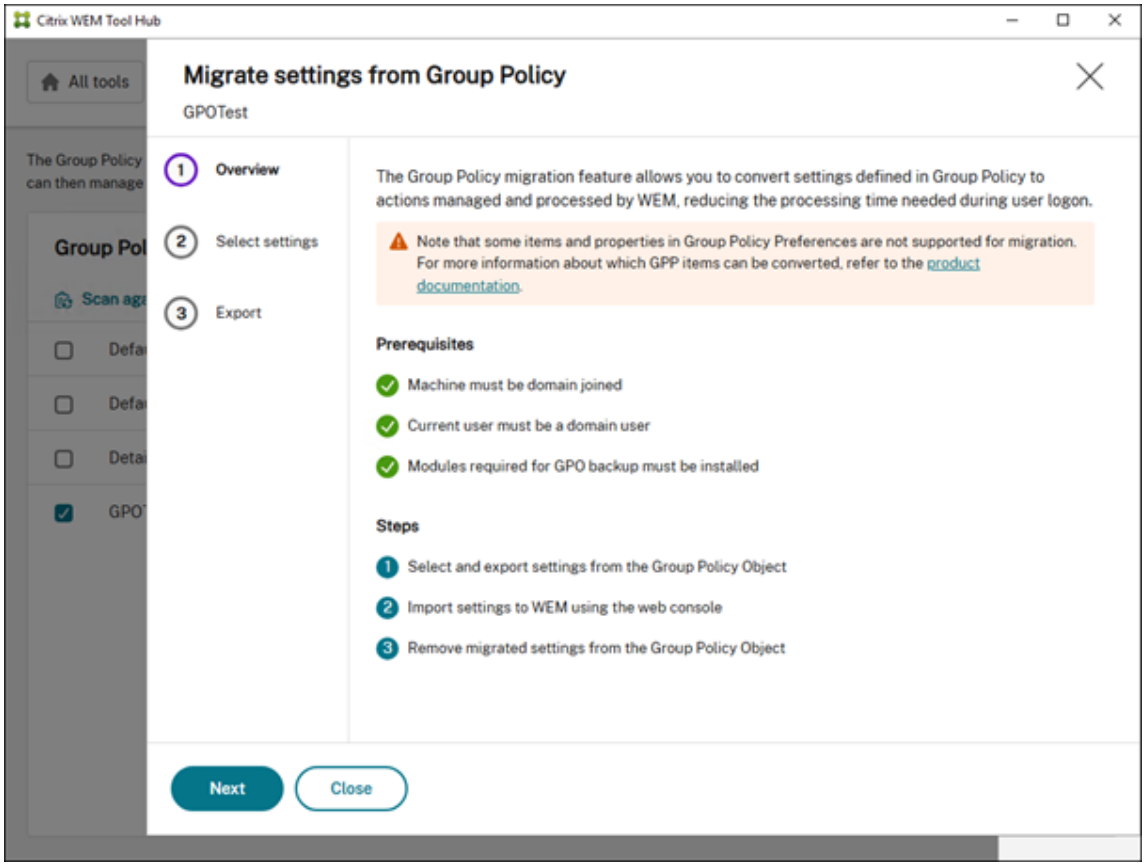


3. Click **Scan for Group Policy Objects**.
4. Select the Group Policy Objects you want to migrate, and then click **Migrate**.

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



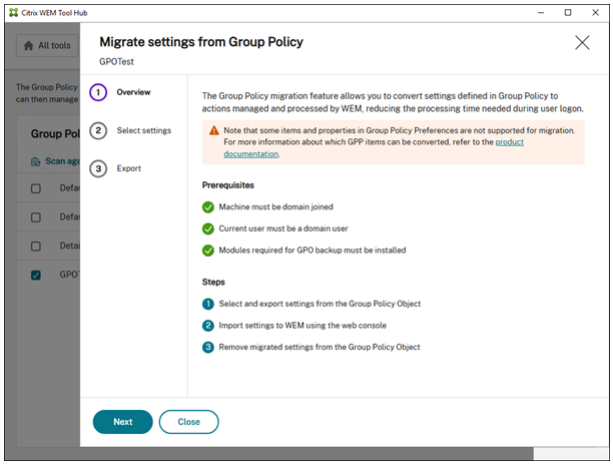
The Migration settings wizard appears.



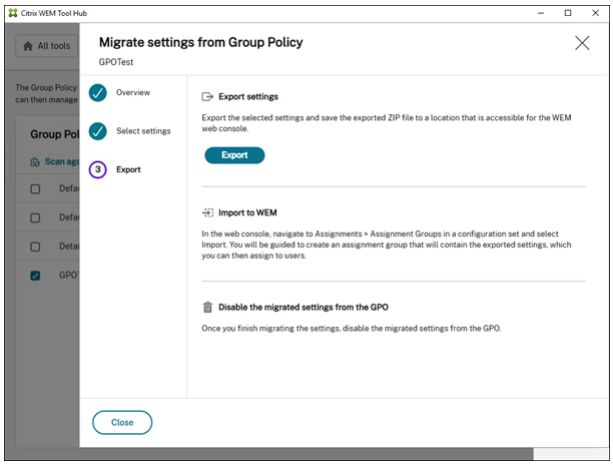
> **Note:**
>
> If prompted, install the required modules for GPO backup.

5. Select the settings that you want to migrate, and then click **Next**.

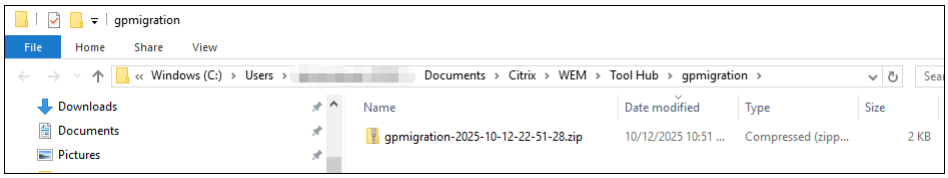
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Export** to back up the selected settings to a local `.zip` file.



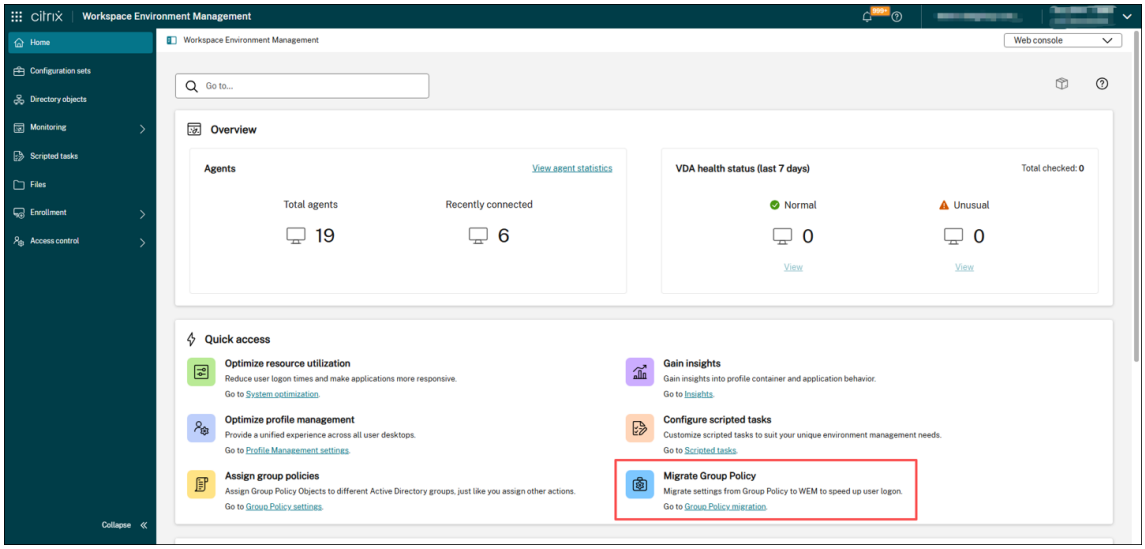
Export result:



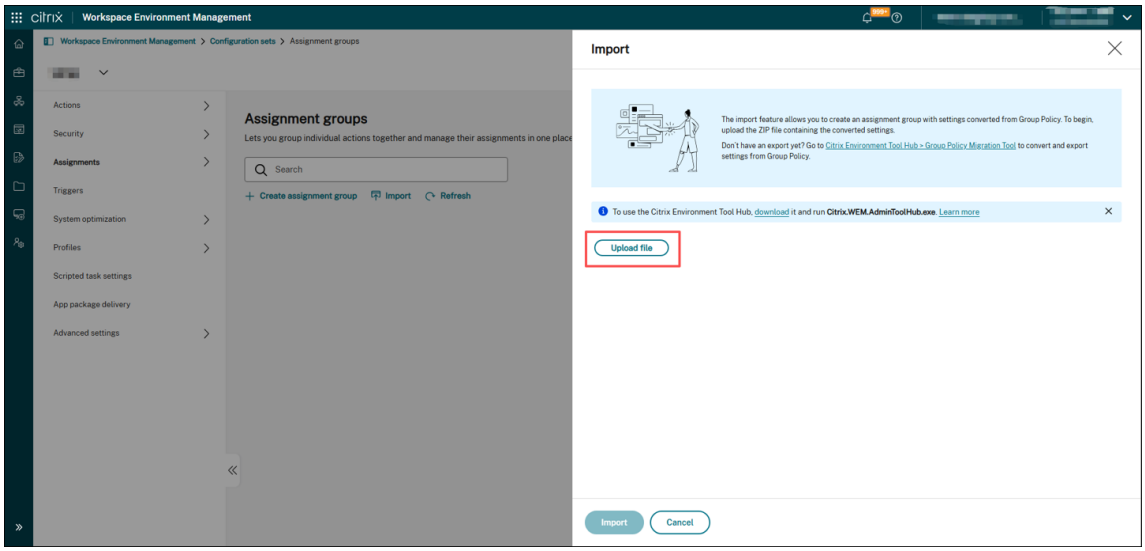
Step 2: Import GPP settings to the WEM Web Console

1. Launch the **WEM Web Console** with the WEM **Full Administrator** role. In the **Quick access** area, click **Migrate Group Policy**, and then select the appropriate configuration set.

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

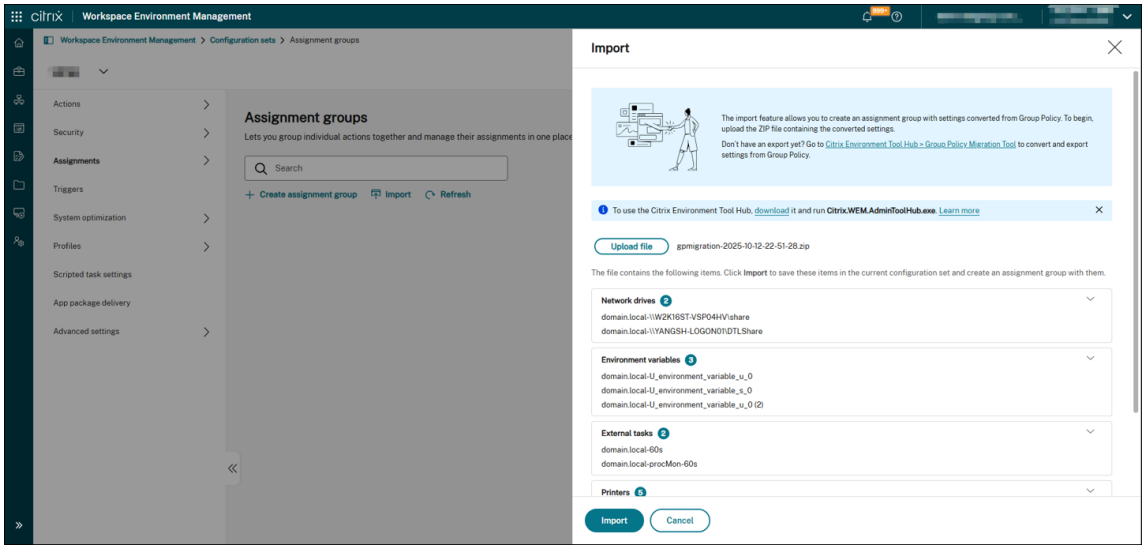


2. Click **Upload file** to upload the exported `.zip` file.

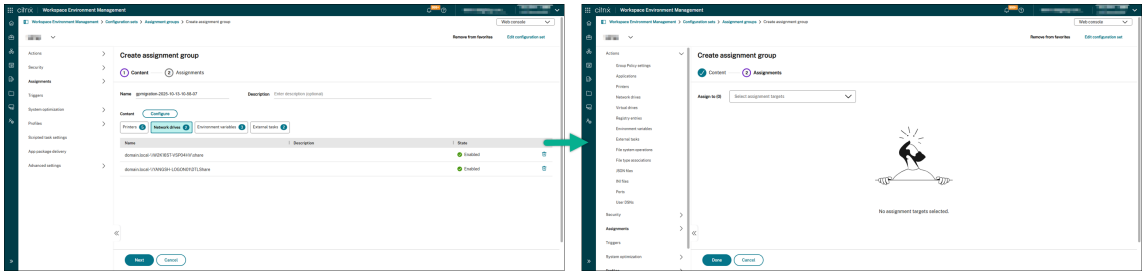


3. Review the settings, and then click **Import**.

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



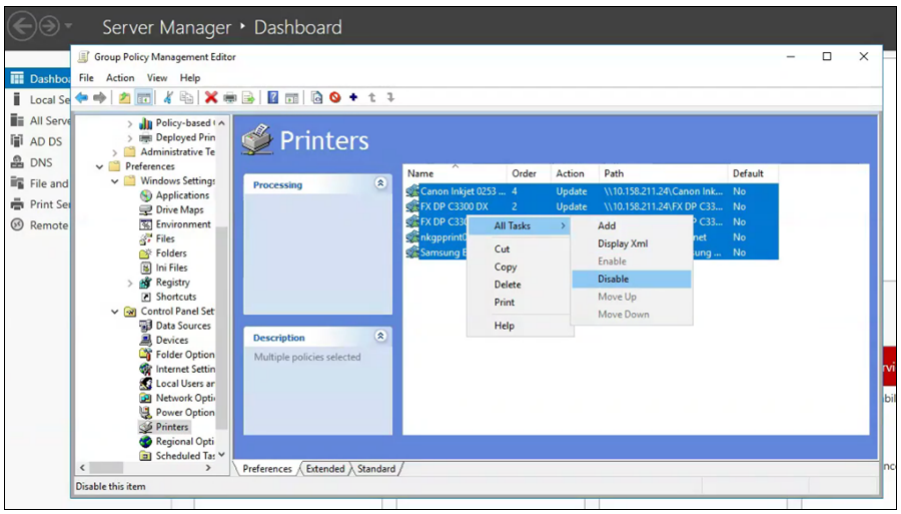
4. Click **Next** to configure the assignment targets.



5. Click **Done** to complete the import process.

Step 3: Disable migrated GPP settings in the Domain Controller

1. Log on to the Domain Controller with administrator privileges.
2. Disable all configurations that correspond to the migrated settings.



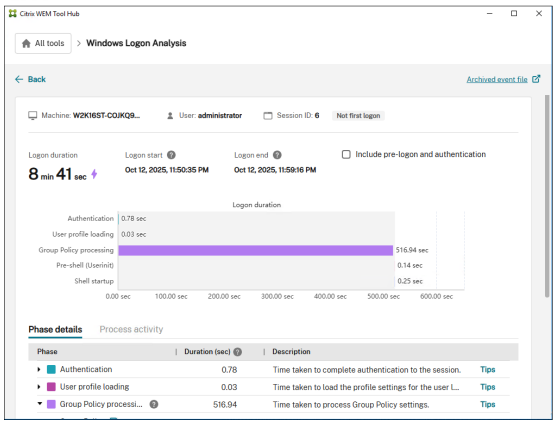
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> Disable only the settings that were successfully migrated to WEM to prevent disrupting user functionality.

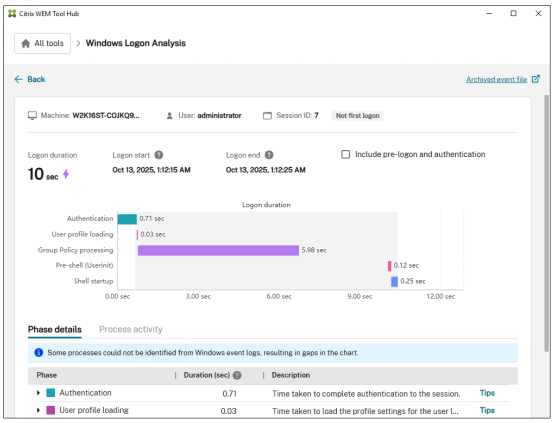
Step 4: Re-log on and verify results

1. Log off and then log on again.
2. Use the **Windows Logon Analysis** tool to collect logon times for each session.
3. Compare logon times before and after migration to confirm performance improvements.

Before



After



> **Note:**
>
> The comparison results shown above are environment-specific and provided for reference only.

For more information about identifying specific Group Policy settings that cause slow logons, see Troubleshoot Login Time Issues Using Citrix Environment Tool Hub and WEM.

Aggregate assigned applications in one place

September 7, 2025

As an administrator, you might want to aggregate all applications you assigned to your user in one place for quick and convenient launch. Also, your users might prefer to directly open their bookmarked websites rather than take additional steps —open the browser first and then access the websites.

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

Workspace Environment Management (WEM) provides an application launcher tool that lets users launch assigned applications in one place and directly open bookmarked websites using a browser (if assigned). For more information about the tool, see Application launcher.

A general workflow to use the tool is as follows:

1. As an administrator, assign applications to target users or user groups through the administration console.
2. Users log on to the agent machine to launch applications using the tool.

Prerequisites

Before you use the tool, keep the following in mind:

- Make sure that the assigned applications are present on the agent machine. Only applications present on the agent machine appear in the application launcher window.
- This feature supports only Google Chrome and Microsoft Edge. For the browser bookmark feature to work, make sure that Google Chrome or Microsoft Edge is present on the agent machine.

Recommendation

The tool can run independently as part of WEM. For best user experience, we recommend that you do the following:

- **Publish the tool as a Citrix virtual app**. When used as a published app in Citrix Workspace™, the tool launches assigned applications faster and makes it convenient for users to open bookmarked websites. If used otherwise, the browser bookmark feature does not work.
- **Use the tool with Citrix Profile Management**. Application launcher lets users mark assigned applications as favorites. When used with Profile Management, users' favorites and browser bookmarks can roam regardless of which machine they log in to.

Assign applications (as an administrator)

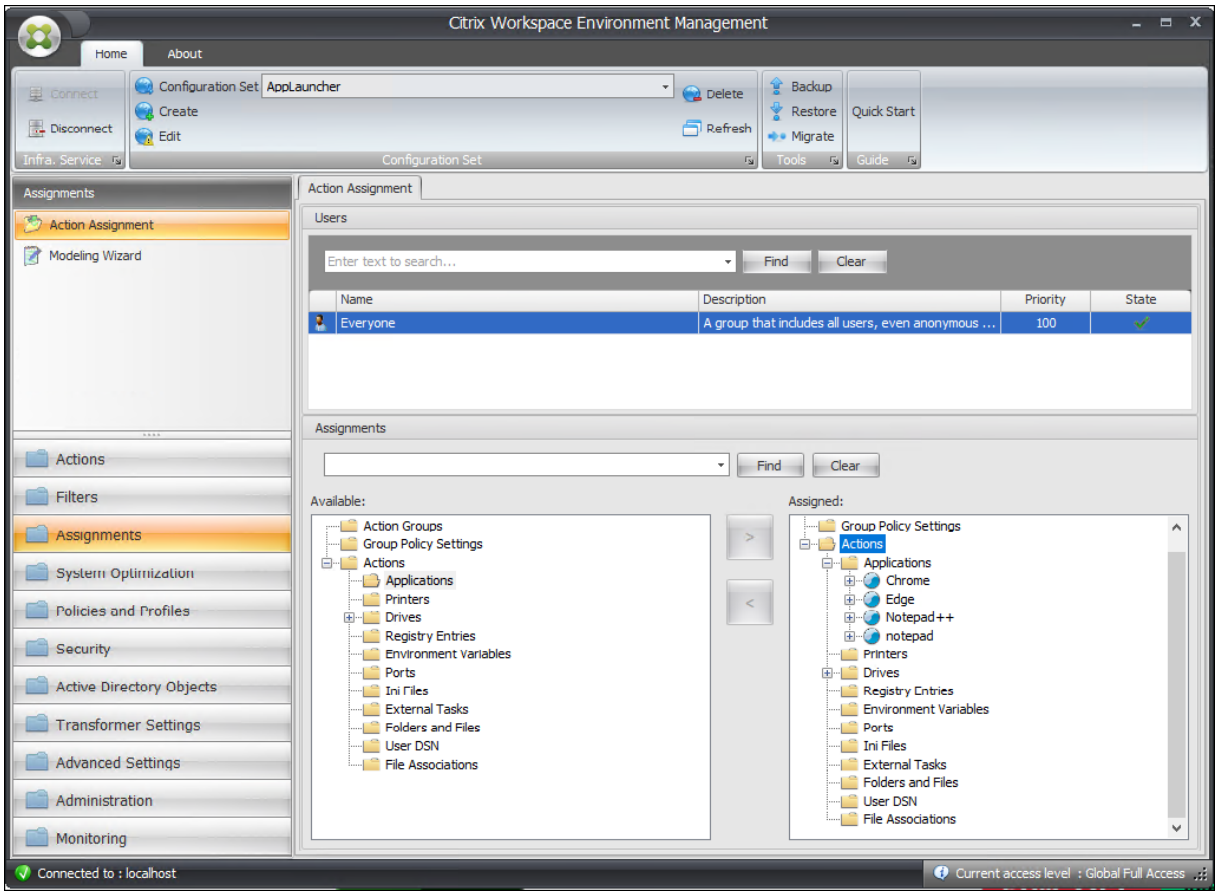
The following information is supplemental to the guidance in Action assignment. To assign applications, follow the general guidance in that article.

In this example, the following applications are assigned:

- Chrome
- Edge

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

- Notepad++
- notepad



Launch applications using the tool (as users)

After users log on to their agent machines, they can launch the application launcher tool and then do the following:

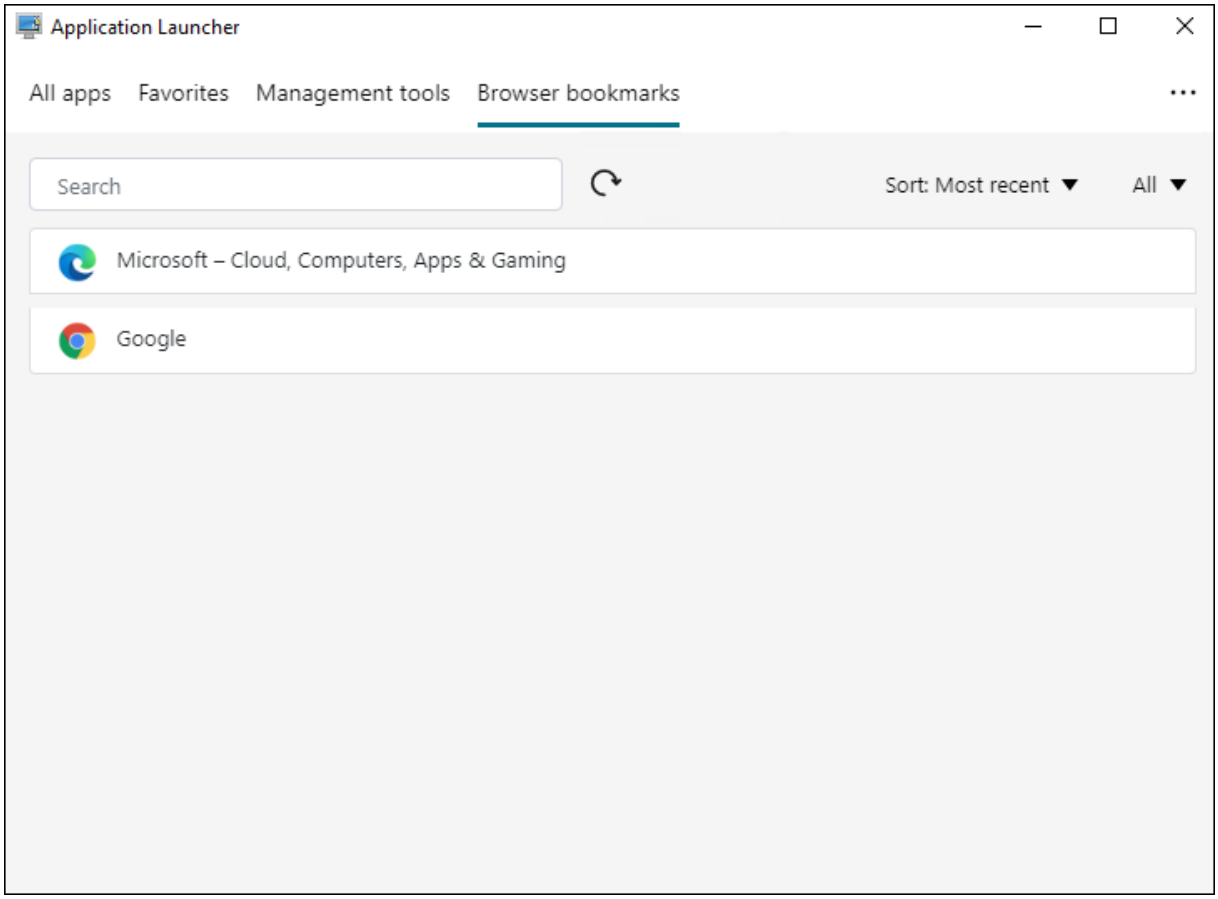
- Open assigned applications
- Favorite applications
- Launch management tools
- Access bookmarked websites
- Sign out of the current session

For more information, see Application launcher.

The following information is supplemental to the Application launcher article. Follow the general guidance in that article and mind details below.

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

Users can directly open bookmarked websites. The browser bookmarks feature provides a faster and more convenient way to open bookmarked websites.



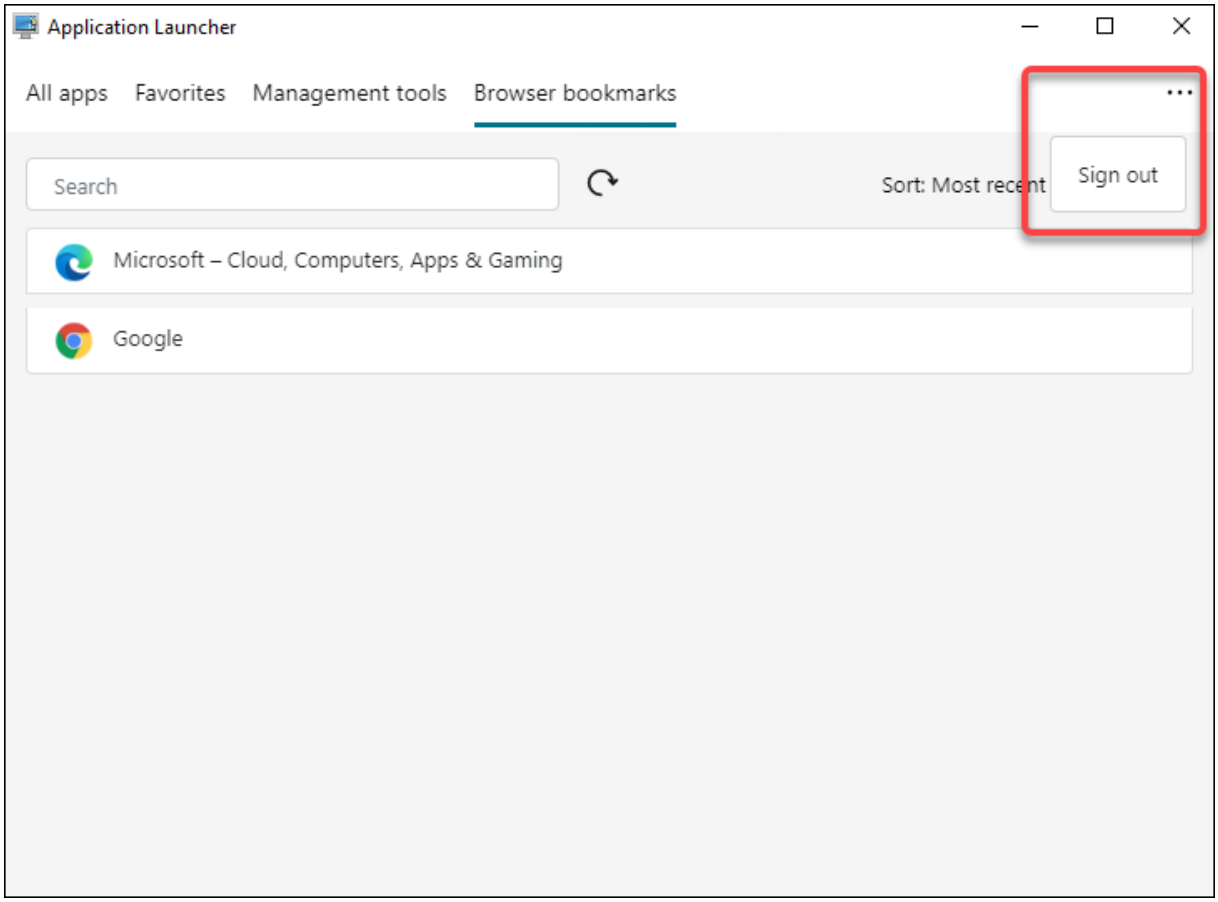
To add bookmarks, users open the assigned browser using application launcher, access websites, and then bookmark them. The bookmarked websites then appear in **Browser bookmarks**.

To delete or modify bookmarks, users complete the following steps:

1. Open the browser or click a bookmarked website to open the browser.
2. Delete or modify bookmarks as needed.

To sign out of the current session, users click the ellipsis icon in the upper right corner and select **Sign out**.

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



Unlike closing the window, signing out ensures that the application session ends.

Analyze logon duration using scripted tasks

September 7, 2025

Long logon times decrease user productivity and result in a poor user experience. As an administrator, you might want to get a detailed overview of logon times to identify processes that cause slow logons so that you can take remedial action accordingly.

To achieve this goal, you can use the script `analyzeLogonDuration.ps1`. It is a PowerShell script that queries the event log for every major event relating to the logon process. The script offers the following benefits and more:

- It gives you a logon duration breakdown of a user's most recent logon.
- It displays all major sequential phases of the logon process and makes it easy to see which phase is slowing down the logon.
- It lets you check whether there is a delay between the end of one phase and the start of the next.

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

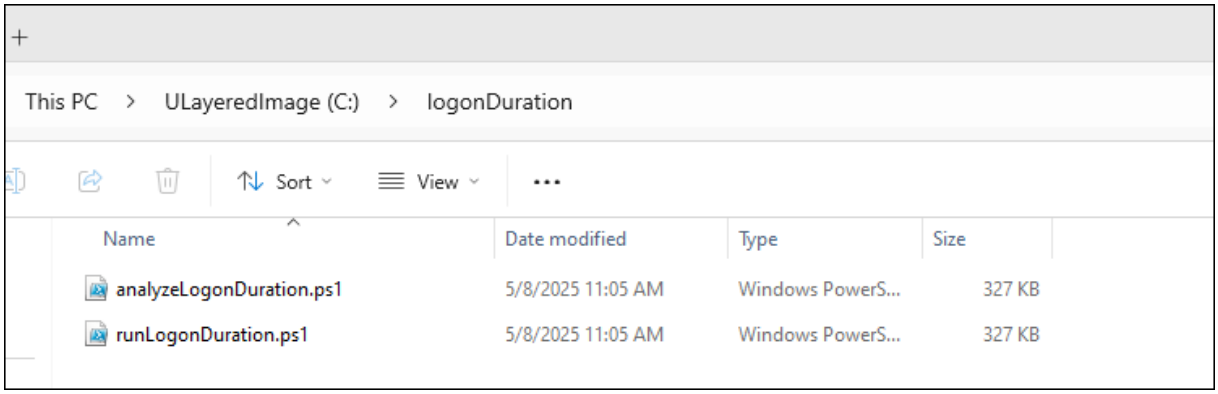
To see more benefits, go to https://www.controlup.com/script-library-posts/analyze-logon-duration/.

Workspace Environment Management™ (WEM) provides you with a scripted task feature that automates the running of the script for you. All you need to do is configure a scripted task. A general workflow is as follows:

1. Prepare relevant scripts.
2. Signature of the script is mandatory when the scripted task is granted full access.
3. Add a scripted task.
4. Configure the scripted task.
5. View the task execution report.

Prepare relevant scripts

Prepare a zip file that contains the following two scripts:



- `analyzeLogonDuration.ps1`. You can get this script from https://www.controlup.com/script-library-posts/analyze-logon-duration/.
- `runLogonDuration.ps1`. As the logon duration script requires the domain name and the username, we provide a wrapper script to pass the domain and user name to it. For example, we provide a way to get the domain name and the user name under the service account. But, this wrapper script requires one user session.

In this example, the script `runLogonDuration.ps1` contains the following content:

```
$User = tasklist /v /FI "IMAGENAME eq explorer.exe" /FO list | find "
    User Name:"
$User = $User.Substring(14)
$UserName = $User.Split("\")[1]
$DomainUser = "$env:userdomain\$UserName"
&.\analyzeLogonDuration.ps1  -DomainUser $DomainUser
```

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

Sign the script

The scripted task needs to run with full access. You need to add a signature for the entry point script: `runLogonDuration.ps1`. We recommend you use an official certificate, If you have an official certificate you can skip step 1 through step 3. If you don't have a certificate, you can use a Self-Signed SSL Certificate only for your test. Self-signed SSL Certificates are risky because they have no validation from a third-party authority, which is usually a Trusted SSL Certificate Company.

Step 1: Create a Self-Signed certificate

1. Open PowerShell as an Administrator. Right-click the **Start** button, and choose `Windows PowerShell (Admin)` or `Windows Terminal (Admin)`.
2. Use the `New-SelfSignedCertificate` cmdlet to create a self-signed certificate. Specify parameters like the certificate's name (friendly name), its validity period, and its usage (KeyUsage).

```
$cert = New-SelfSignedCertificate -Type CodeSigningCert -DnsName "
    MyTestCertificate.com" -CertStoreLocation "cert:\LocalMachine\My" -
    NotAfter (Get-Date).AddYears(10) -KeyUsage DigitalSignature -
    FriendlyName "MyTestCertificate"
```

This command creates a new certificate with one year validity and labels it as **MyTestCertificate**. This certificate is stored in the personal store of the local machine.

When the certificate is created successfully, the following details are displayed

```
PS C:\logonDuration>
PS C:\logonDuration>
PS C:\logonDuration> echo $cert


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
980CEB1DFC4FC9D29FDD755B918506BE721CE593  CN=MyTestCertificate.com
```

Step 2: Export the Self-Signed certificate

Export the certificate with a private key, if needed. To use the certificate for signing, you must export it with its private key. This is essential to use the certificate on another machine, or to safeguard the key. Run the following command:

```
$pwd = ConvertTo-SecureString -String "YourStrongPassword" -Force -
    AsPlainText
```

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

```
Export-PfxCertificate -cert $cert -FilePath "C:\MyTestCertificate.pfx"
    -Password $pwd
```

Replace **YourStrongPassword** with a strong password of your choice. This command exports the certificate to a `.pfx` file, which includes the private key.

Step 3: Install the certificate

If you have already exported the certificate and need to install it on the same or on a different machine, you can import it back into the certificate store. Copy the `*.pfx` file to the target machine, and then use the `Import-PfxCertificate` cmdlet.

```
$pwd = ConvertTo-SecureString -String "YourStrongPassword" -Force -
    AsPlainText

Import-PfxCertificate -FilePath "C:\MyTestCertificate.pfx" -
    CertStoreLocation "Cert:\LocalMachine\Root" -Password $pwd
```

Step 4: Sign a file using the certificate

If you use an official certificate, you need to input the right CN value. In this example, we use `MyTestCertificate.com`. To find the certificate, use the cmdlet:

```
$cert = ls Cert:\LocalMachine\Root| where {
 $_.subject -eq CN=MyTestCertificate.com" }
```

Use the `Set-AuthenticodeSignature` cmdlet to sign a PowerShell script or any other file that supports digital signatures.

```
Set-AuthenticodeSignature -FilePath "C:\logonDuration\runLogonDuration.
    ps1" $cert -IncludeChain all -HashAlgorithm SHA1 -TimestampServer
    http://timestamp.digicert.com
```

This command applies a digital signature to `runLogonDuration.ps1` using the certificate created earlier.

Step 5: Verify the signature

To verify that the file has been signed correctly, you can use the following command:

```
Get-AuthenticodeSignature -FilePath "C:\logonDuration\runLogonDuration.
    ps1"
```

If the script's signature is valid, the following details are displayed□

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

```
PS C:\logonDuration> Get-AuthenticodeSignature -FilePath "C:\logonDuration\runLogonDuration.ps1"

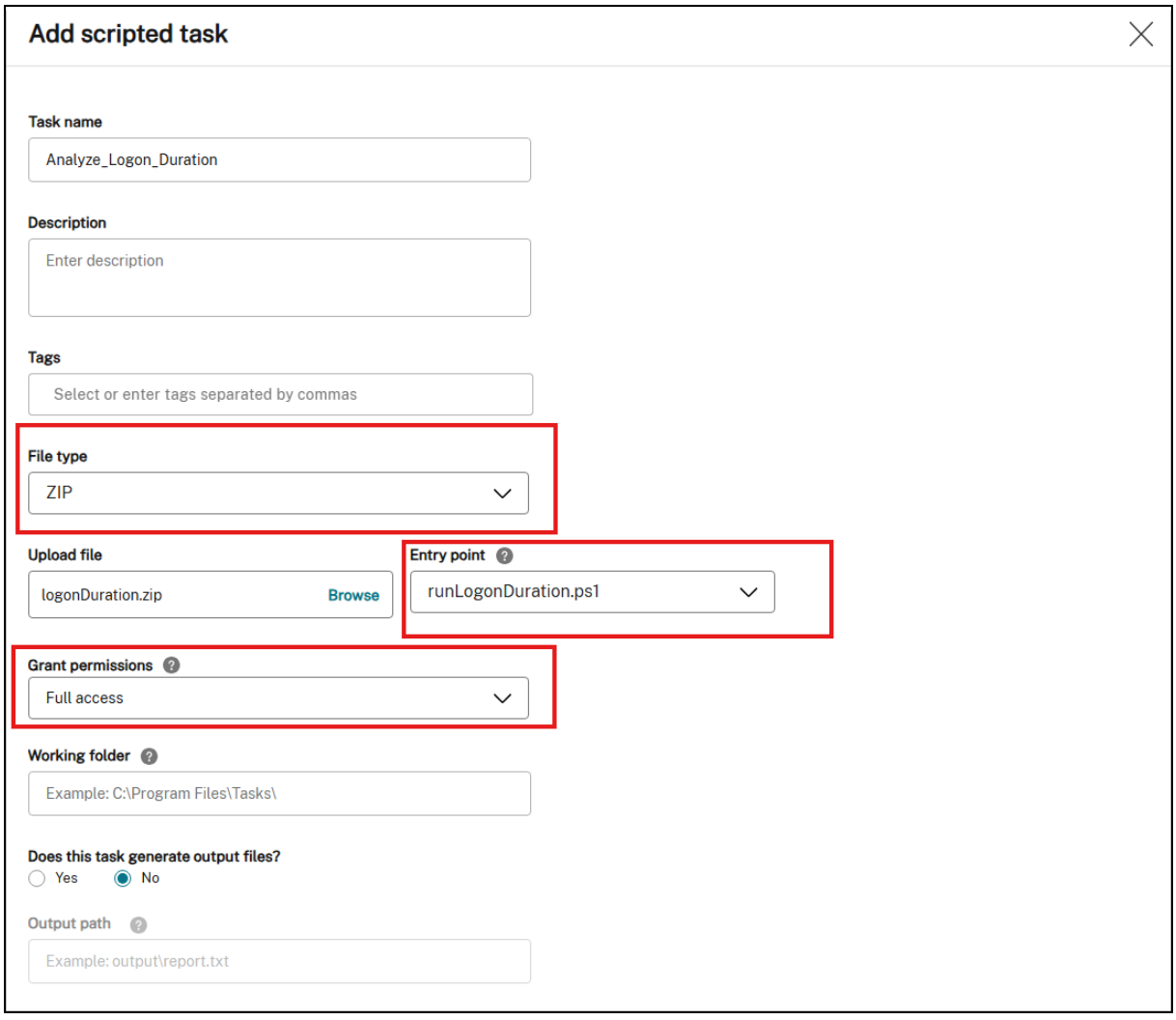

    Directory: C:\logonDuration


SignerCertificate                         Status                                                Path
-----------------                         ------                                                ----
980CEB1DFC4FC9D29FDD755B918506BE721CE593  Valid                                                 runLogonDuration.ps1
```

Add a scripted task

The following information is supplemental to the guidance in Add a scripted task. To create a task that analyzes logon duration, follow the general guidance in that article, minding the details below.

In **Web Console > Scripted Tasks**, add the task as follows:



- For **File type**, select **ZIP**.
- Create a zip file that contains the following two scripts.

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

    - `analyzeLogonDuration.ps1`
    - `runLogonDuration.ps1`

- Browse to the zip file to upload it and set the script `runLogonDuration.ps1` as the entry point.
- The **Grant permissions** option is designed to add an extra layer of security to protect against attacks originating from untrusted scripts, which might otherwise pose security risks. The Analyze_Logon_Duration task must run in full access.

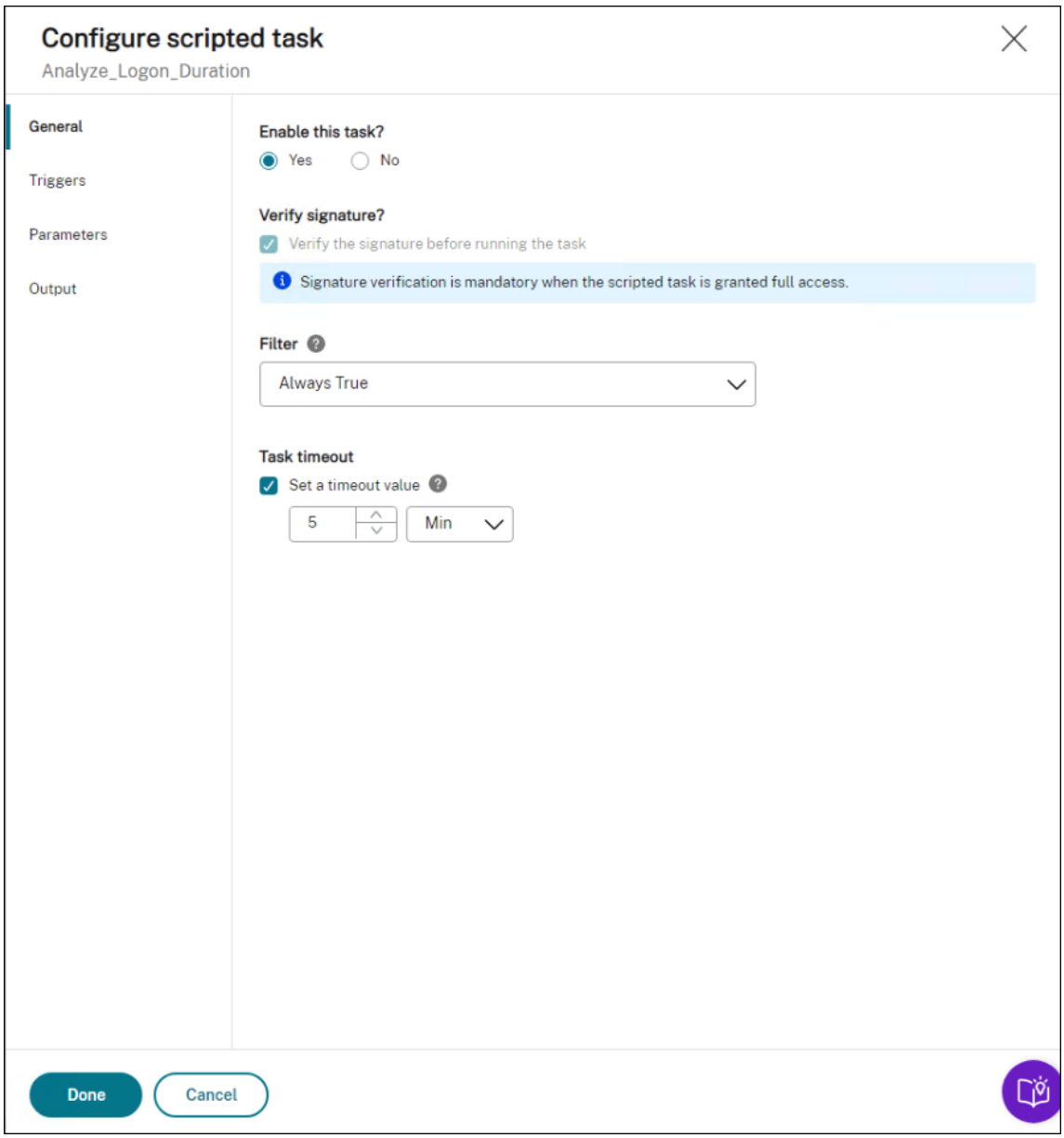
Configure the scripted task

The following information is supplemental to the guidance in Configure a scripted task. To configure the Analyze_Logon_Duration task, follow the general guidance in that article, minding the details below.

1. Go to the relevant configuration set, navigate to **Scripted Task Settings**, and configure the Analyze_Logon_Duration task in **General** as follows:

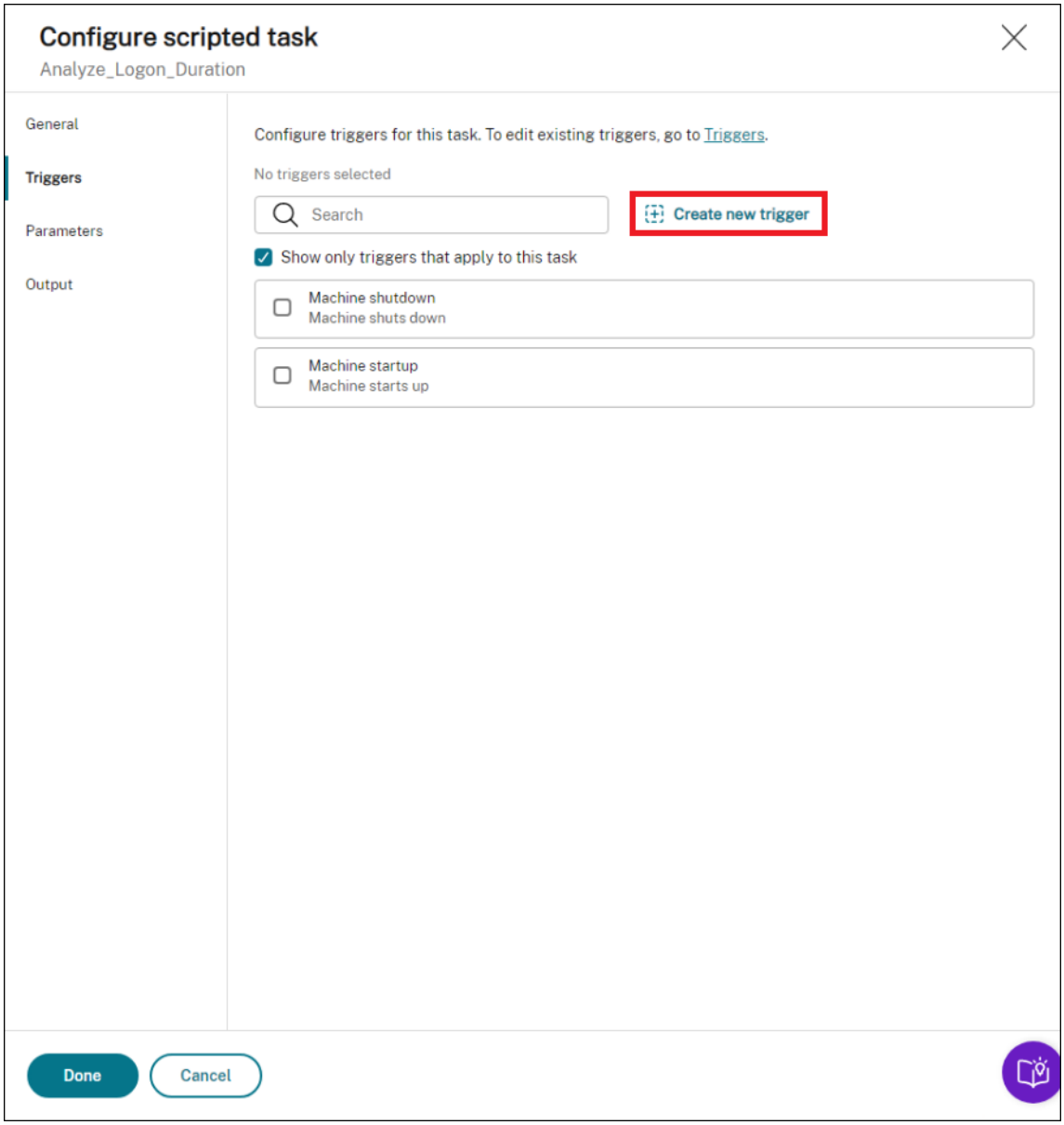
    - WEM lets you decide whether to verify the signature before running the task. Signature verification is mandatory when the scripted task is granted full access. This ensures security by protecting the scripts from being compromised. The **Filter** and **Task timeout** settings are optional.

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



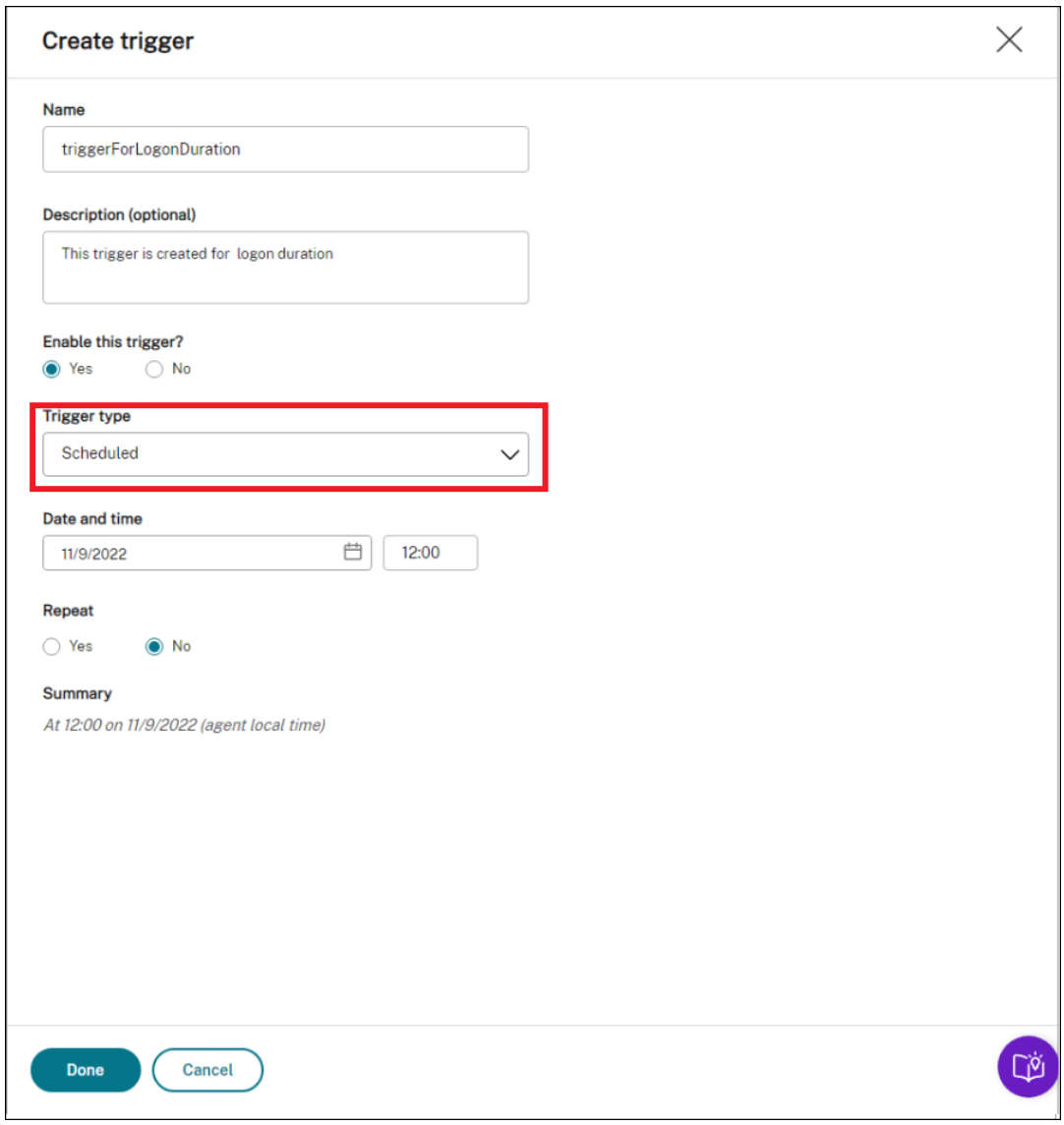
2. In **Triggers**, configure triggers for the task.

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

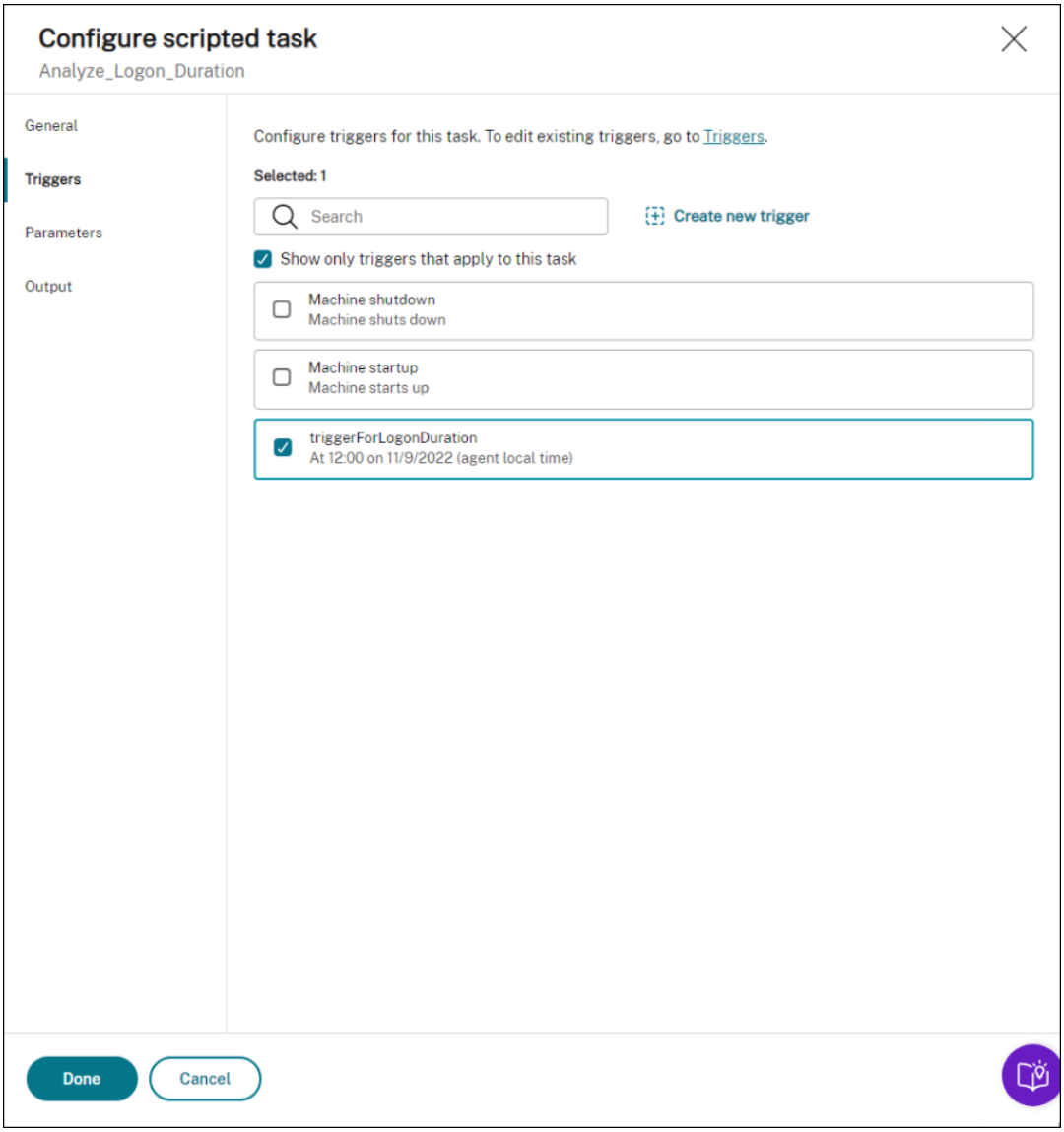


- Use triggers to control when to run the task. For example, you can create a "scheduled" trigger to schedule the running of the task and then associate the trigger with the task.

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



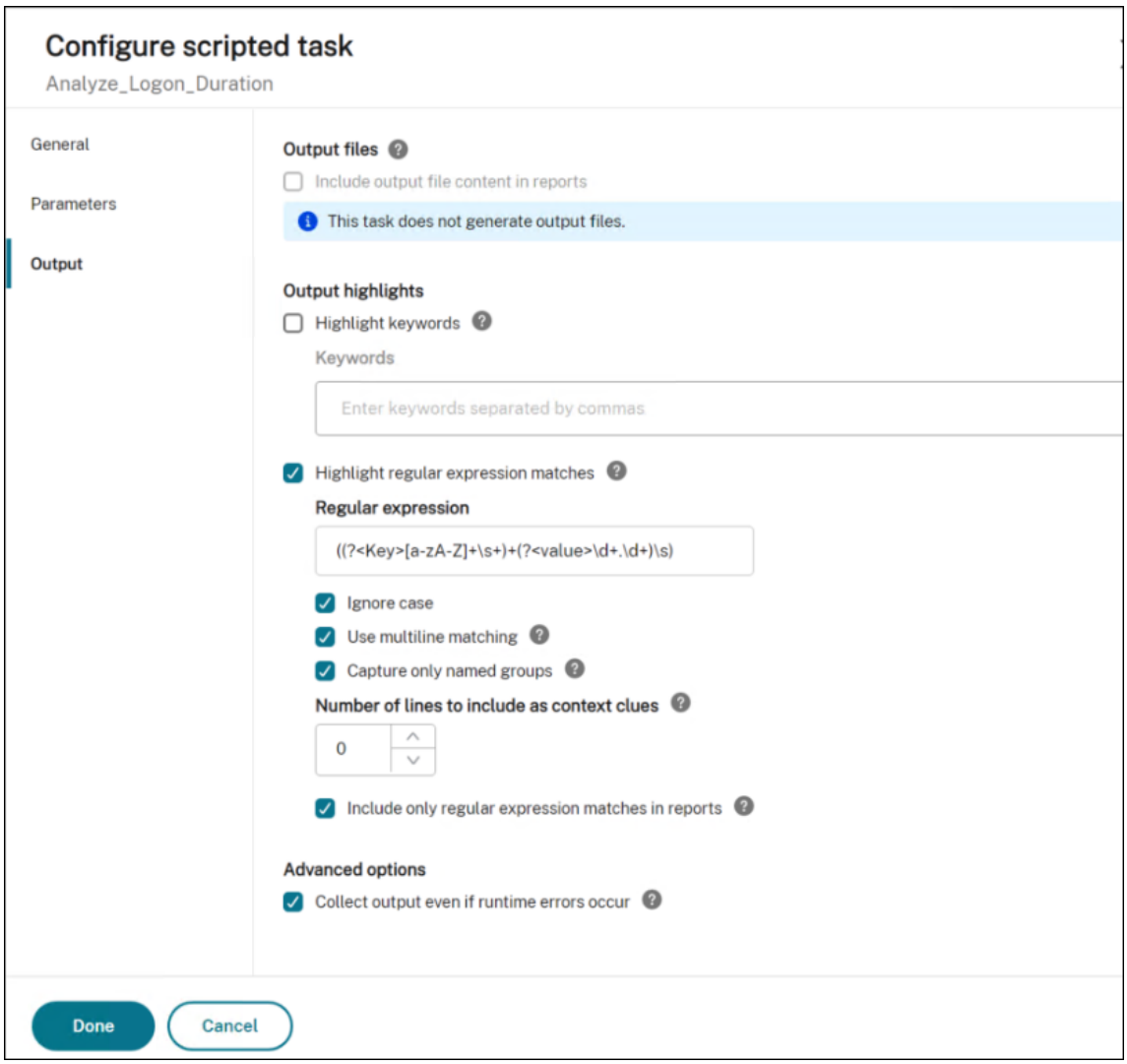
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. In **Parameters**, choose whether to pass parameters to the task. In this example, you can skip this step.
4. In **Output**, configure settings as follows. Set the regular expression value:

```
((?<Key>[a-zA-Z]+\s+)+(?<value>\d+.\d+)\s)
```

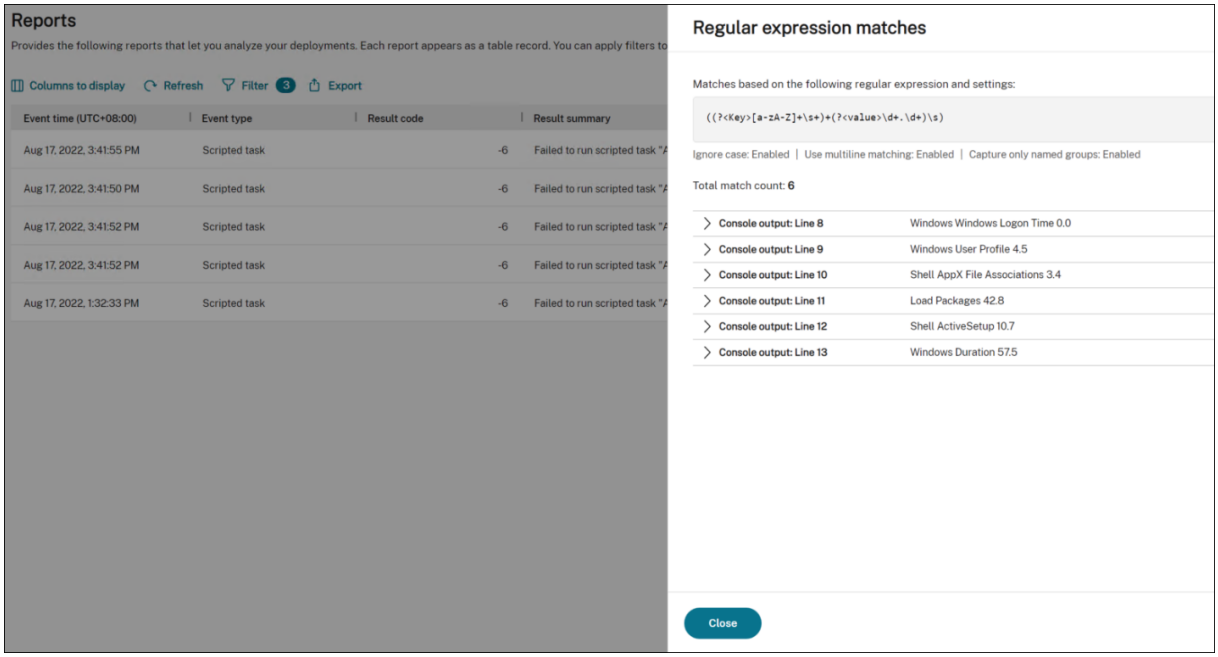
© 1997–2026 Citrix Systems, Inc. All rights reserved.



View the task execution report

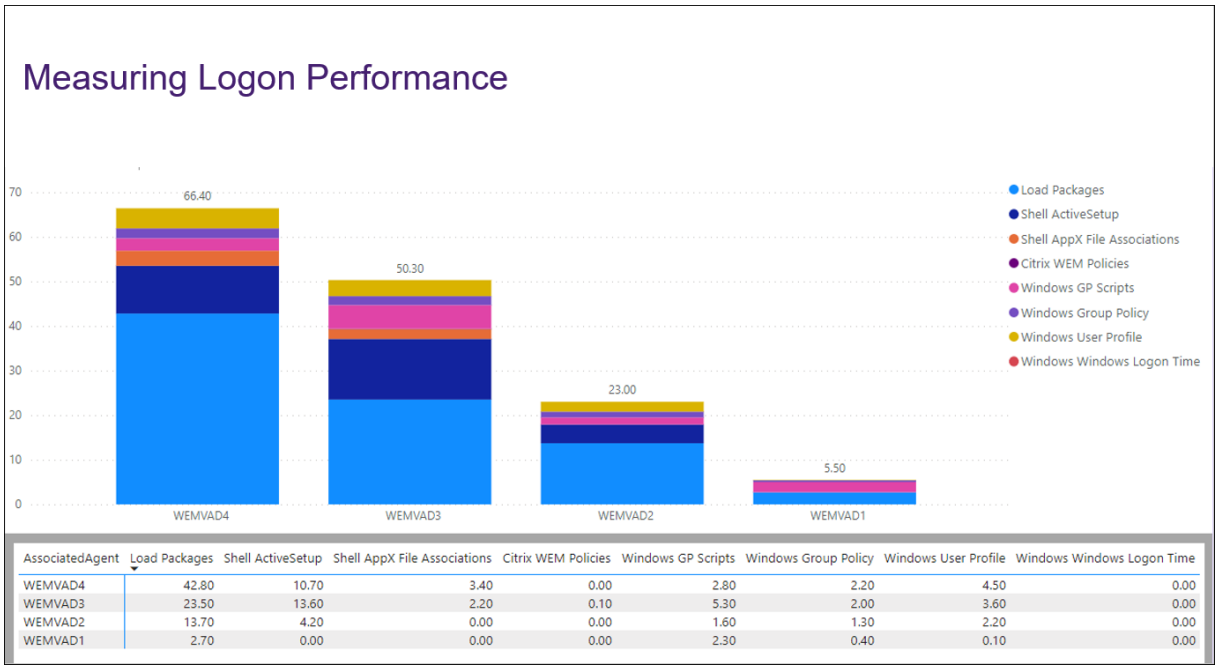
After the task runs successfully, you can view the results by checking the reports. For more information, see Reports. In this example, you can see the following report:

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



You can use filters to narrow your view to relevant reports and then export them. For information about exporting reports, see Export reports. Based on the exported data, you can perform further analysis.

The following is an example of visualizing data of interest in Power BI. It shows a breakdown of the user's logon duration.



AssociatedAgent	Load Packages	Shell ActiveSetup	Shell AppX File Associations	Citrix WEM Policies	Windows GP Scripts	Windows Group Policy	Windows User Profile	Windows Windows Logon Time
WEMVAD4	42.80	10.70	3.40	0.00	2.80	2.20	4.50	0.00
WEMVAD3	23.50	13.60	2.20	0.10	5.30	2.00	3.60	0.00
WEMVAD2	13.70	4.20	0.00	0.00	1.60	1.30	2.20	0.00
WEMVAD1	2.70	0.00	0.00	0.00	2.30	0.40	0.10	0.00

> **Tip:**

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

> Logon performance optimization is one of the highlights of the Workspace Environment Management service. The feature can change the overall logon process to drastically reduce logon times. See Logon Optimization.

Analyze logon performance using Citrix Environment Tool Hub

October 23, 2025

Citrix Environment Tool Hub provides detailed logon phase analysis, process monitoring, and deep performance metrics to help you identify and resolve logon delays efficiently.

This article builds on the concepts described in Troubleshoot Login Time Issues Using Citrix Environment Tool Hub and WEM and introduces the Tool Hub's enhanced diagnostic features through a complete, step-by-step diagnostic workflow.

About enhanced diagnostic capabilities

Citrix Environment Tool Hub introduces several enhancements that make logon performance analysis more comprehensive and actionable:

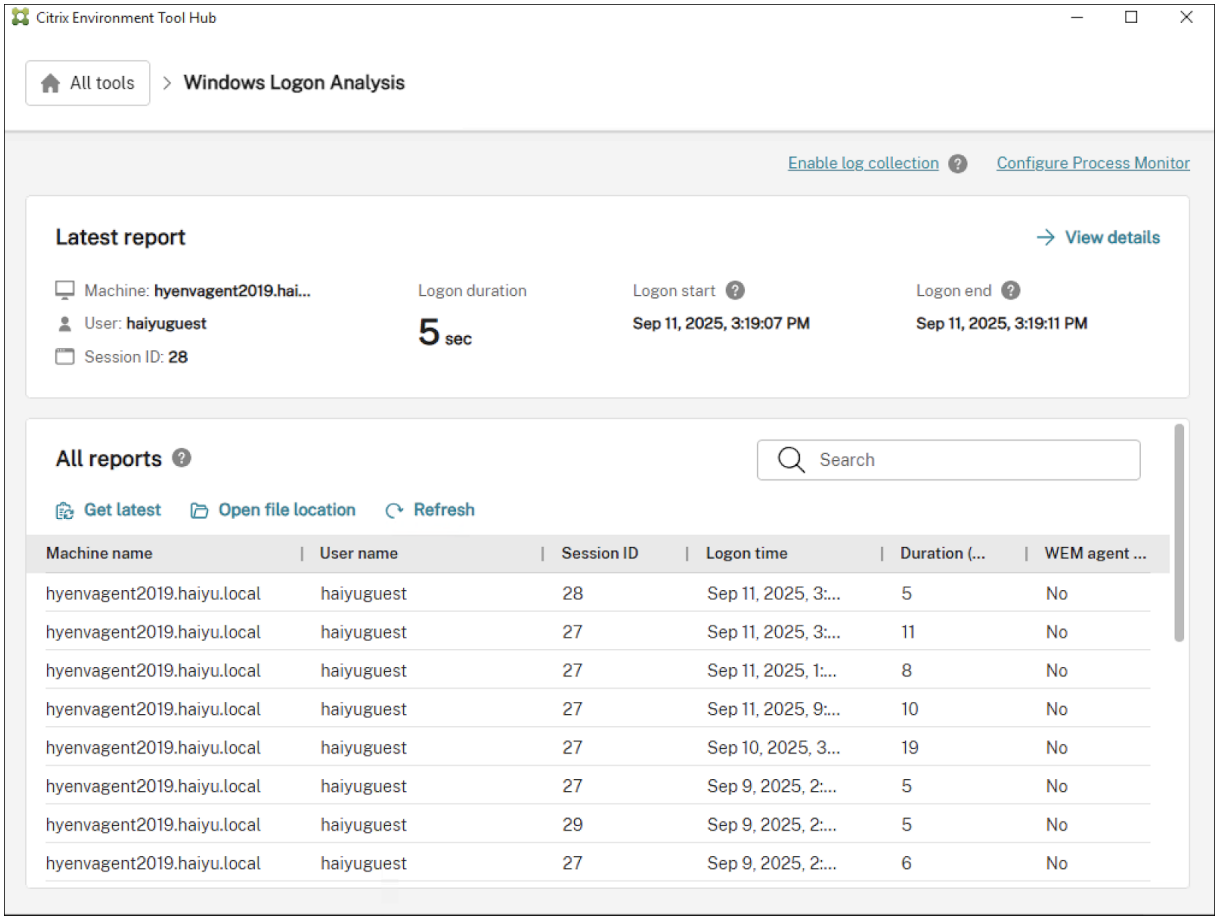
- Optimized report presentation
- Enhanced Process Monitor integration
- Deep metrics from Process Monitor log integration

Optimized report presentation

The Windows Logon Analysis tool now provides an improved, tabular report view that presents logon analysis results in a clear and structured format:

- Logon analysis results appear in a table.
- Each record includes fields such as **Logon time**, **Duration**, **Username**, **Session ID**, and **Machine name**.
- Clicking a record opens a detailed view that breaks down each logon phase (for example, *Group Policy*, *Shell*, and *Profile*).

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



This layout helps you identify the slowest logon phases quickly and focus your investigation on potential bottlenecks.

Enhanced Process Monitor integration

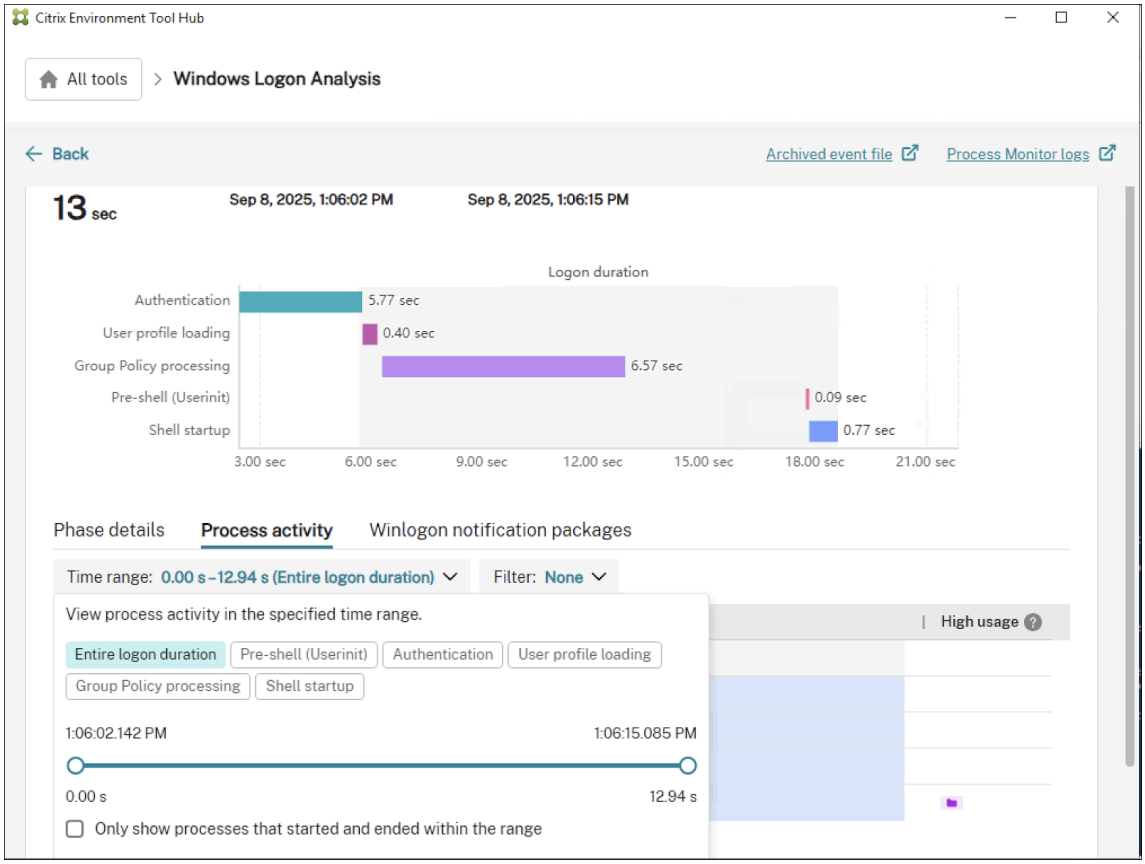
The Process Monitor module now provides granular insights into process behavior during logon, including:

- Time-based filtering
- Lifecycle visualization and usage markers
- Linked detail view

Time range and resource filtering With this feature, you can:

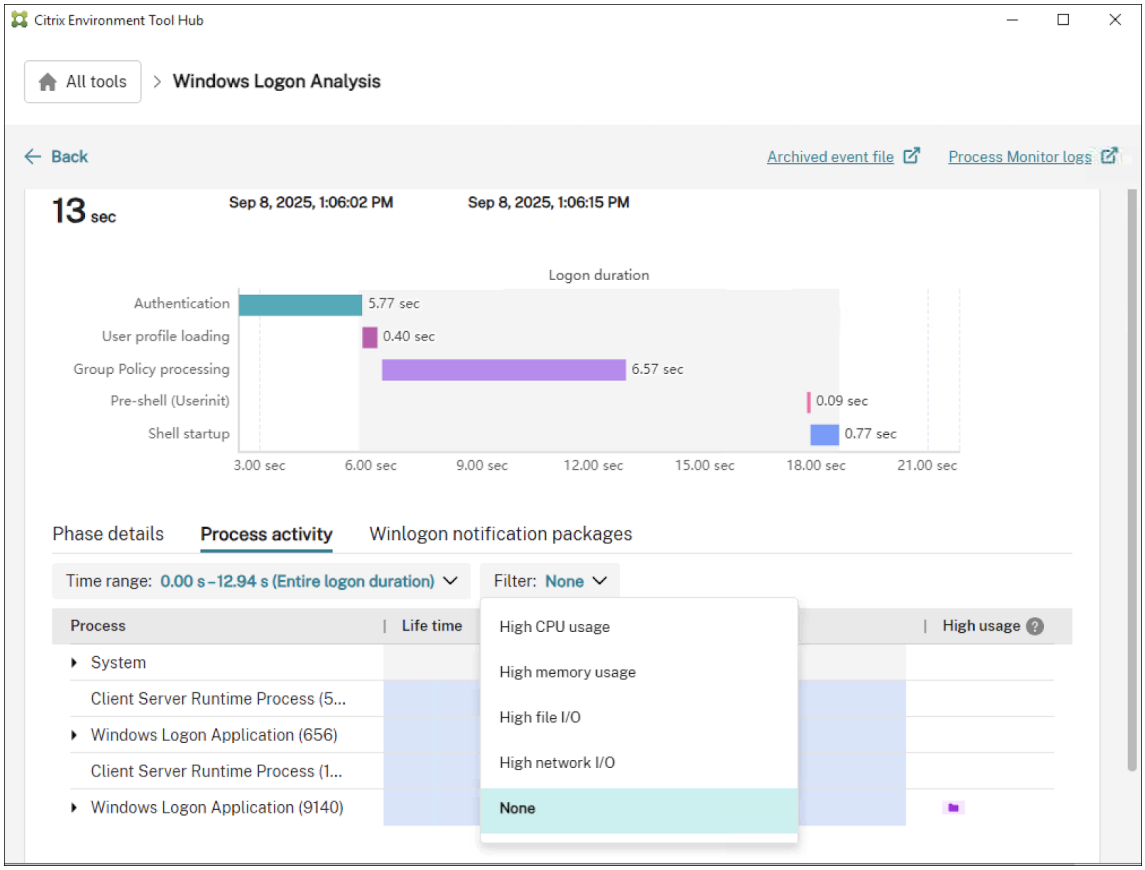
- Drag to select a time range on the logon timeline.
- Use predefined phase filters such as *Authentication* or *Shell startup*.
- Optionally enable **Show only processes that start and end within the selected time range**.

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



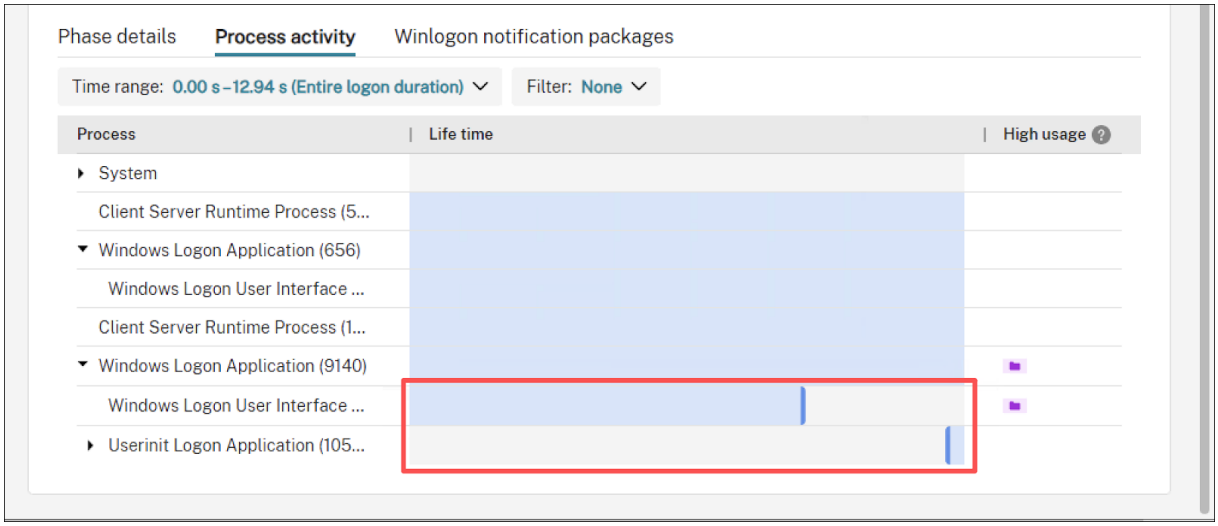
- Apply resource filters to identify:
  - High CPU usage
  - High memory usage
  - High file I/O
  - High network I/O

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



Lifecycle visualization and usage markers Detailed features include:

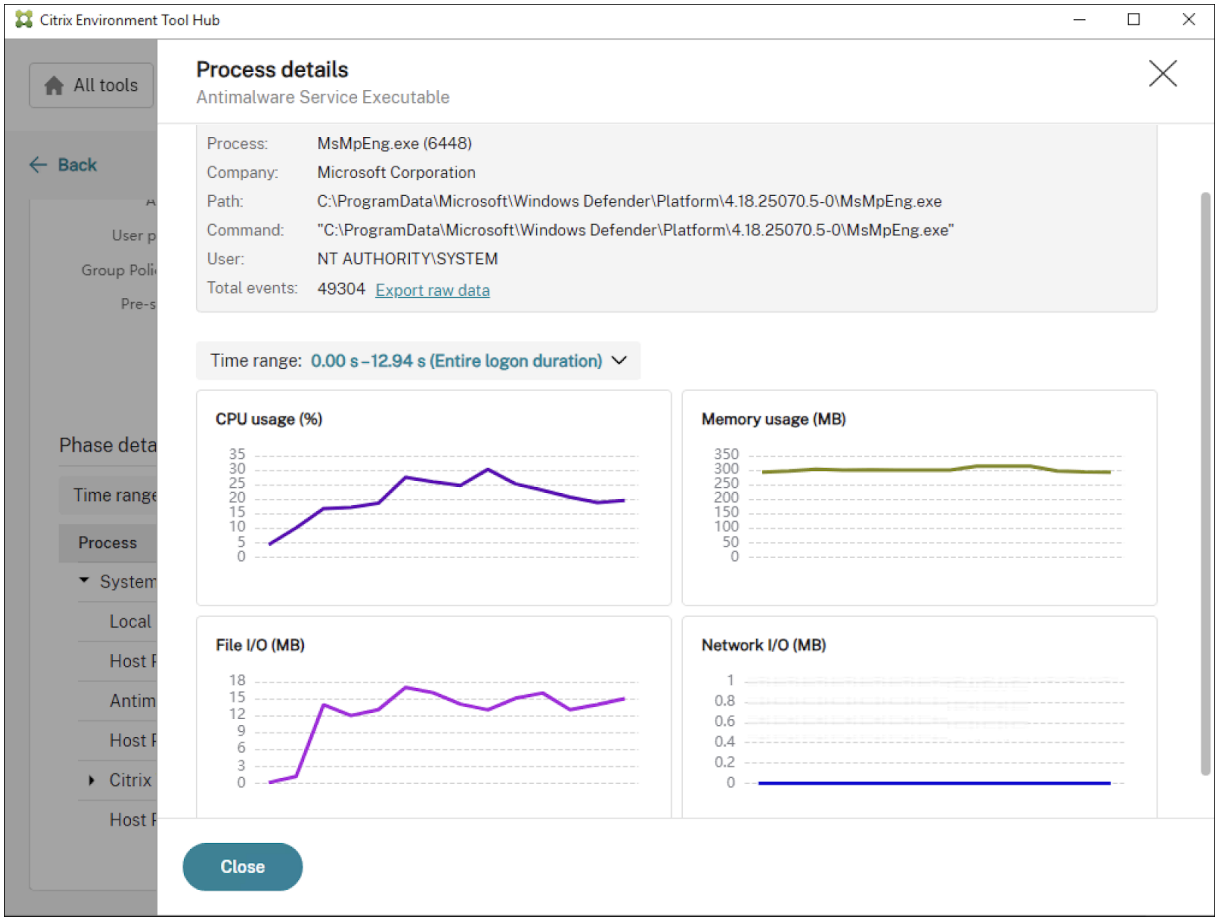
- Each process appears as a horizontal lifecycle bar.
- High resource usage is marked with visual indicators.
- Start and end points are highlighted for easy identification.



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

Linked detail view Detailed features include:

- Selecting a lifecycle bar opens a detailed process view.
- The detail view includes process metadata such as **Name**, **PID**, **Start time**, **User**, and **Command line**.
- Four resource usage charts are available:
  - CPU usage (%)
  - Memory usage (MB)
  - File I/O activity (MB)
  - Network usage (MB)
- The **Export raw data** option lets you download event-level details, such as thread activity, module loads, or system calls, for advanced analysis or archiving.



Deep metrics from Process Monitor log integration

When you enable **Process Monitor logging** during logon analysis, the Windows Logon Analysis tool automatically parses the log and adds detailed performance metrics to your report.

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

Examples include:

- **Temporary folder traversal time**: If a user's %TEMP% directory includes many files or nested folders, logon delays can occur during folder access.
- **Default profile copy time**: During a first-time logon, the system copies the default profile from `C:\Users\Default` to the user directory, which can significantly extend logon duration.

Other metrics might appear depending on your environment and captured activity.

Case study: Diagnose a slow logon

A user reported slow logon performance. The following example demonstrates how an administrator diagnosed and resolved the issue using Citrix Environment Tool Hub.

Step 1: Analyze the initial logon

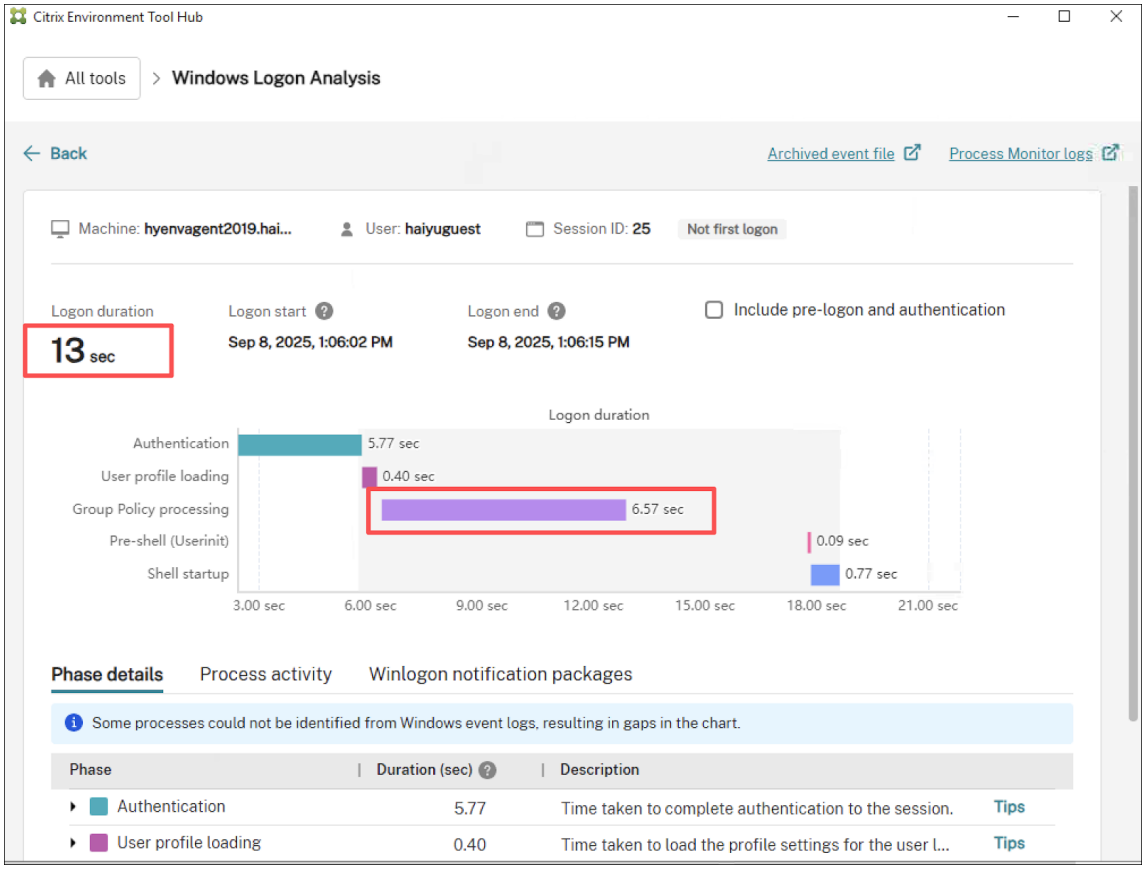
1. Open Citrix Environment Tool Hub.
2. Run a logon analysis and review the results.

   Initial findings:

   - Total logon duration: 13 seconds
   - Group Policy processing: 6.57 seconds (about half of the total duration)

   This initial analysis suggests Group Policy is the primary bottleneck. Continue the investigation using Process Monitor.

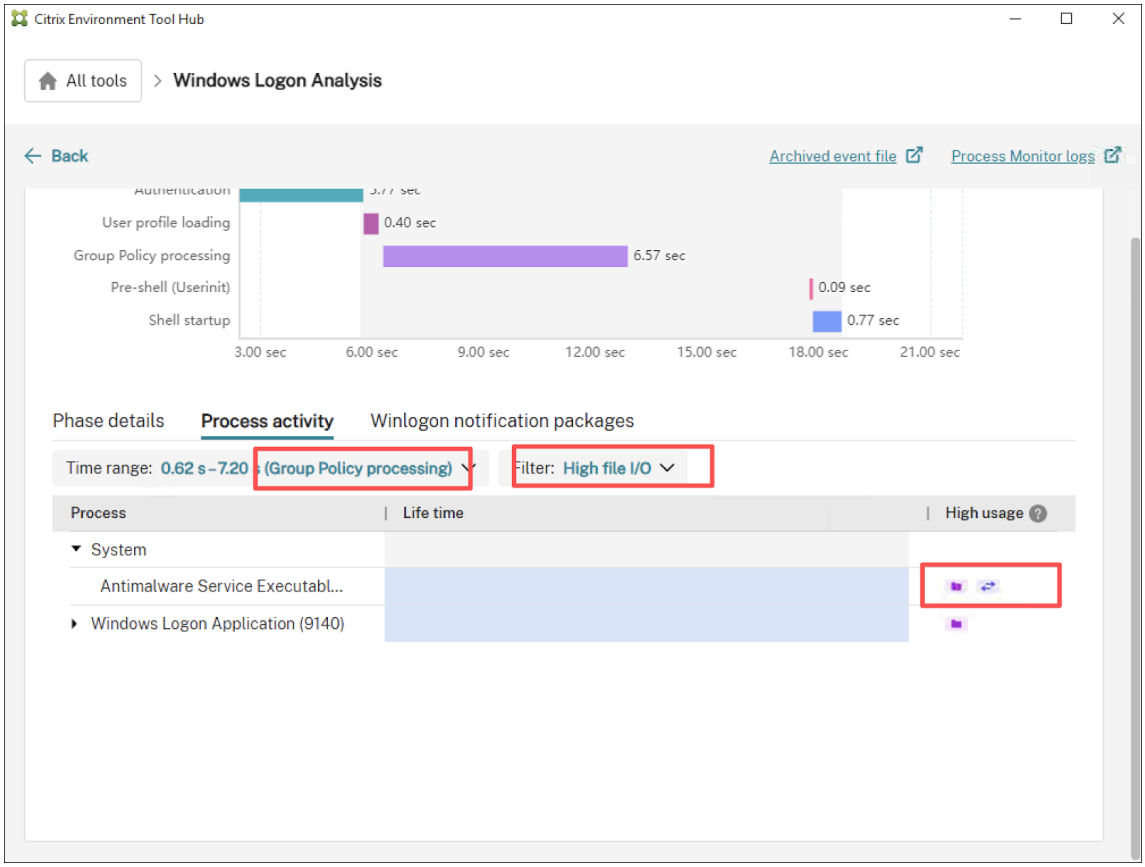
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 2: Enable Process Monitor and reproduce the issue

1. Enable **Process Monitor** in the Windows Logon Analysis tool. For more information, see Process activity and details.
2. Ask the user to log on again to capture a complete trace.
3. After the logon completes, run another logon analysis.
4. Open the **Process activity** tab to view process behavior during the logon.
5. Select the Group Policy phase time range and apply high-usage filters to pinpoint resource-intensive processes.

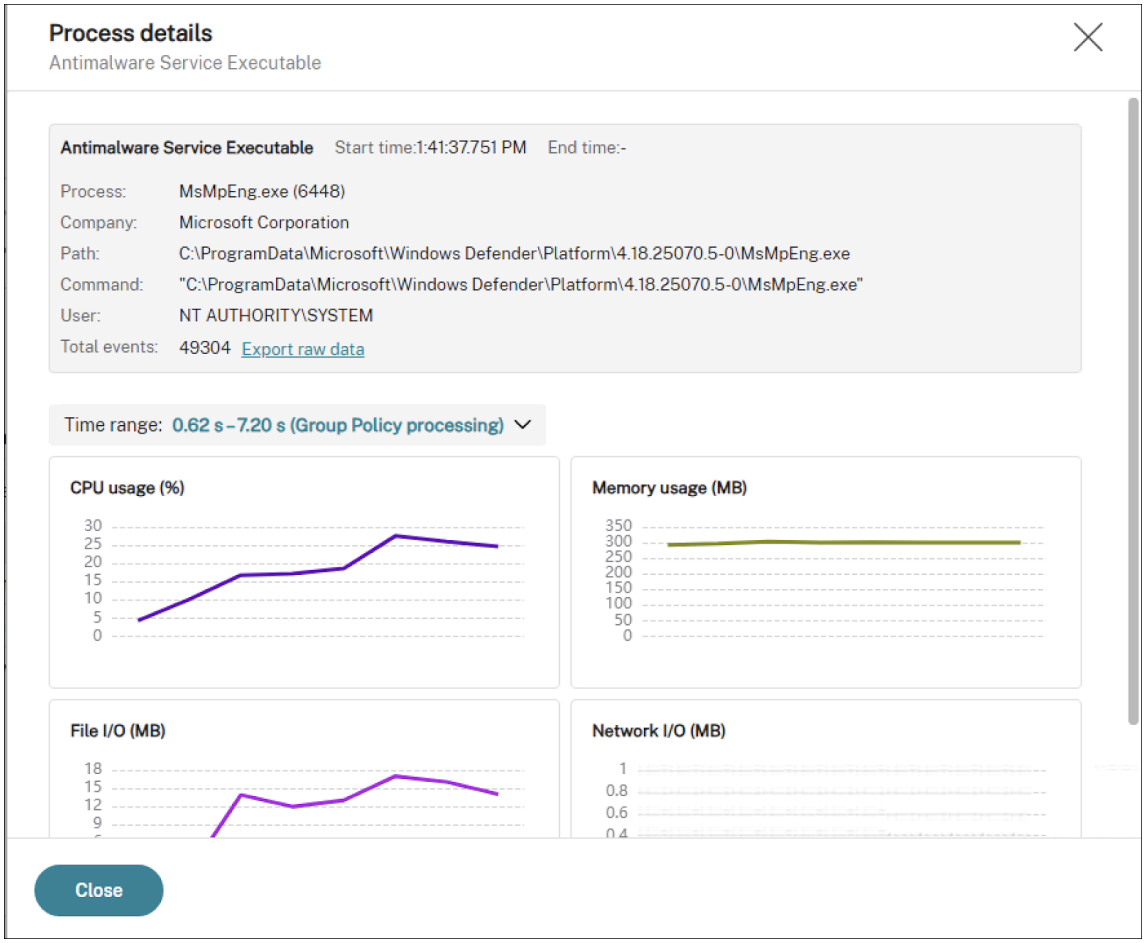
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 3: Identify the high-usage process

1. Among the highlighted processes, **MsMpEng.exe** (Microsoft Defender's Antimalware Service Executable) showed sustained file I/O activity during the Group Policy phase.
2. Open the **Process details** view to confirm Defender's real-time file scanning during policy execution.

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

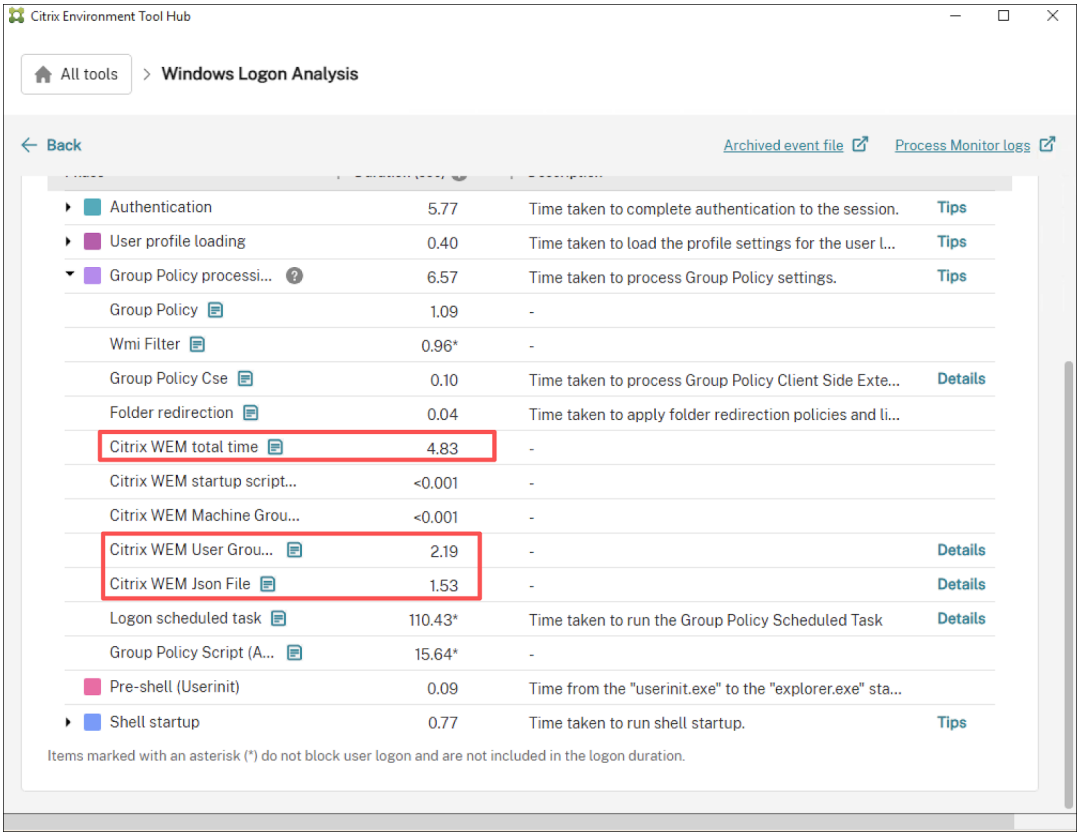


Step 4: Confirm the root cause and apply a fix

1. Review the detailed log to identify which WEM agent tasks triggered Defender scans. Examples include:

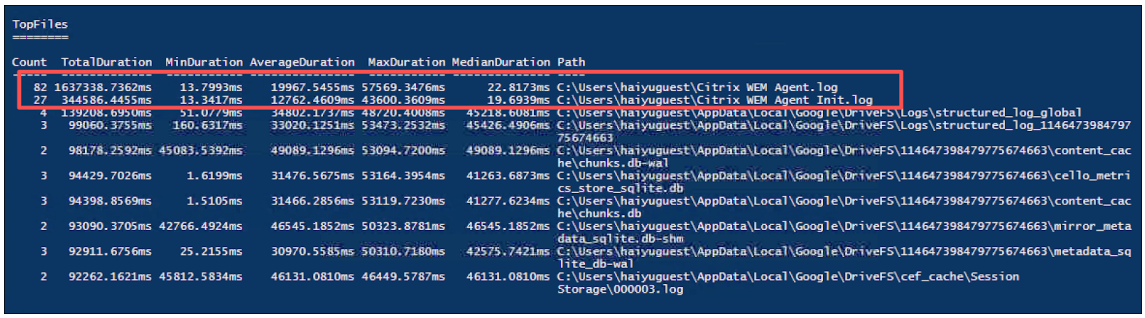
   - **Citrix WEM User Group Policy** (2.19 seconds)
   - **Citrix WEM JsonFile processing** (1.53 seconds)

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



2. Start performance monitoring to confirm Defender scan impact:

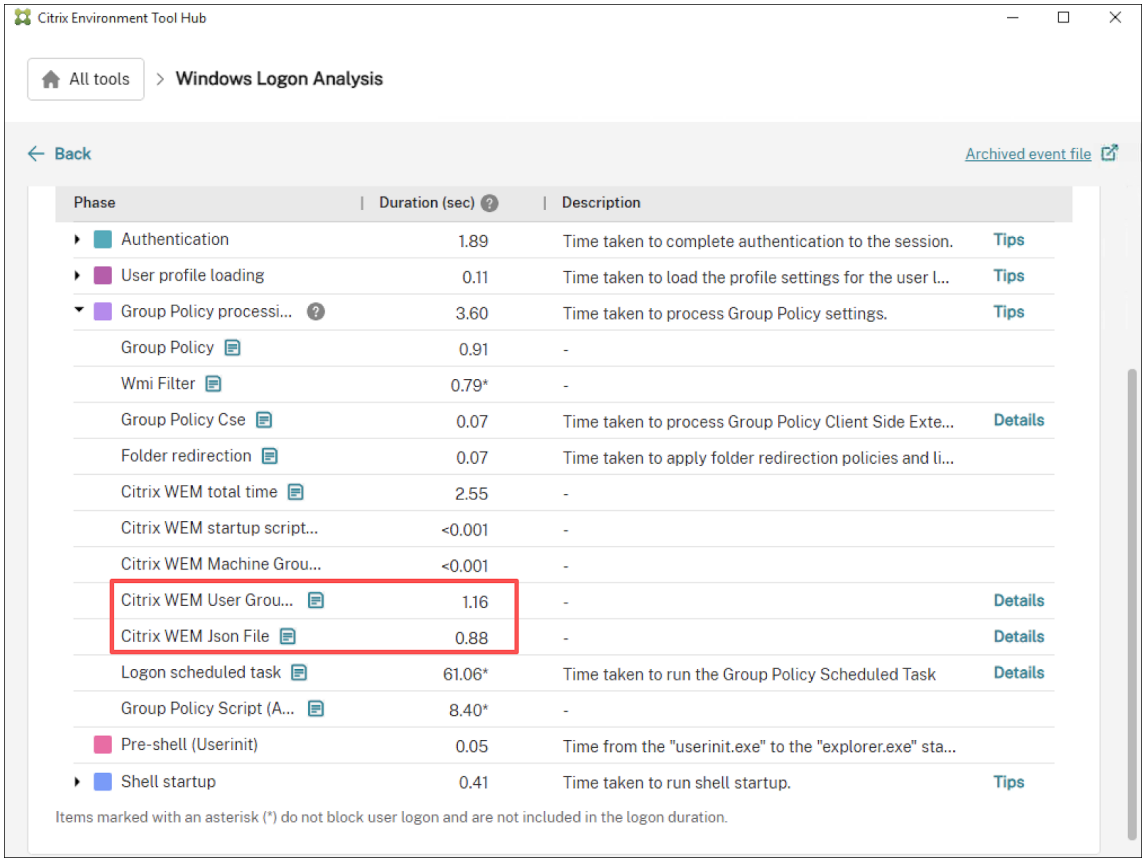
   a) Run `New-MpPerformanceRecording` to start monitoring.
   b) Ask the user to log on again.
   c) Run `Get-MpPerformanceReport` to summarize Defender's scan impact.



   For more information, see the following Microsoft articles about New-MpPerformanceRecording and Get-MpPerformanceReport.

3. Verify that the WEM agent is a trusted Citrix component.
4. Add exclusions in Microsoft Defender for the WEM agent's processes and file paths.
5. After applying the exclusions, ask the user to log on again.
6. Verify that the Group Policy duration decreases and that overall logon performance improves.

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



Summary

This example illustrates a complete diagnostic workflow: from user report to analysis, trace capture, root cause identification, and resolution.

The integration of Process Monitor with Citrix Environment Tool Hub helps you uncover hidden bottlenecks and apply targeted optimizations to improve user experience across your Citrix environment.

Automatically apply Windows updates using scripted tasks

September 7, 2025

As an administrator, you might have many devices to manage. They might exist in different domains and have different security levels or Windows OS versions. Updating those devices in a timely manner to prevent potential risks can be a tedious task. To achieve this goal, you might do the following:

- Collect information related to updates.

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

- Draw comparisons between the collected information to identify the devices where updates are missing.
- Apply one or more updates to relevant devices one by one.

Workspace Environment Management™ (WEM) provides you with a scripted task feature that simplifies the task of applying updates to your devices.

All you need to do is configure two scripted tasks. A general workflow is as follows:

1. Prepare two scripts and create a file
2. Add two scripted tasks
3. Configure the two scripted tasks
4. View the task execution report

Prepare two scripts and create a file

1. Prepare a script that monitors available updates.

```
$List = Get-Content \\hyenvwemserver\share\hotfix.list
$Applied = Get-HotFix | Select-Object -ExpandProperty HotFixID
$ExitCode = 0
$List | ForEach-Object {

    if(-not ($Applied.Contains($_)))
    {

        Write-Host $_
        $ExitCode = 1
     }

 }

Exit $ExitCode
```

2. Prepare another script that applies updates.

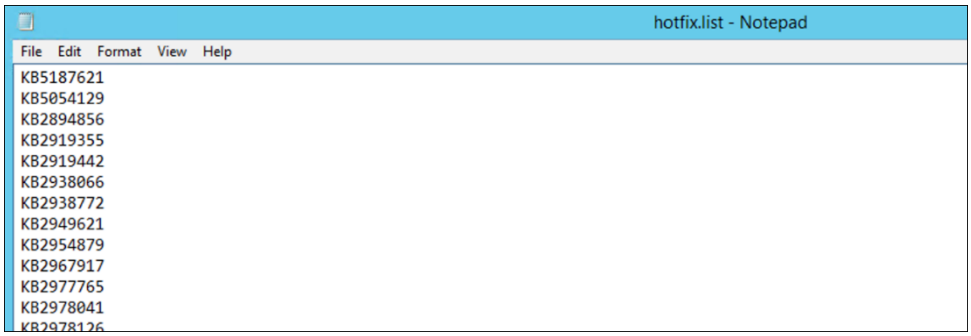
```
Param(
  [string]$consoleOutputPath
  )
$List = Get-Content $consoleOutputPath
$List | ForEach-Object {

  Write-host "Installing hotfix: $_"
  Get-WindowsUpdate -Install -KBArticleID $_
 }
```

3. Create a file that includes a list of updates.

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

> **Note:**
>
> Put this file in a place that the WEM agent can access, for example, in a shared path: `\\hyenvwenserver\share\hotfix.list`.



Add two scripted tasks

The following information is supplemental to the guidance in Add a scripted task. To create the two scripted tasks, follow the general guidance in that article, minding the details below.

In **Web Console > Scripted Tasks**, add the two scripted tasks.



Configure the two scripted tasks

The following information is supplemental to the guidance in Configure a scripted task. To configure the two scripted tasks, follow the general guidance in that article, minding the details below.

1. Go to the relevant configuration set, navigate to **Scripted Task Settings**, and configure the "Apply updates"task.

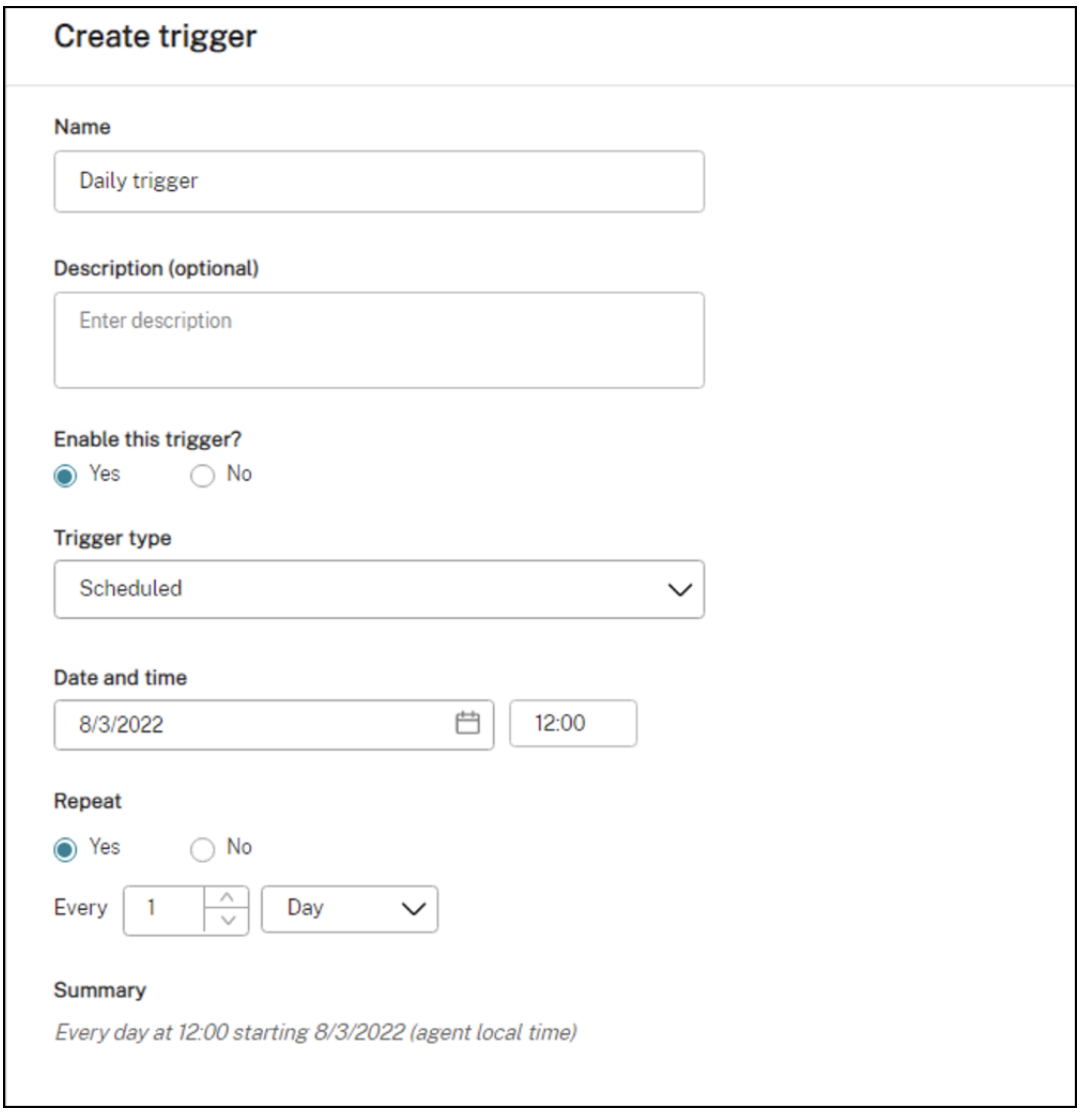
   In this example, the task is specifically configured as follows:

   a) Select **Yes** to enable the task.

   b) Clear **Verify the signature before running the task**.

   c) In **Triggers**, create a "Scheduled"trigger as follows.

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



2. In the same configuration set, configure the “Monitor updates”task.

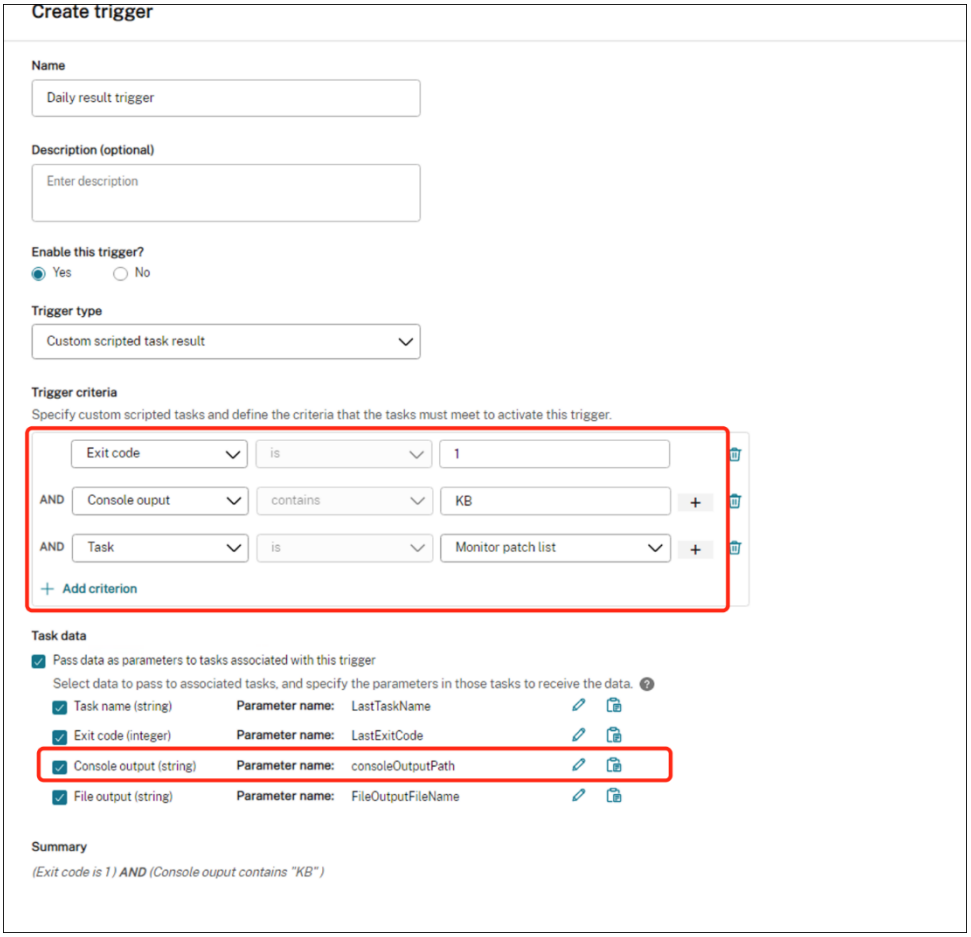
   In this example, the task is specifically configured as follows:

   a) Select **Yes** to enable the task.

   b) Clear **Verify the signature before running the task**.

   c) In **Triggers**, create a “Custom scripted task result”trigger as follows.

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



View the task execution report

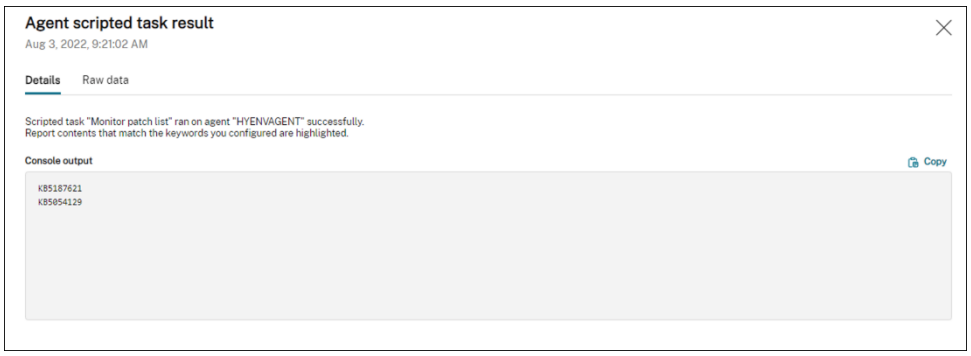
After the tasks run successfully, you can view the results by checking the reports. For more information, see Reports. In this example, you can see the following reports:

Report summary:

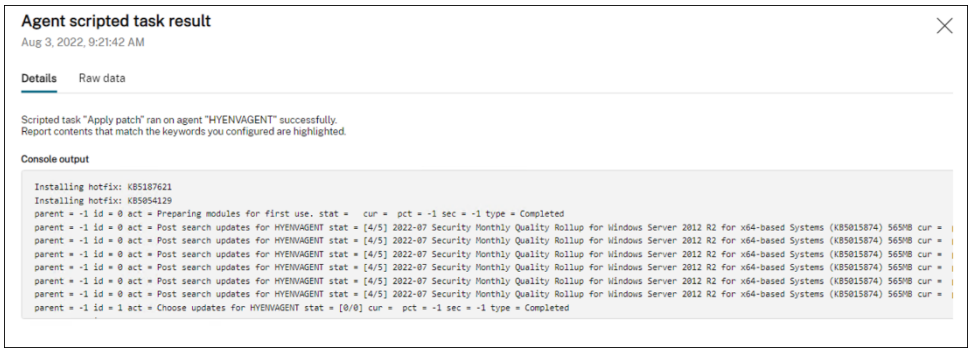


Report detail of the “Apply updates”task:

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



Report detail of the ‘‘Monitor updates’’task:



Automatically back up configuration sets using WEM APIs and Windows PowerShell

October 8, 2026

As a Workspace Environment Management™ (WEM) administrator, you might need to back up your configuration sets regularly to prevent settings from getting lost. You might want to trigger the backup, for example, every 12 hours, and manage the backup files locally and automatically. Using WEM public APIs and Windows PowerShell, you can accomplish that goal.

A general workflow is as follows:

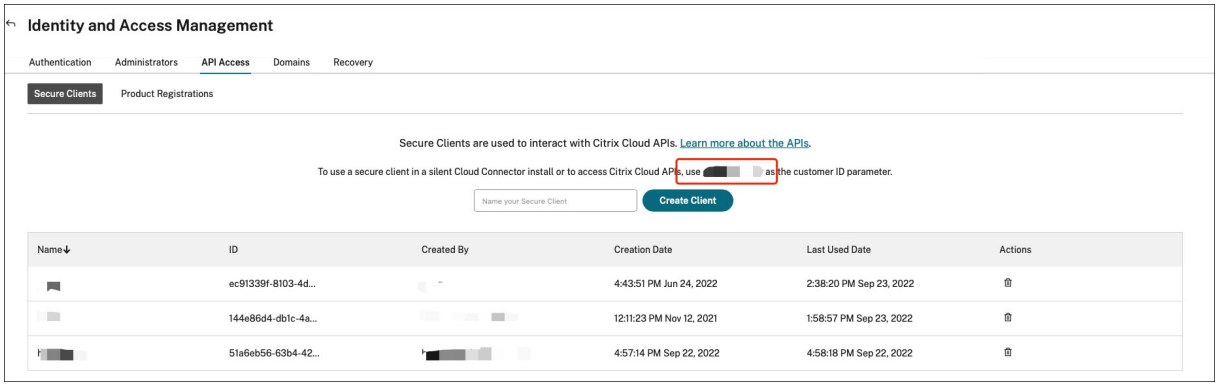
1. Apply for a Citrix Cloud™ API client
2. Write a PowerShell script to back up your configuration sets
3. Configure a scheduled task to run the script

Prerequisites

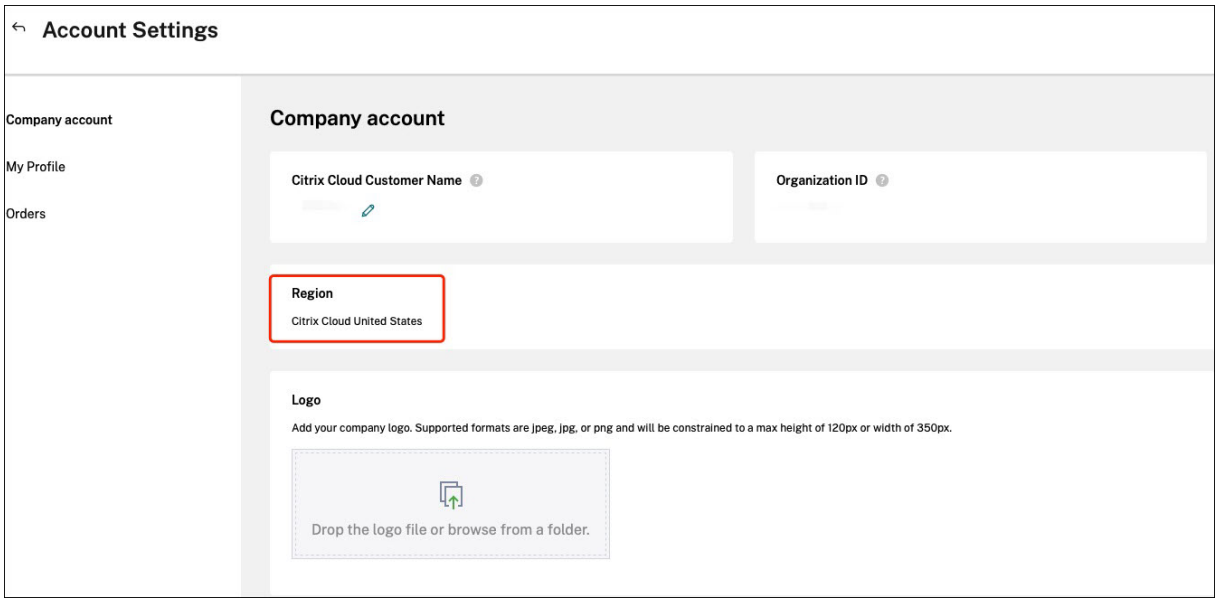
Before you start, make sure that you know your Citrix® customer ID and the related API-base URLs.

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

Sign in to Citrix Cloud, navigate to **Identity and Access Management > API Access**, and find your Citrix customer ID.



The API-base URLs, including Citrix Auth API base URL and WEM API base URL, are related to the region of Citrix Cloud you're connecting to. The region is determined when you onboard to Citrix Cloud. You can also query your region in **Account Settings**.



You can find the API-base URLs by checking the following table.

Region	Citrix Auth API base URL	WEM API base URL
United States (US)	api-us.cloud.com	api.wem.cloud.com
European Union (EU)	api-eu.cloud.com	eu-api.wem.cloud.com
Asia Pacific South (AP-S)	api-ap-s.cloud.com	aps-api.wem.cloud.com
Japan (JP)	api.citrixcloud.jp	jp-api.wem.citrixcloud.jp

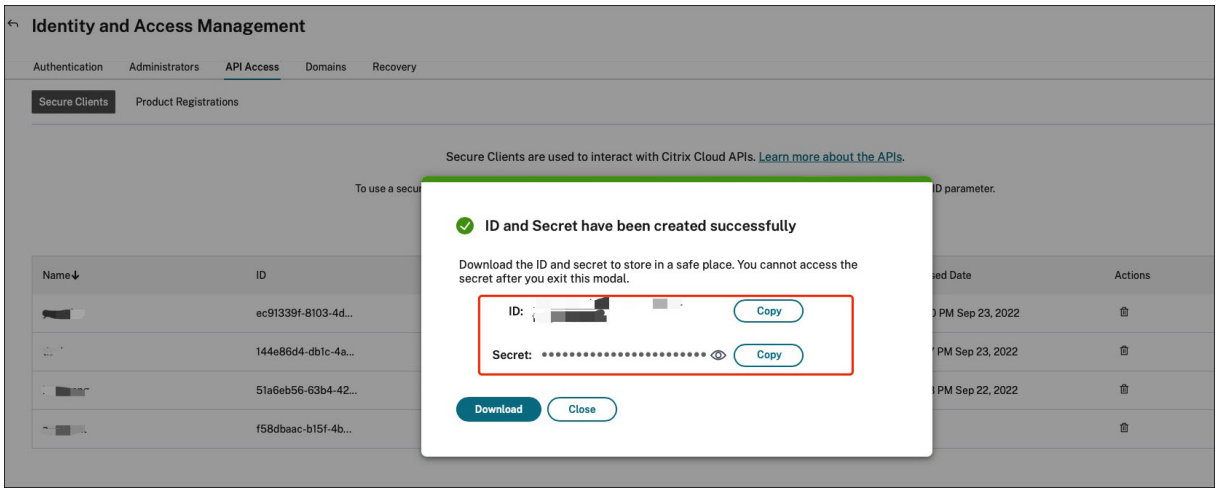
For more information about the API base URLs, see Get Started With Citrix Cloud APIs and WEM API

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

overview.

Apply for a Citrix Cloud API client

Navigate to **Identity and Access Management > API Access**. Type the name of your secure client, click **Create Client**, and save the secure client ID and client secret locally.



Write a PowerShell script to back up your configuration sets

Use the following PowerShell script and save it as `Invoke-WEMConfigSetBackupAPI.ps1`. Be sure to replace the variables at the beginning of the script.

```
# replace the variables before running the script

$CitrixCustomerId = 'your-citrix-customer-id'
$CitrixAuthAPIBaseURL = 'api-us.cloud.com'
$CitrixWEMAPIBaseURL = 'api.wem.cloud.com'
$ClientId = 'your-api-client-id'
$ClientSecret = 'your-api-client-secret'

$ConfigSetsToBackUp = @('Default Site', 'MyConfigSet') # leave it empty if you want to back up all configuration sets
$FolderToSaveBackup = 'C:\ProgramData'

# get bearer token

$ErrorActionPreference = 'Stop'

$URL = "https://${
 CitrixAuthAPIBaseURL }
 /cctrustoauth2/${
 CitrixCustomerId }
 /tokens/clients"
```

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

```
$Body = "grant_type=client_credentials&client_id=${
 ClientId }
 &client_secret=${
 ClientSecret }
 "
$Response = Invoke-RestMethod -Method 'Post' -Uri $URL -Body $Body -
    ContentType 'application/x-www-form-urlencoded'

$BearerToken = $Response.access_token

if ([string]::IsNullOrEmpty($BearerToken))
{

    throw 'Cannot retrieve bearer token.'
 }


Write-Host "Retrieved bearer token successfully."

# back up WEM configuration sets

if (-not (Test-Path -Path $FolderToSaveBackup -PathType 'Container'))
{

    throw 'The folder to save backup not exists.'
 }


$Headers = @{

    'Citrix-CustomerId' = $CitrixCustomerId
    'Accept' = 'application/json'
    'Authorization' = "CWSAUTH bearer=${
 BearerToken }
 "
 }


if ($ConfigSetsToBackUp.Count -eq 0 -or $ConfigSetsToBackUp -eq $null)
{

    $URL = "https://${
 CitrixWEMAPIBaseURL }
 /services/wem/sites"
    $Response = Invoke-RestMethod -Method 'Get' -Uri $URL -Headers
       $Headers
    $ConfigSetsToBackUp = $Response.items |% {
  $_.name  }

 }


$ConfigSetsToBackUp | ForEach-Object {
```

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

```
72
73      Write-Host "Backing up configuration set ""$_"""
74      $URL = "https://${
75    CitrixWEMAPIBaseURL }
76    /services/wem/sites/%24export?name=$_"
77      Write-Host "GET $URL"
78      $Response = Invoke-RestMethod -Method 'Get' -Uri $URL -Headers
            $Headers
79      $Timestamp = Get-Date -Format "yyyyMMddHHmmss"
80      $Response | ConvertTo-Json -Depth 10 | Out-File (Join-Path
            $FolderToSaveBackup "${
81    _ }
82    -${
83    Timestamp }
84    .json")
85    }
```

For more information about bearer tokens, see Get Started With Citrix Cloud APIs.

For more information about using the WEM API to back up configuration set, see Exporting WEM configuration set API.

> **Note:**
>
> Each bearer token expires after an hour. To avoid frequently invoking the Citrix Cloud auth APIs and WEM APIs, cache the bearer token and reuse it if the backup duration takes less than an hour.

If you encounter the error **504 Gateway Time-out**, it likely means that your configuration set is too large, causing the backup time to exceed the 1-minute API timeout. In such cases, try using the following PowerShell script instead. Note that this script uses APIs that are not currently public, and these APIs may change in the future.

```
1  # replace the variables before running the script
2
3  $CitrixCustomerId = 'your-citrix-customer-id'
4  $CitrixAuthAPIBaseURL = 'api-us.cloud.com'
5  $CitrixWEMAPIBaseURL = 'api.wem.cloud.com'
6  $ClientId = 'your-api-client-id'
7  $ClientSecret = 'your-api-client-secret'
8
9  $ConfigSetsToBackUp = @('Default Site', 'MyConfigSet') # leave it empty
       if you want to back up all configuration sets
10 $FolderToSaveBackup = 'C:\ProgramData'
11
12 # get bearer token
13
14 $ErrorActionPreference = 'Stop'
15
16 $URL = "https://${
17  CitrixAuthAPIBaseURL }
18  /cctrustoauth2/${
19  CitrixCustomerId }
```

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

```
 /tokens/clients"
$Body = "grant_type=client_credentials&client_id=${
 ClientId }
 &client_secret=${
 ClientSecret }
 "
$Response = Invoke-RestMethod -Method 'Post' -Uri $URL -Body $Body -
    ContentType 'application/x-www-form-urlencoded'

$BearerToken = $Response.access_token

if ([string]::IsNullOrEmpty($BearerToken))
{

    throw 'Cannot retrieve bearer token.'
 }


Write-Host "Retrieved bearer token successfully."

# back up WEM configuration sets

if (-not (Test-Path -Path $FolderToSaveBackup -PathType 'Container'))
{

    throw 'The folder to save backup not exists.'
 }


$Headers = @{

    'Citrix-CustomerId' = $CitrixCustomerId
    'Accept' = 'application/json'
    'Authorization' = "CWSAUTH bearer=${
 BearerToken }
 "
 }


$URL = "https://${
 CitrixWEMAPIBaseURL }
 /services/wem/sites"
$Response = Invoke-RestMethod -Method 'Get' -Uri $URL -Headers $Headers
$Sites = $Response.items

if ($ConfigSetsToBackUp -ne $null -and $ConfigSetsToBackUp.Count -gt 0)
{

    $Sites = $Sites | Where-Object {
  $_.name -in $ConfigSetsToBackUp  }

 }

```

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

```
72
73  $Sites | ForEach-Object {
74
75      $Name = $_.name
76      Write-Host "Backing up configuration set `"$Name`""
77      $URL = "https://${
78   CitrixWEMAPIBaseURL }
79   /services/wem/export/site?async=true"
80      $FolderName = "BACKUPFOLDER-" + [Guid]::NewGuid().ToString()
81      $Body = @{
82
83          folderName = $FolderName
84          id = $_.id
85          name = $_.name
86          type = 'Configuration set'
87       }
88    | ConvertTo-Json
89      $Response = Invoke-RestMethod -Method 'Post' -Uri $URL -Headers
            $Headers -Body $Body -ContentType 'application/json; charset=utf
            -8'
90
91      Write-Host "Waiting for the backup job to complete..."
92      $URL = "https://${
93   CitrixWEMAPIBaseURL }
94   /services/wem/export/site/recentJobs"
95      do
96      {
97
98          Start-Sleep -Seconds 5
99          $Response = Invoke-RestMethod -Method 'Get' -Uri $URL -Headers
                $Headers
100         $BackupJob = $Response.backup[0]
101         $IsOnGoing = $BackupJob.id -eq $_.id -and $BackupJob.status -eq
                'Running'
102      }
103   while ($IsOnGoing)
104
105     $URL = "https://${
106  CitrixWEMAPIBaseURL }
107  /services/wem/export/site/contentView?name=${
108  FolderName }
109  "
110     $Response = Invoke-RestMethod -Method 'Get' -Uri $URL -Headers
            $Headers
111
112     $Timestamp = Get-Date -Format "yyyyMMddHHmmss"
113     $Response | ConvertTo-Json -Depth 10 | Out-File (Join-Path
            $FolderToSaveBackup "${
114  Name }
115  -${
116  Timestamp }
117  .json") -Encoding utf8
118
```

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

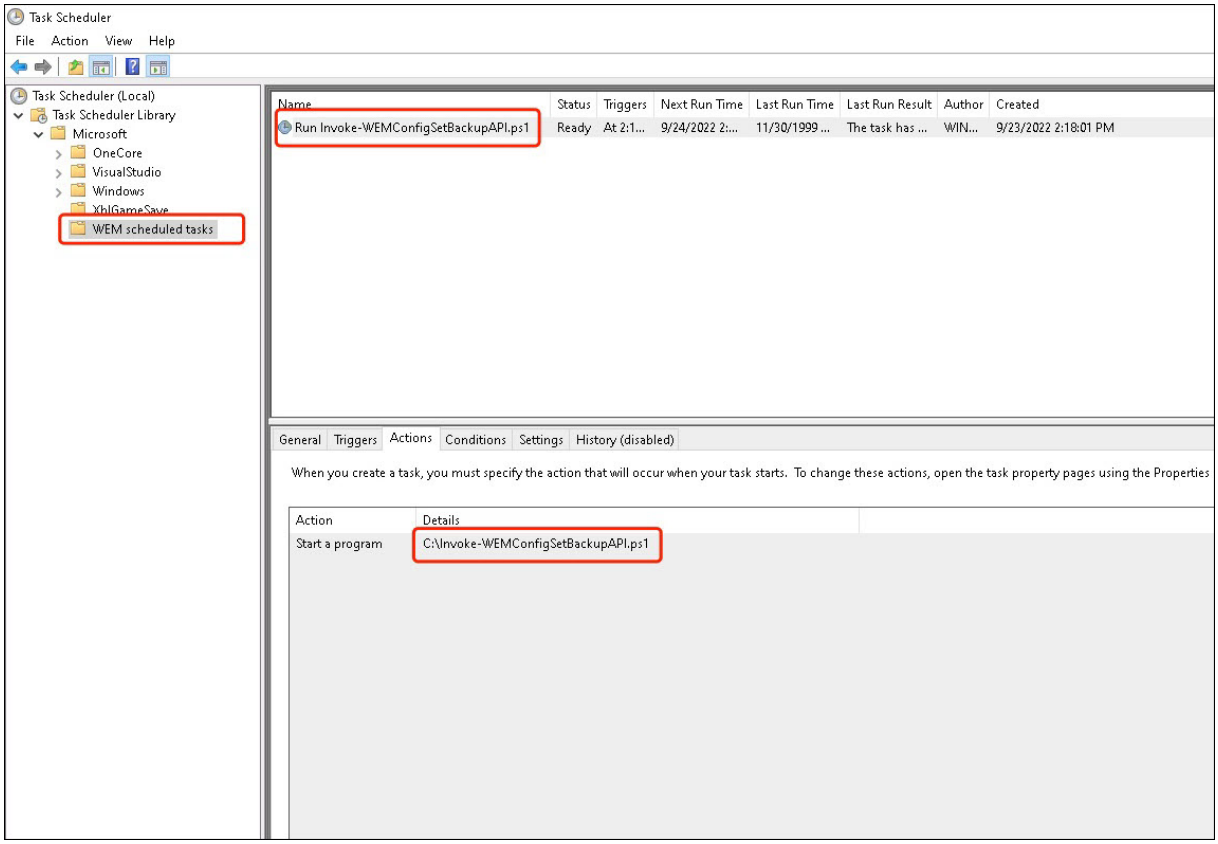
```
119     $URL = "https://${
120  CitrixWEMAPIBaseURL }
121  /services/wem/export?prefix=site%2F${
122  FolderName }
123  %2F"
124     $Response = Invoke-RestMethod -Method 'Delete' -Uri $URL -Headers
           $Headers
125  }
```

Configure a scheduled task to run the script

On a machine with access to Citrix Cloud, start `Task Scheduler` from the **Windows Start** menu or start `taskschd.msc` from the **Windows** command prompt.

You can create a folder named `WEM scheduled task`.

In the folder, create a task named `launch Invoke-WEMConfigSetBackupAPI.ps1`. Add a new trigger *repeat every 12 hours for a duration of 1 day* and add a new action of starting script `Invoke-WEMConfigSetBackupAPI.ps1`.



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

Configure file type associations

September 7, 2025

Configuring file type associations (FTA) used to be an easy task. As an administrator, you could achieve that by using scripts. However, a hash was introduced for FTA validation starting with Windows 8, making FTA configuration a pain for administrators.

You can use Workspace Environment Management (WEM) to customize FTA for a specific user or user group. For example, you can associate URL types (HTTP and HTTPS) and file types (*.htm and *.html) with Google Chrome, making it the default browser.

The configuration process includes the following steps:

1. Create FTA actions
2. Assign FTA actions to the target user or user group

Prerequisites

Before you start, do the following:

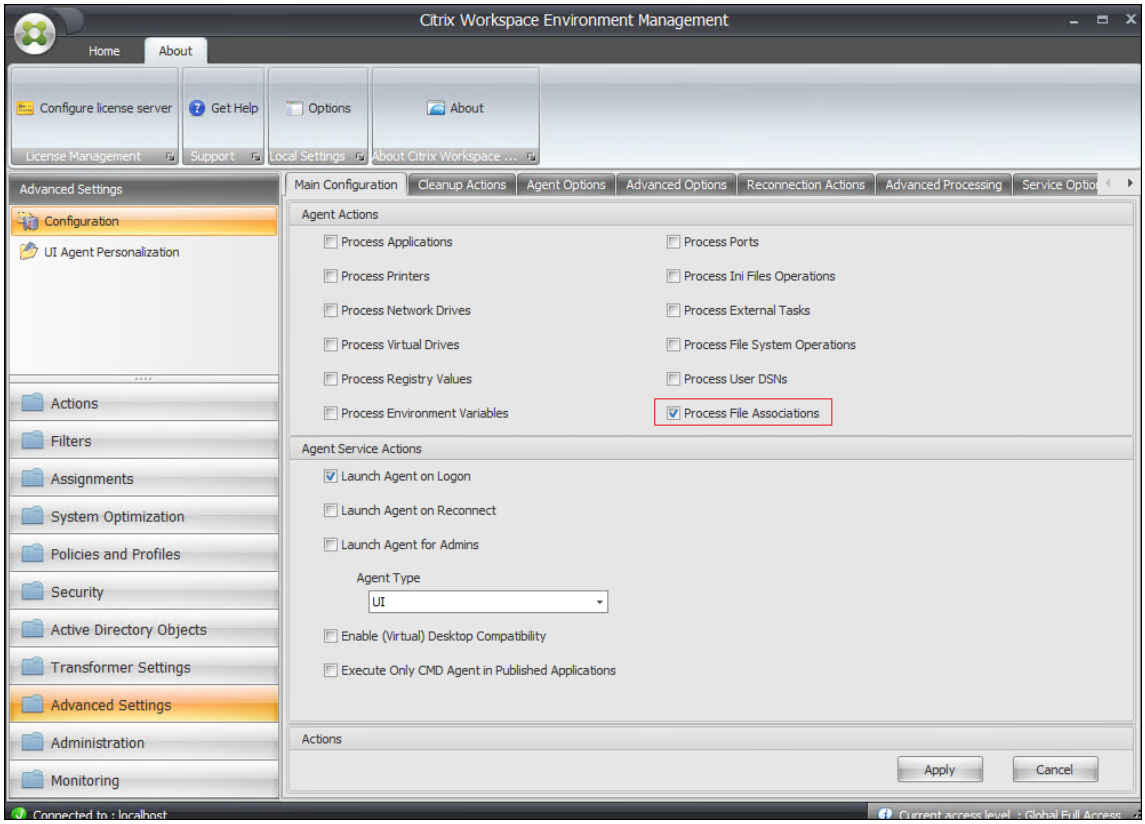
- Make sure that the agent machines have Google Chrome installed.
- Get ProgID for Google Chrome.

  The ProgID for Google Chrome is `ChromeHTML`. To discover the ProgID of an installed application, use the OLE/COM Object Viewer (oleview.exe) and look for it in Object Classes/Ole 1.0 Objects. For more information about ProgID, see Programmatic identifier (ProgID).

Create FTA actions

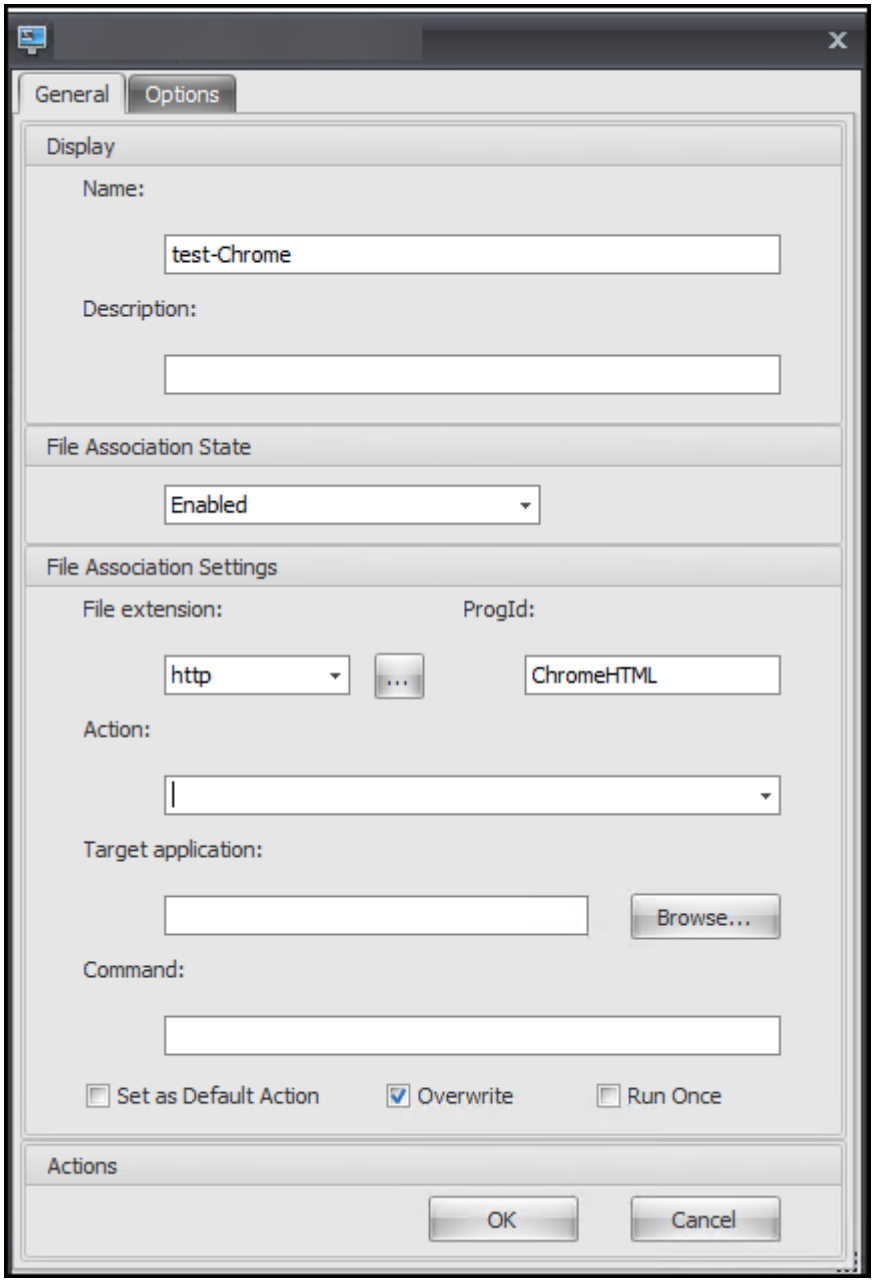
1. Go to **Legacy Console** > **Advanced Settings > Configuration > Main Configuration** and enable **Process File Associations**.

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



2. Go to **Legacy Console > Actions > File Associations > File Association List** and click **Add**.
3. In the **New File Association** window, type the information as follows and then click **OK**.

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



Note:

In this example, the correct ProgID `ChromeHTML` is provided, so there is no need to fill out the following three fields: **Action**, **Target application**, and **Command**. However, if you can't provide the ProgID for an installed application or the installed application doesn't register a ProgID during installation, you must fill out the three fields. For more information, see File Associations.

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

Assign FTA actions to the target group

1. Go to **Legacy Console > Assignments > Action Assignment** and then double-click the user or user group to which you want to assign the action.
2. Go to **Legacy Console > Administration > Agents > Statistics** and then click **Refresh**.
3. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.

For more information about FTA configuration in WEM, see File Associations.

Configure FSLogix Profile Container using WEM GPO

September 7, 2025

With Workspace Environment Management™ (WEM), you can configure FSLogix Profile Container settings without logging on to the domain controller. After uploading the administrative templates (.admx) to WEM, you can configure the policy in WEM just as you usually do on a domain controller. You then assign the policy to desired assignment targets. For precise control, you can also contextualize the assignment using predefined filters.

A general workflow for configuring FSLogix settings using WEM GPO is as follows:

1. Upload FSLogix-related administrative templates (.admx) to WEM.
2. Create a GPO to configure FSLogix and then enable the corresponding settings in the GPO.
3. Assign the GPO to the desired assignment targets.

Prerequisites

Before you start, do the following:

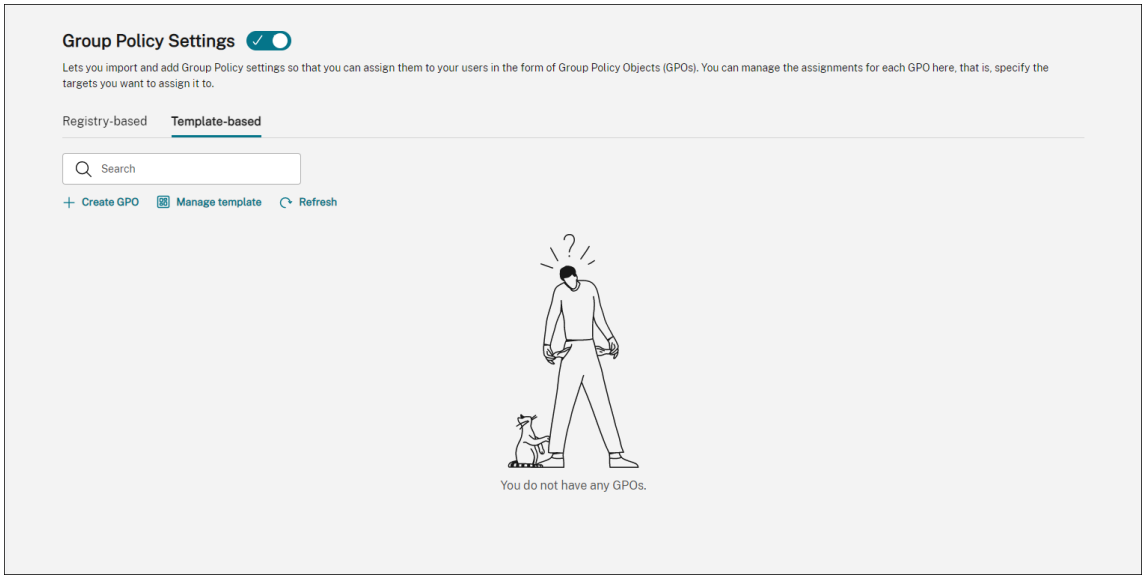
- Install FSLogix on the agent machine.
- Bundle the "fslogix.admx"and "fslogix.adml"files (available in the installation package of FSLogix) into a zip file, for example, `fslogix.zip`.

Import the zip file

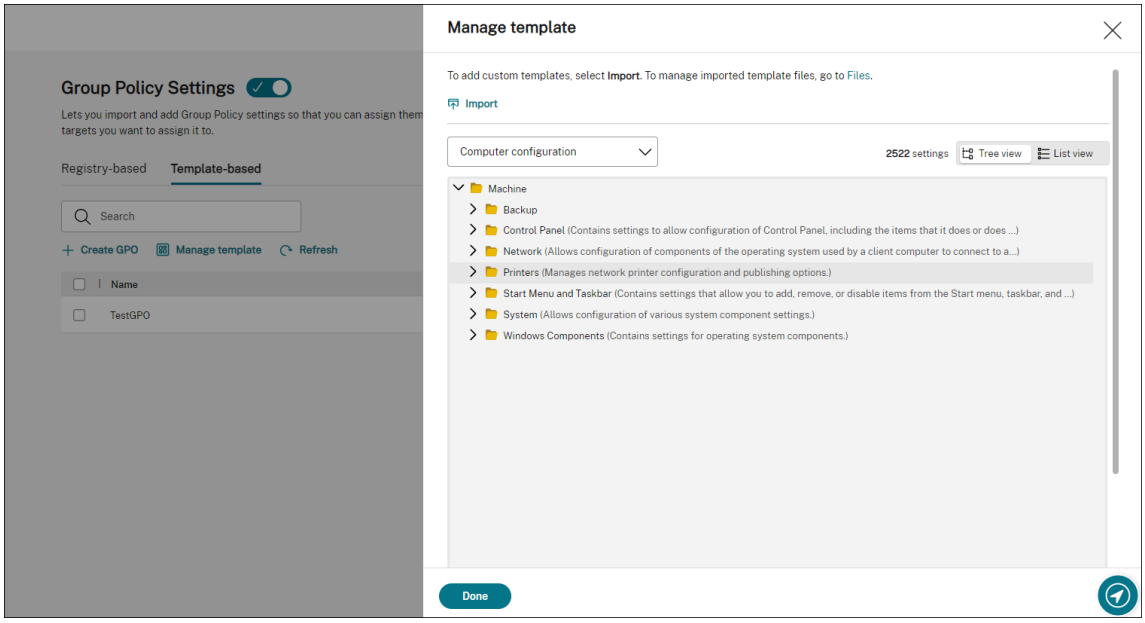
WEM supports creating template-based and registry-based GPOs. To create a template-based GPO for FSLogix, upload the zip file as follows:

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

1. Enable **Group Policy Settings**.

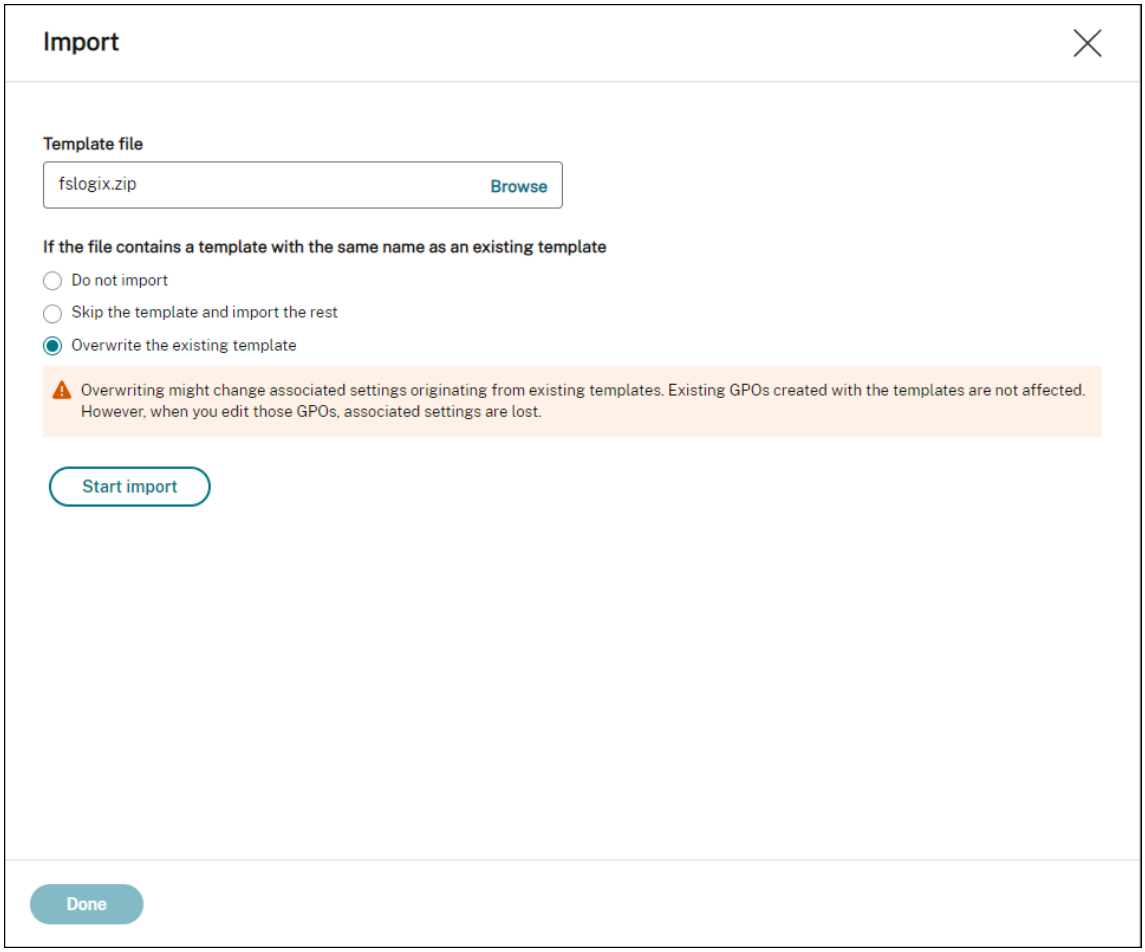


2. On the **Template-based** tab, click **Manage template**. The **Manage template** wizard appears.



3. Browse to the zip file and then click **Start import**.

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



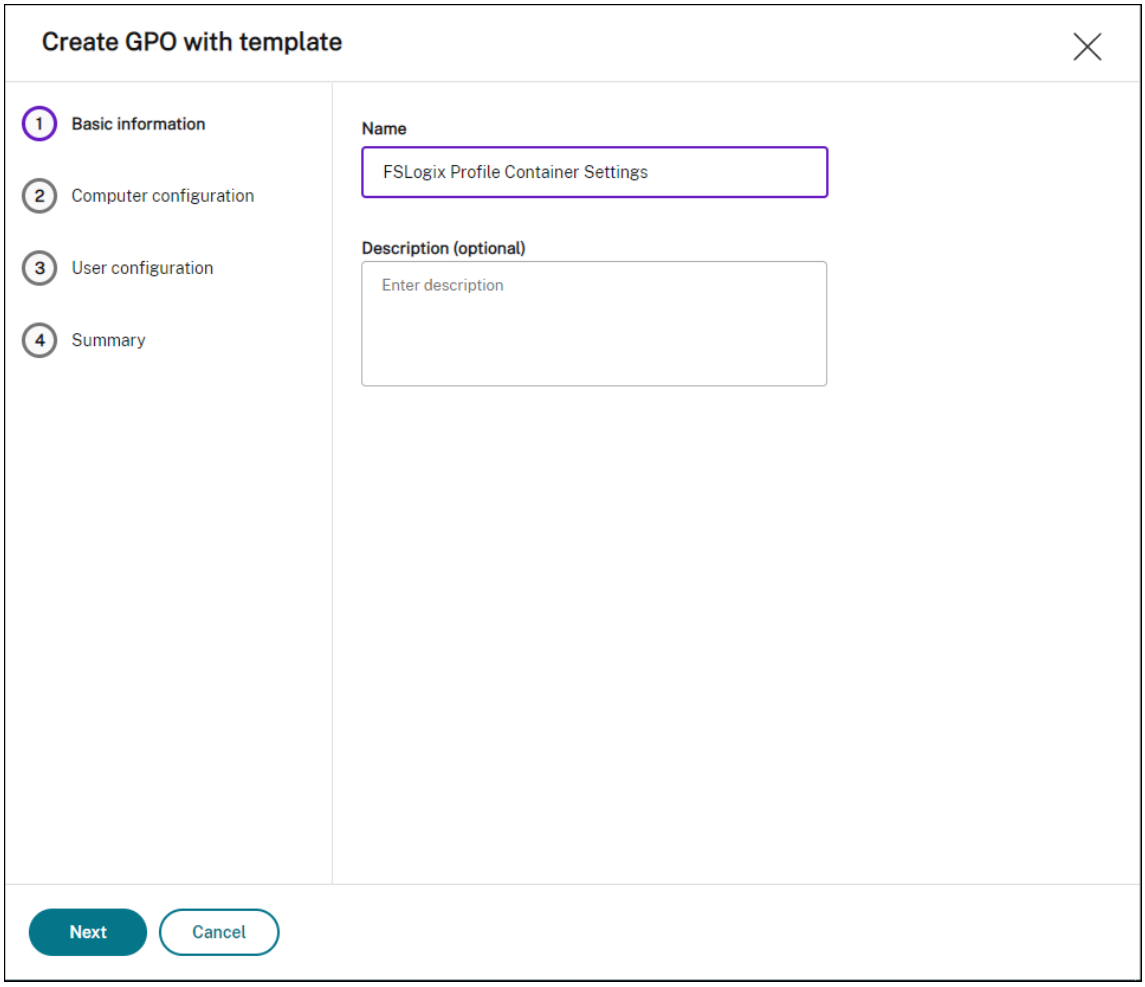
Create and edit a GPO

For a template-based GPO, you can configure both machine-level and user-level settings. In this example, you don't need to configure user-level settings.

Complete the following steps:

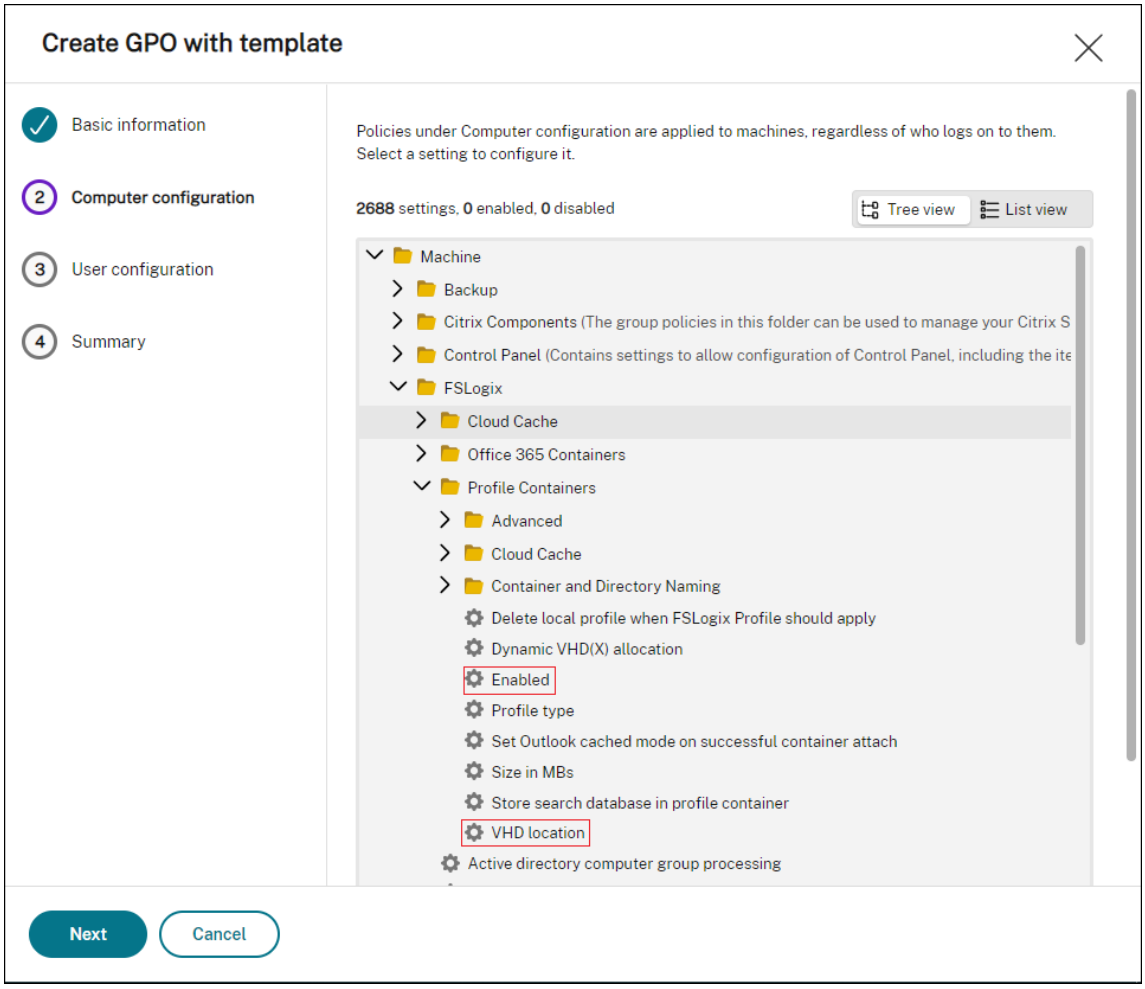
1. On the **Template-based** tab, click **Create GPO**. The **Create GPO with template** wizard appears.
2. In **Basic information**, fill in the required information.

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



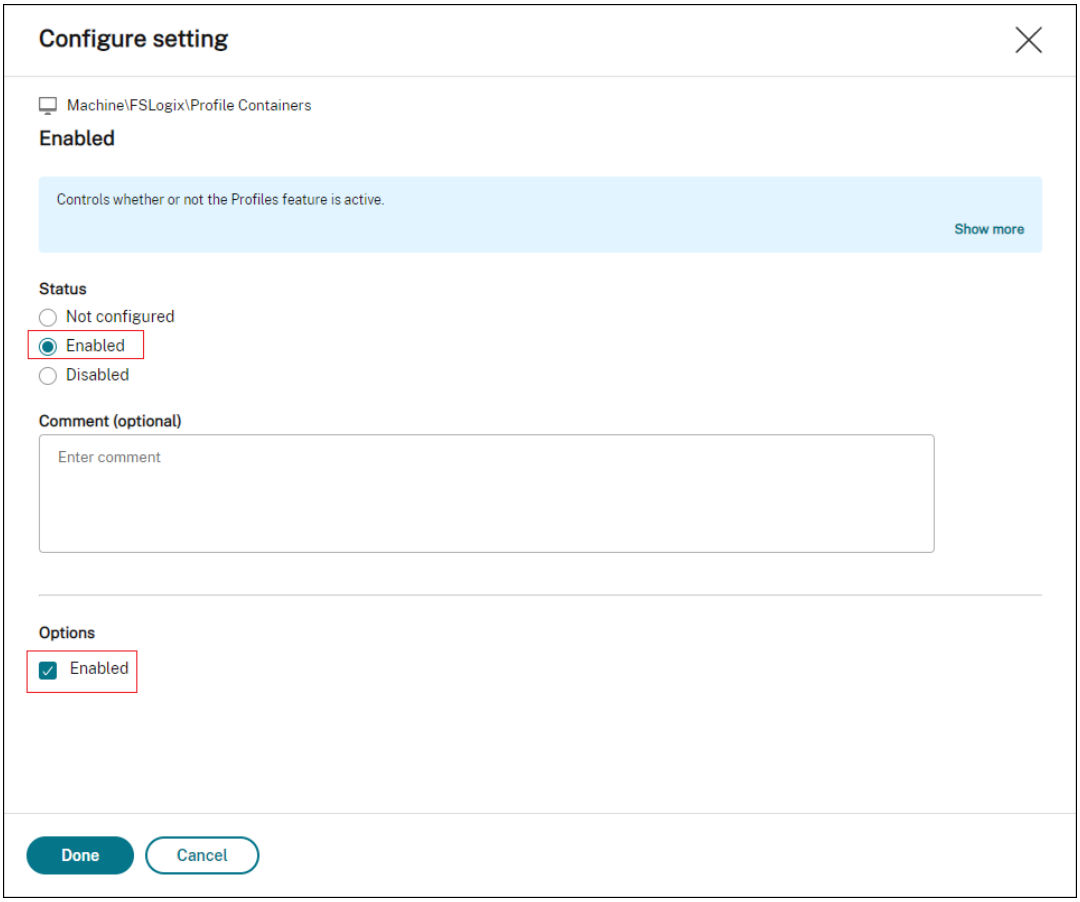
3. In **Computer configuration**, go to **Machine > FSLogix > Profile Containers > Container and Directory Naming** and configure the following two settings:

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



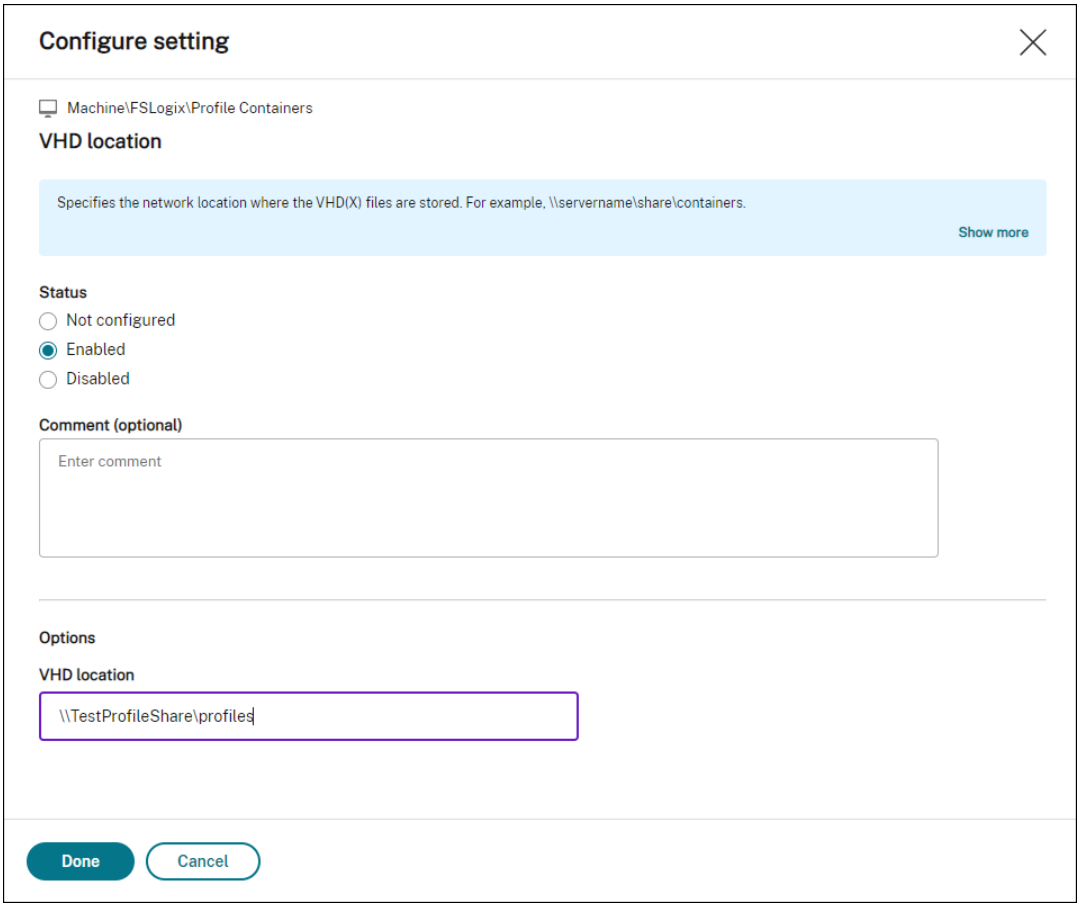
- **Enabled**. Select the setting, set **Status** to **Enabled**, and set **Options** to **Enabled**.

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



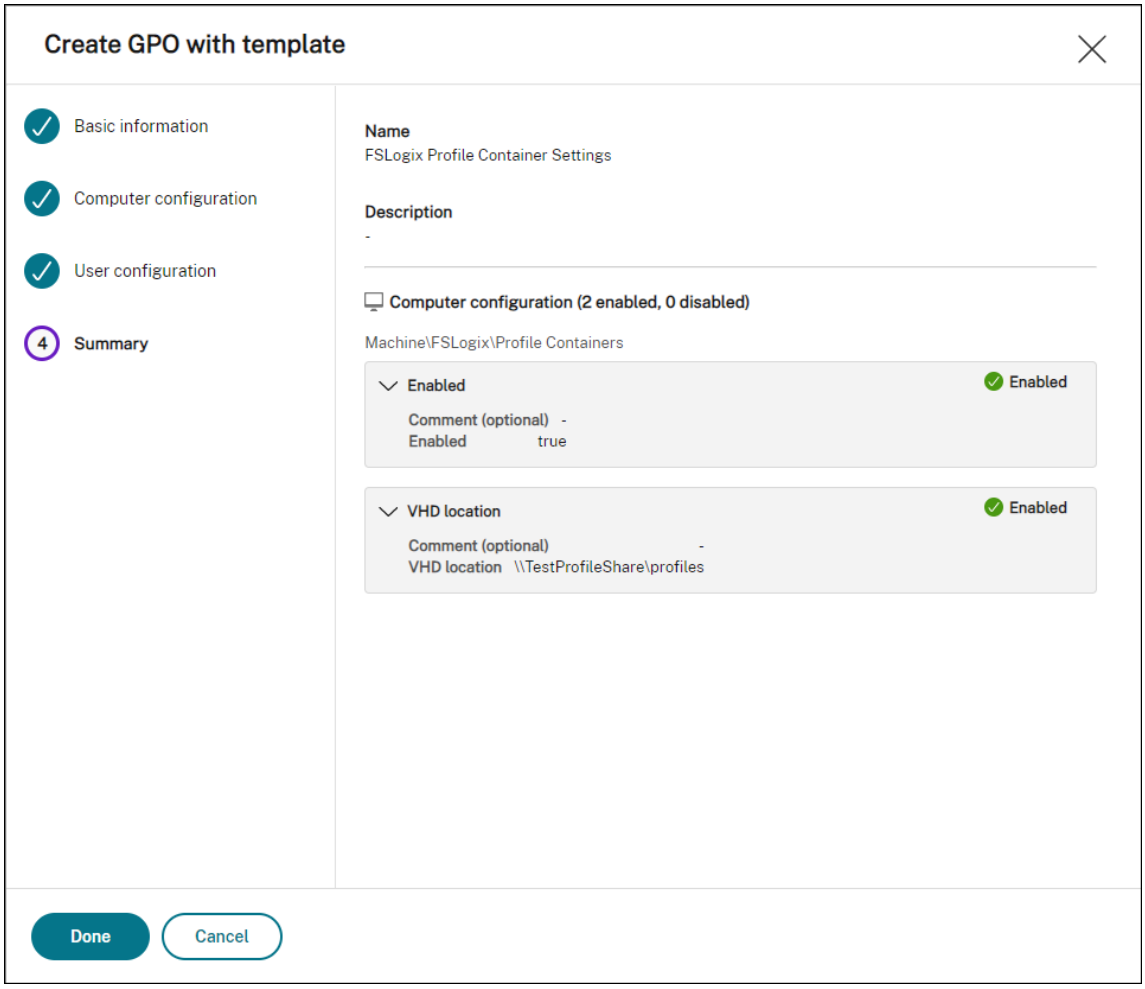
- **VHD location**. Select the setting, set **Status** to **Enabled**, and type the path to the VHD.

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



4. In **Summary**, verify that you configured the settings as intended and click **Done**.

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

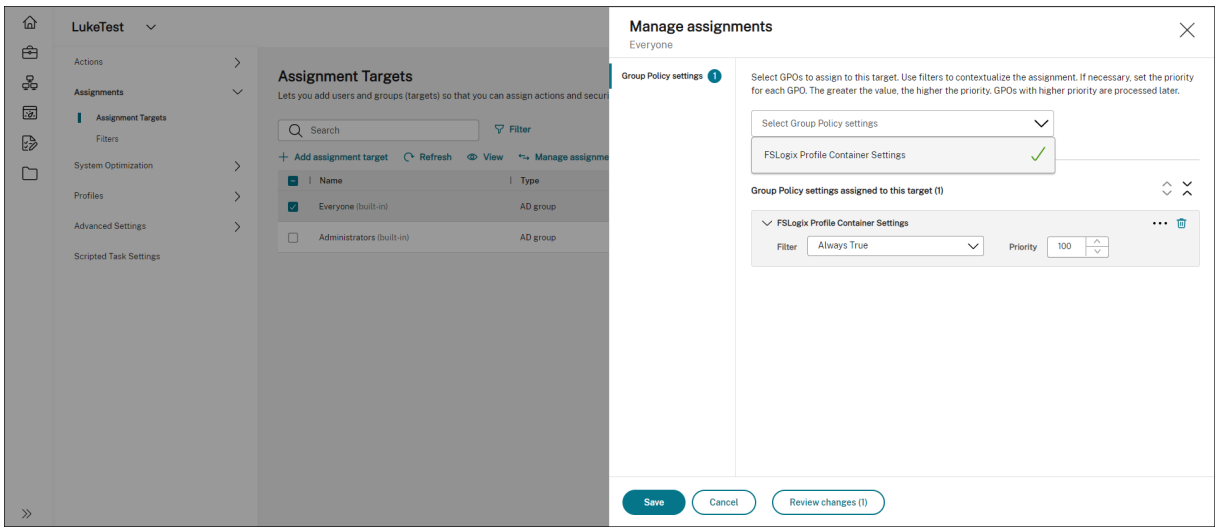


Assign the GPO

After creating the GPO, you can assign it to desired assignment targets. You can assign the GPO to different AD groups, just like you assign other actions. 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.

In this example, the GPO is assigned to the “Everyone”Group, with the default “Always True”filter applied.

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



After assigning the GPO, go to the target agent machine to confirm that the policy has taken effect.

Configure MSIX app attach using scripted and external tasks

September 7, 2025

With Workspace Environment Management (WEM), you can set up MSIX app attach for use in Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) and Citrix Virtual Apps and Desktops environments and on physical workstations. To provide a seamless MSIX app attach based application experience for users, you can roam MSIX app attach data with Profile Management.

The setup process includes the following steps:

- Create scripted tasks
- Create external tasks
- Configure Profile Management

Prerequisites

Before you start, you need to do the following:

- Place an MSIX app attach container (VHDX file) in a file share that Citrix DaaS or Citrix Virtual Apps and Desktops can access. To prepare a VHDX file that contains MSIX applications, use the MSIX packaging tool and the MSIXMGR tool.
- Prepare PowerShell scripts for MSIX app attach. The scripts cover the following four distinct phases to be performed on startup, shut down, sign in, and sign out for MSIX app attach: stage, destage, register, and deregister.

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

Create scripted tasks

Use scripted tasks to implement the functions, such as mounting, staging, destaging, and unmounting MSIX applications. You can also use the scripted task feature with startup and shutdown triggers during machine startup and shutdown to perform the same set of functions.

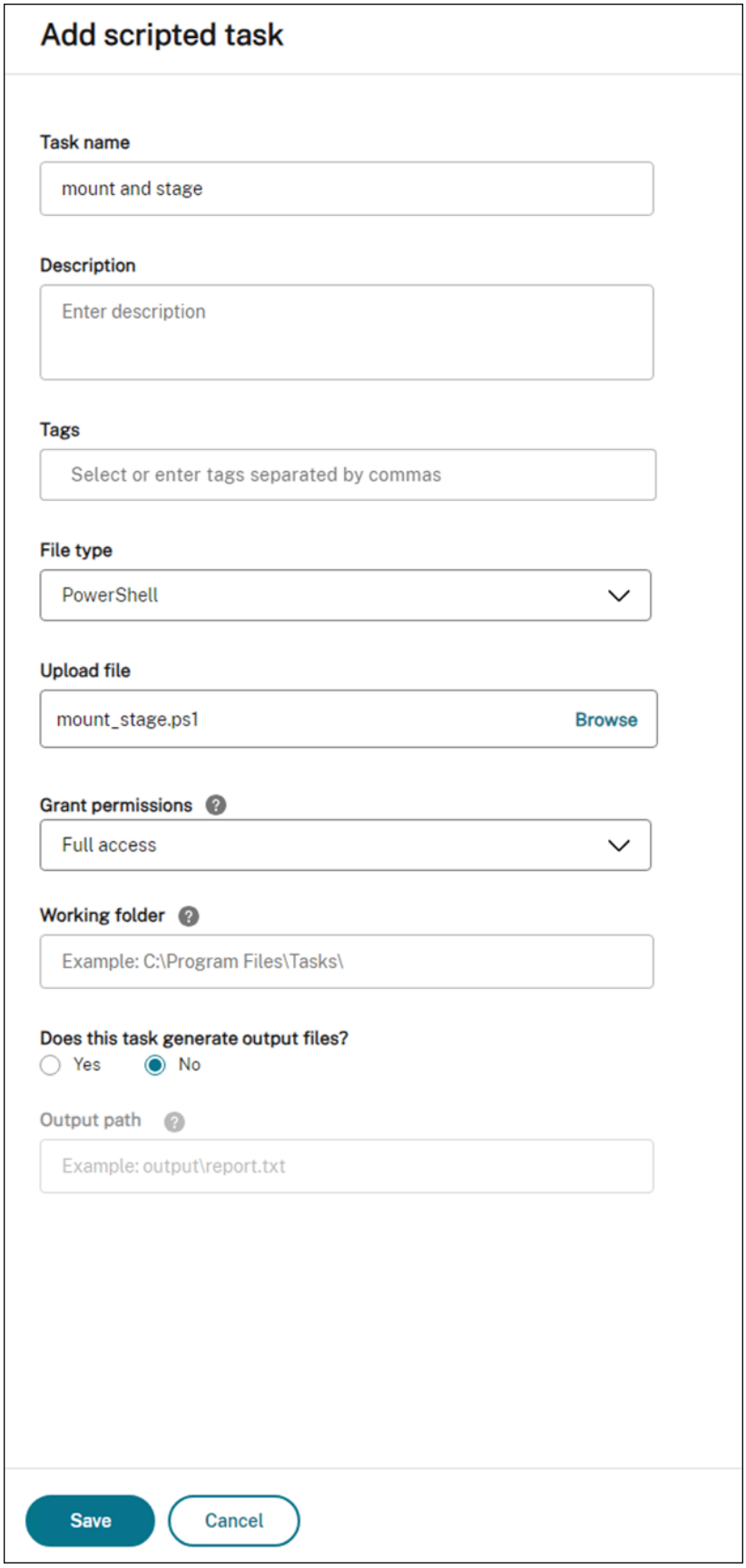
The following information is supplemental to the guidance in Configure startup and shutdown triggers for scripted tasks.

To create scripted tasks, follow the general guidance in that article, minding the details specific to MSIX app attach scenarios.

In **Web Console > Scripted Tasks** of the web console, add the following two tasks:

- A task to mount the MSIX VHD file, stage MSIX app packages during Machine startup.

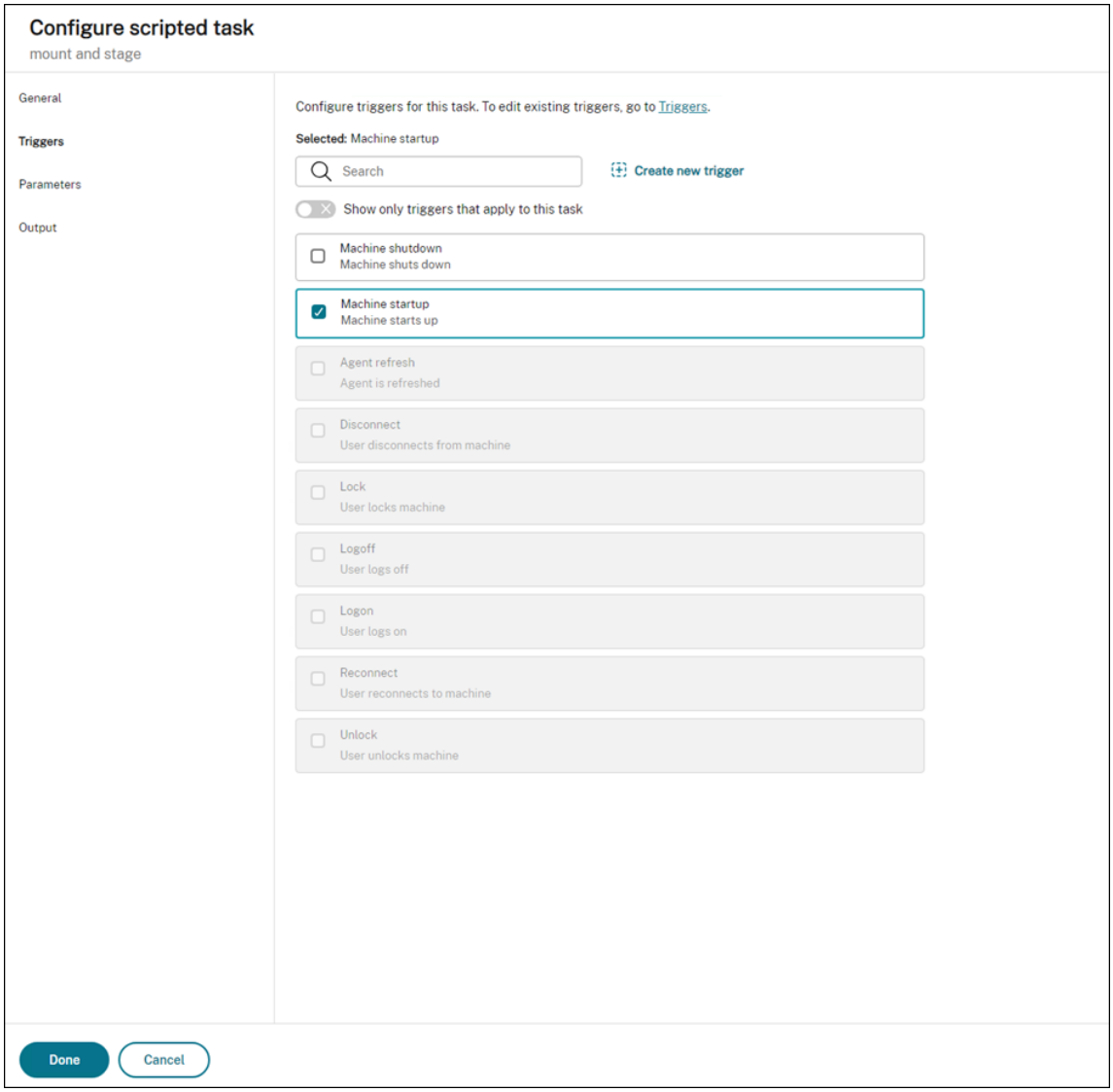
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

For more information, see Add scripted tasks.

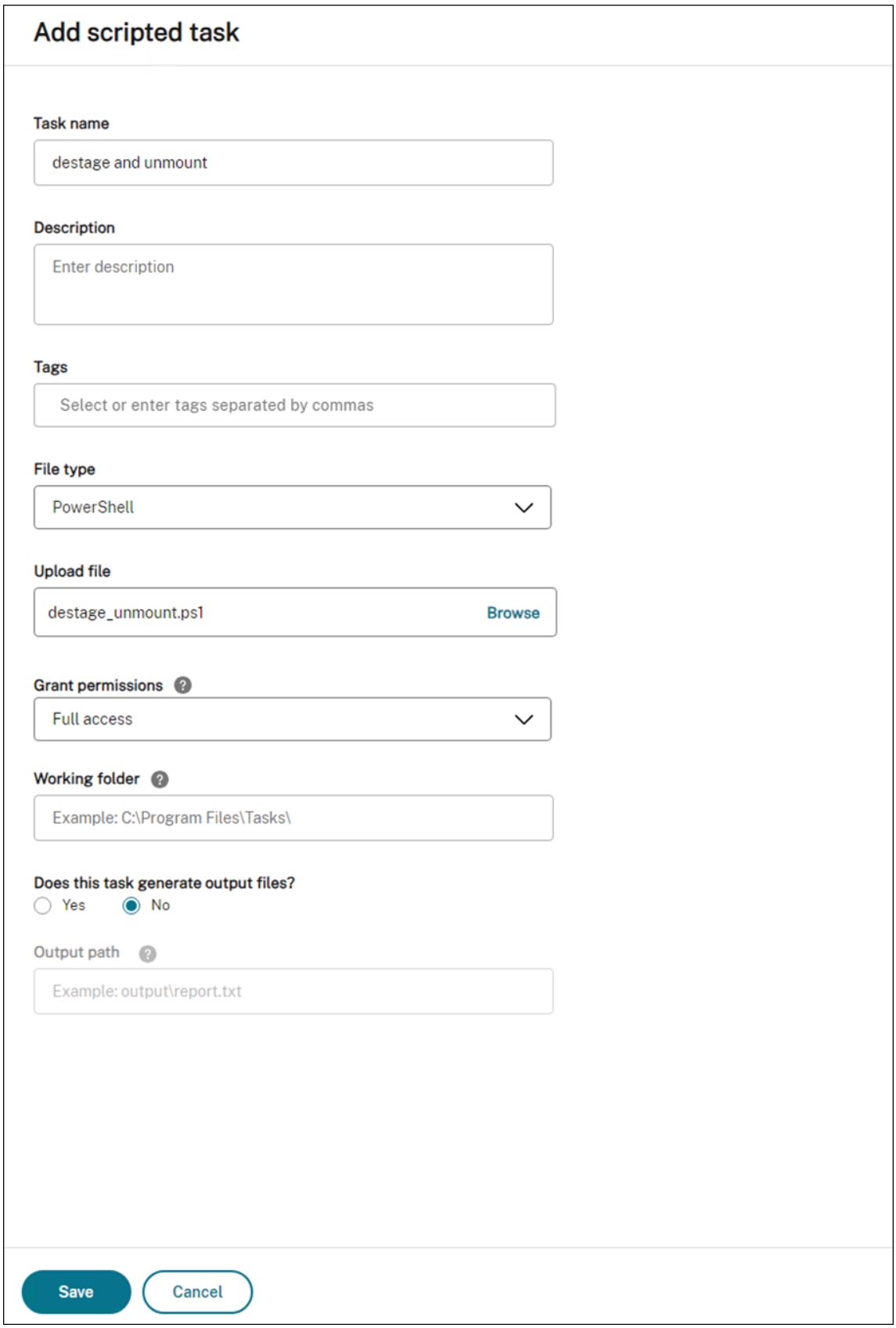
- Configure the triggers for this scripted task during Machine startup.



For more information, see Associate startup and shutdown triggers with scripted tasks.

- A task to remove the MSIX VHD file, destage MSIX app packages during Machine shutdown.

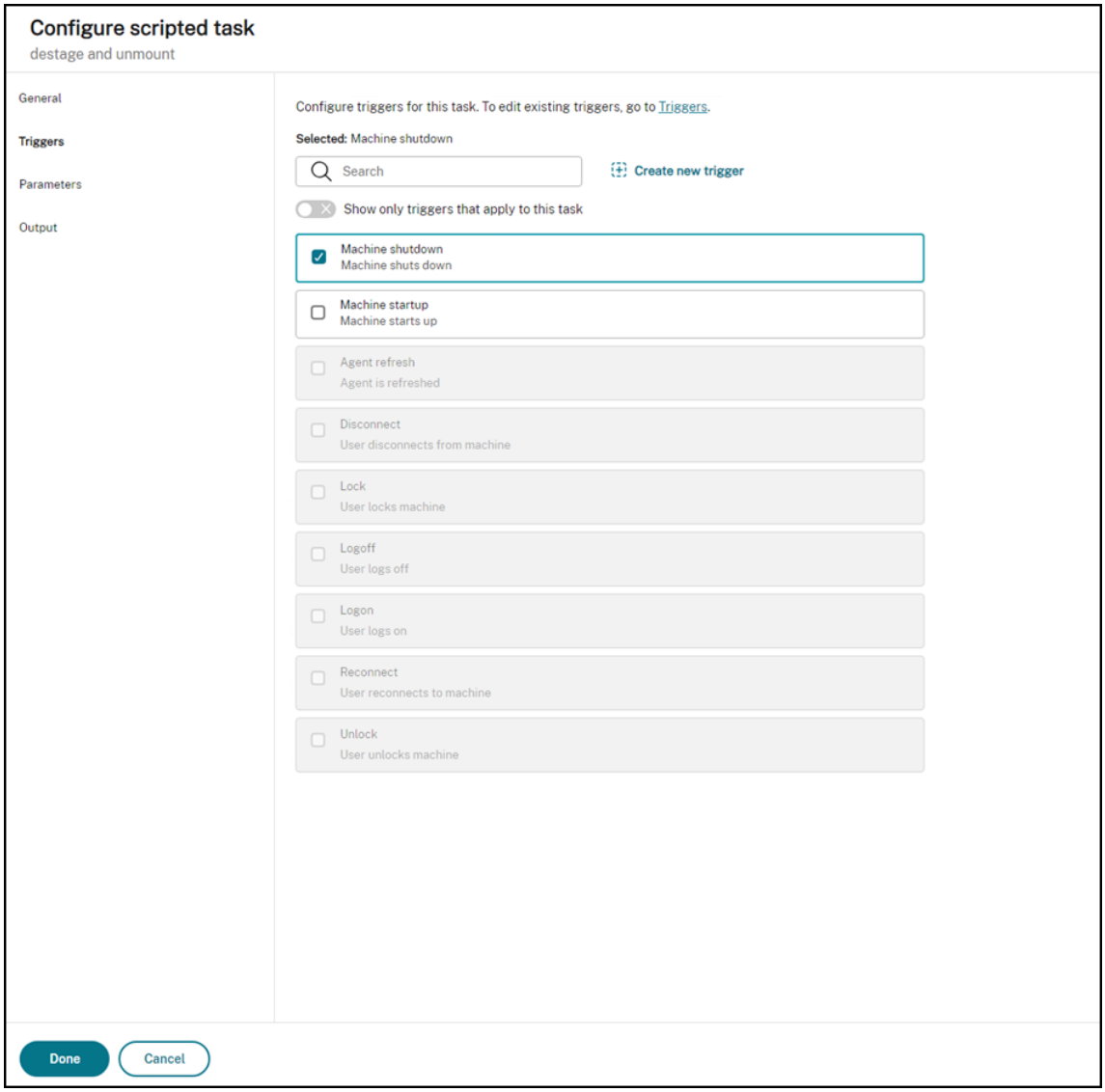
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

For more information, see Add scripted tasks.

- Configure the triggers for this scripted task during Machine shutdown.



For more information, see Associate startup and shutdown triggers with scripted tasks.

Create external tasks

Use external tasks to implement the functions, such as registering, and deregistering MSIX applications.

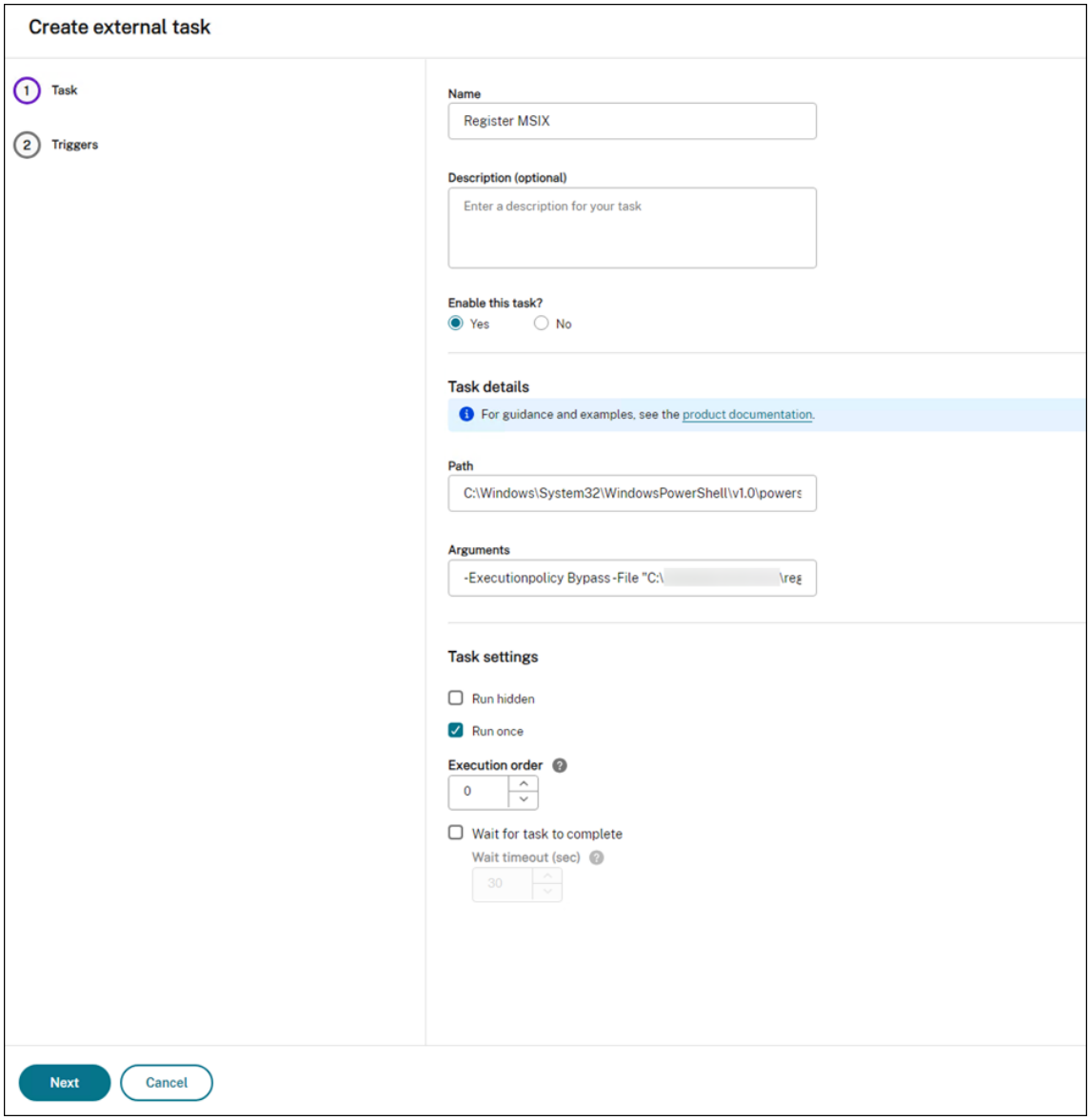
The following information is supplemental to the guidance in External Tasks.

To create external tasks, follow the general guidance in that article, minding the details specific to MSIX app attach scenarios.

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

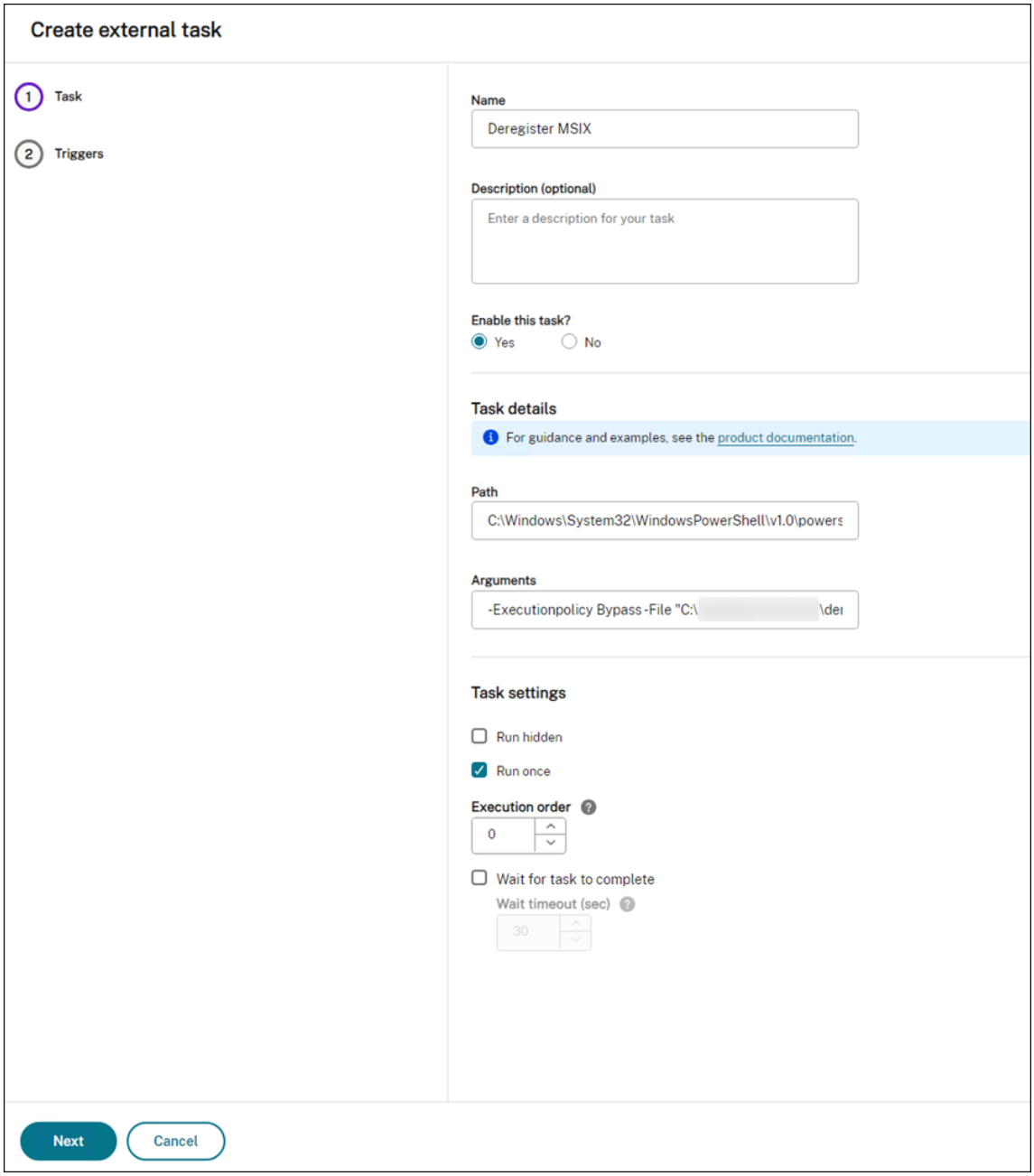
In **Actions > External Tasks** of the legacy console, add the following two tasks:

- A task to register MSIX applications with the desktop session when the end user logs on.



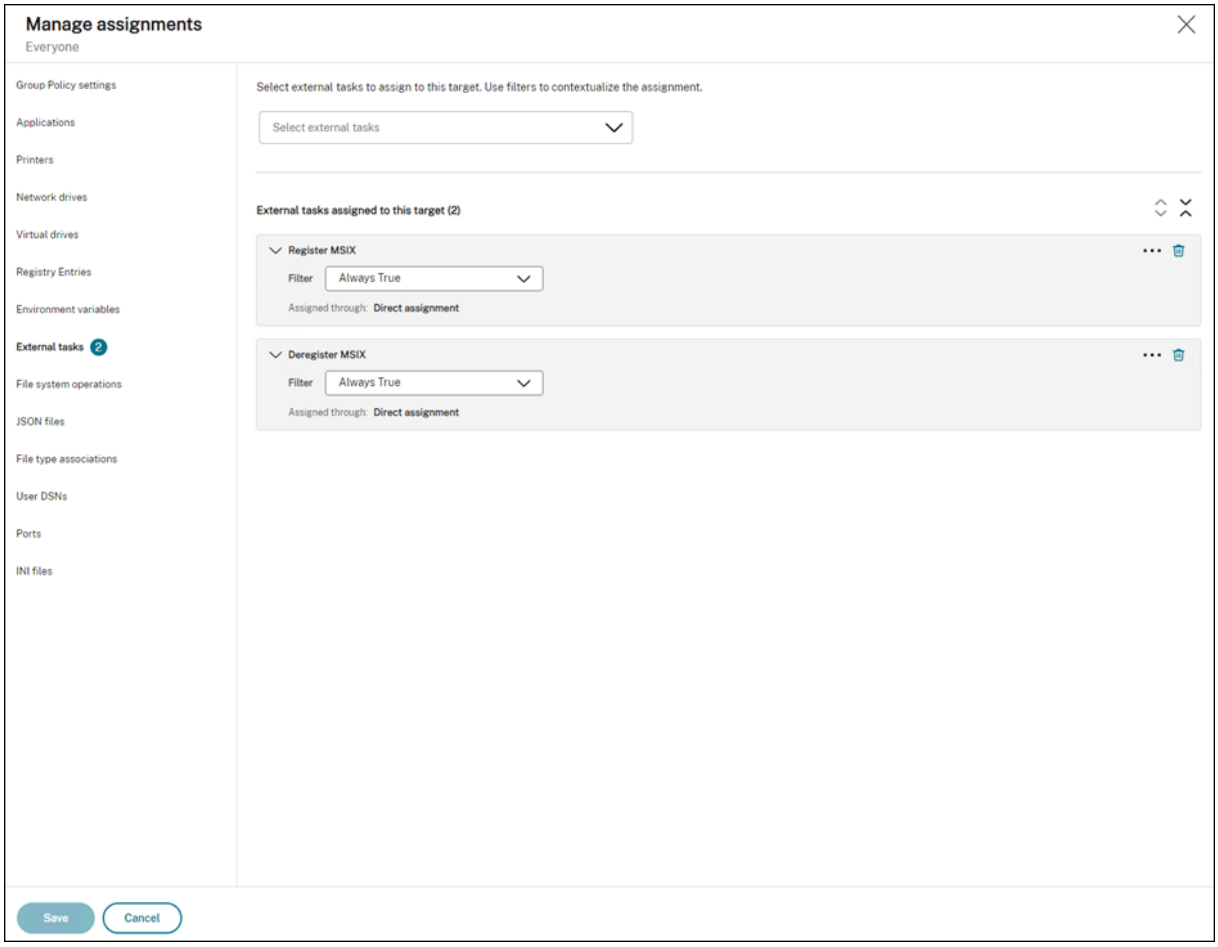
- A task to deregister MSIX applications from the desktop session when the end user logs off.

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



After that, assign the two tasks to the target users you want to enable MSIX app attach for. For information about assigning external tasks, see Assignment. The WEM agent running on the desktop machine will then run the tasks, making the MSIX apps accessible in the desktop session.

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



Configure Profile Management

MSIX app data is saved to the user profile in the user session. To retain MSIX app data in non-persistent desktops or to roam the data across desktops, you can use Profile Management. For information about how to configure profile roaming using Profile Management, see Citrix Profile Management Settings.

Configure Profile Management health check

September 7, 2025

Workspace Environment Management™ (WEM) can check whether Citrix Profile Management is configured optimally on your agent machine.

You might find that the health check returns a warning status in Web Console > Monitoring > Administration > Agents even if Profile Management works properly. The status indicates that not all Profile

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

Management settings are set as recommended. The user experience might be degraded.

To address the issue, use either of the following methods:

- Change settings in **Profiles > Profile Management Settings** under the relevant configuration set.
- Configure the scope of settings to cover in the Profile Management health check report.

Prerequisites

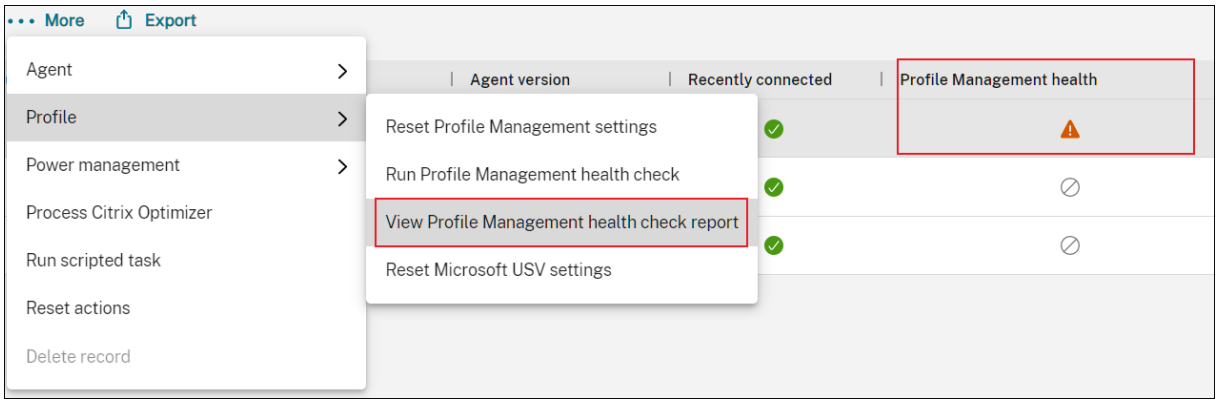
Before you start, make sure that:

- Profile Management is installed and enabled on the agent machine.
- The path to the user store is valid.
- The WEM agent version is 2205.1.0.1 or later.

Check Profile Management health

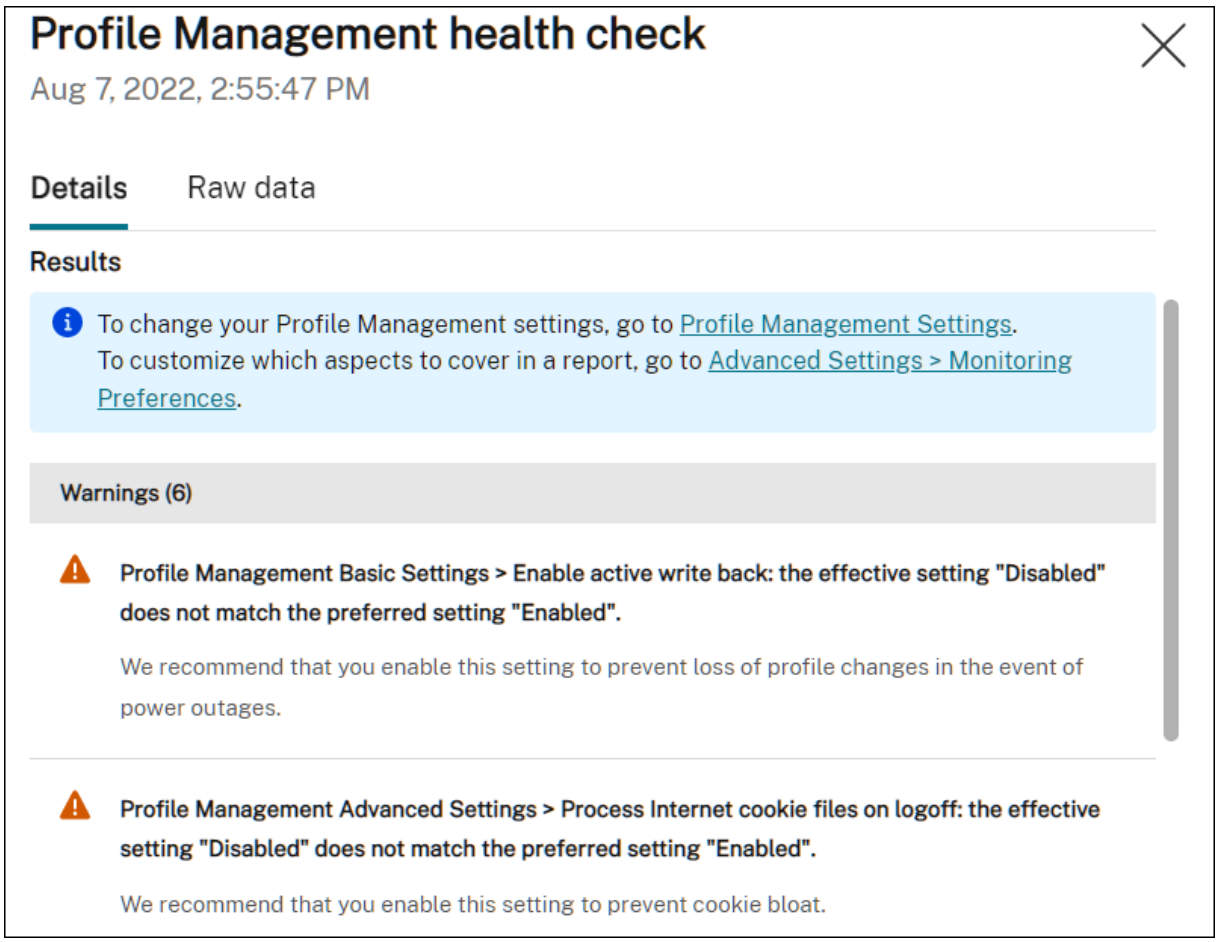
In the web console, go to **Monitoring > Administration > Agents** and check the Profile Management health column. For more information about the health statuses, see Administration.

To view the detailed health check report of an agent, select the agent and then select **More > Profile > View Profile Management health check report**.



The report includes issues found and fix recommendations. For each issue, go to **Profiles > Profile Management Settings** under the relevant configuration set and change the setting accordingly. To dismiss an issue, go to **Advanced Settings > Monitoring Preferences** and specify the scope of settings to cover in the report.

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



When no issue is found, the health check returns a good status, indicating that Profile Management is in good shape.

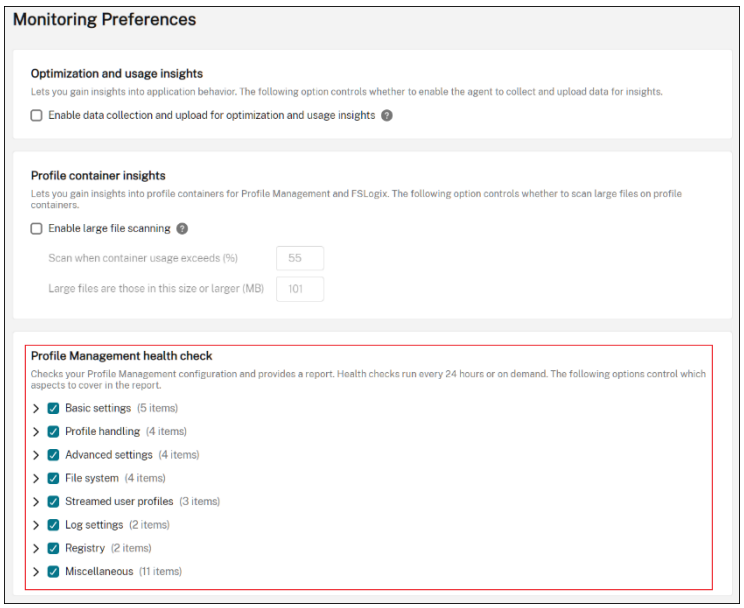
> **Note:**
>
> If the issue is an error, you must fix it in **Profiles > Profile Management Settings** under the relevant configuration set. Otherwise, Profile Management cannot function properly.

Customize the scope of settings to cover in a report

To customize the scope of settings to cover in a health check report, go to **Advanced Settings > Monitoring Preferences** under the relevant configuration set.

By default, all settings are included. For more information, see Advanced Settings.

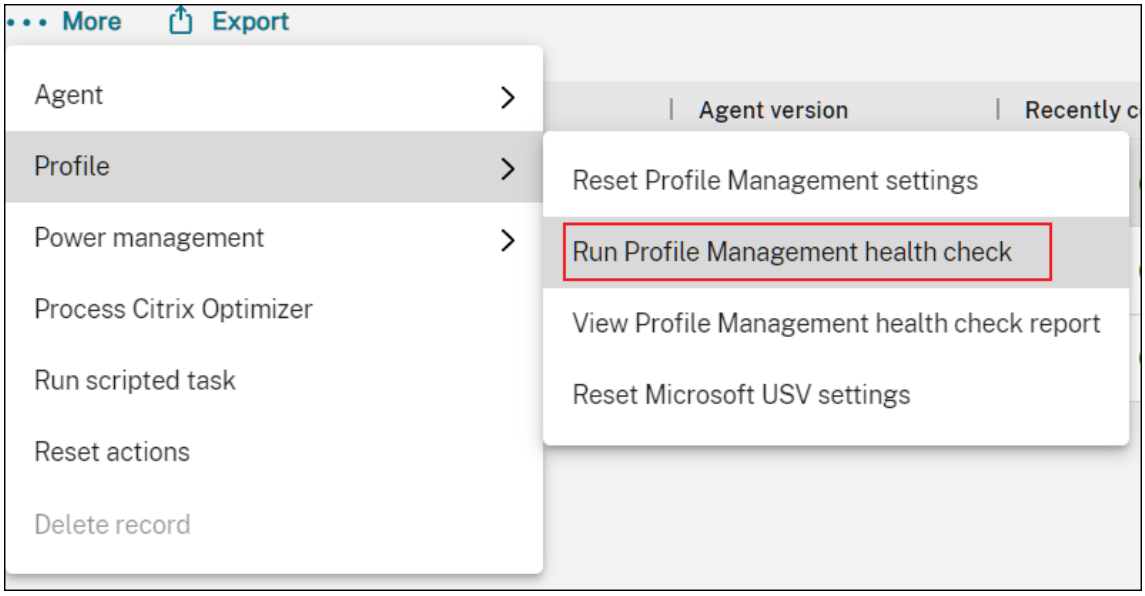
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Run Profile Management health check on demand

To run Profile Management health checks on an agent machine on demand, perform the following steps:

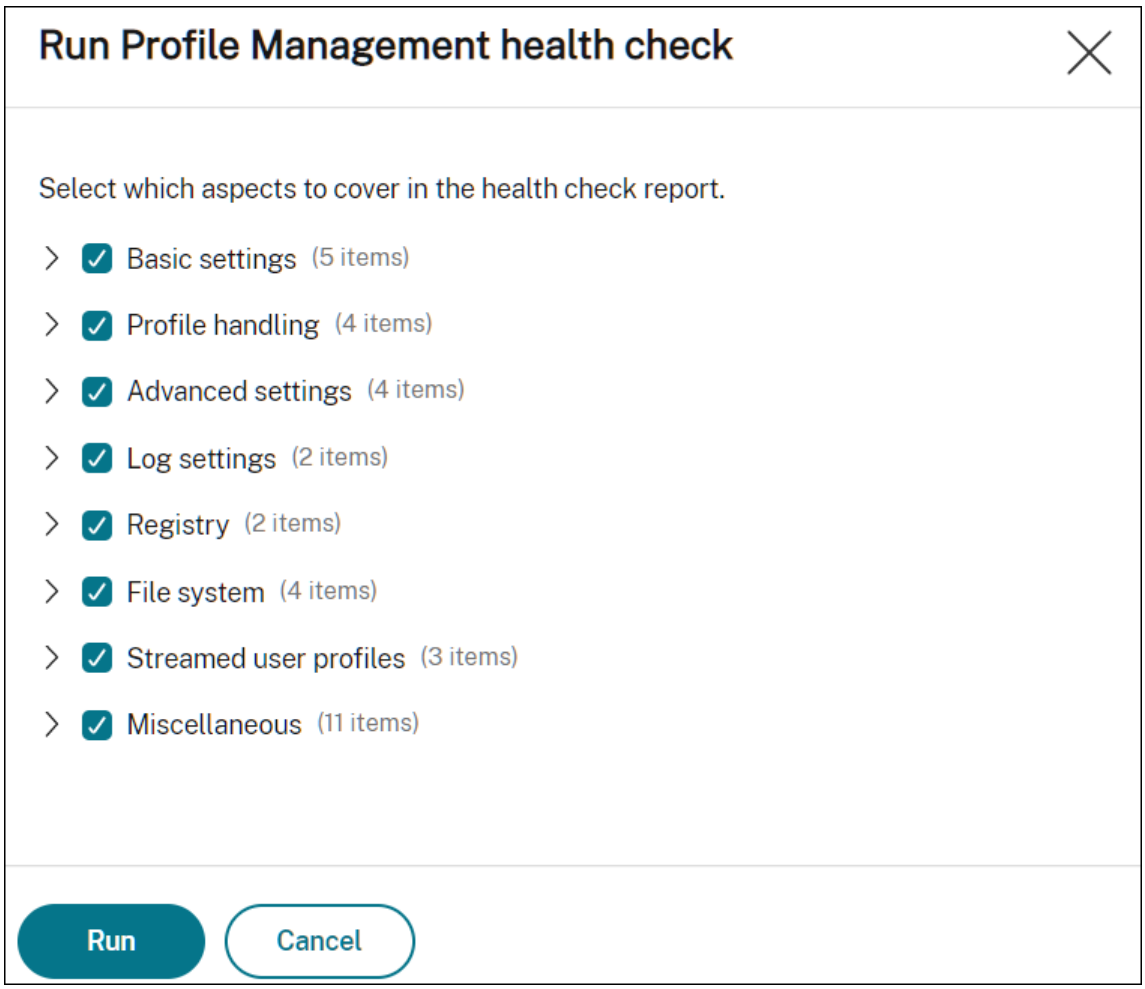
1. In the web console, go to **Monitoring > Administration > Agents**, select the agent, and select **More > Profile > Run Profile Management health check**.



2. In the wizard that appears, choose whether to change the scope of the settings that the health check report covers and then click **Run**.

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

> **Note:**
>
> The changes you make here affect only the health check report to be generated.



Configure SMB shares for Profile Management to use

September 7, 2025

As an administrator who manages user profiles with Citrix Profile Management, you need to specify file shares as user stores.

You might want to put user stores in storage repositories (for example, Azure Files) that the current user has no permission to access. Using Workspace Environment Management™ (WEM) to establish SMB connections to the storage repositories accomplishes that goal. Doing so enables Profile Management to access the user stores.

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

The setup process includes the following steps:

- Configure SMB shares
- Configure Profile Management

Prerequisites

Before you start, do the following:

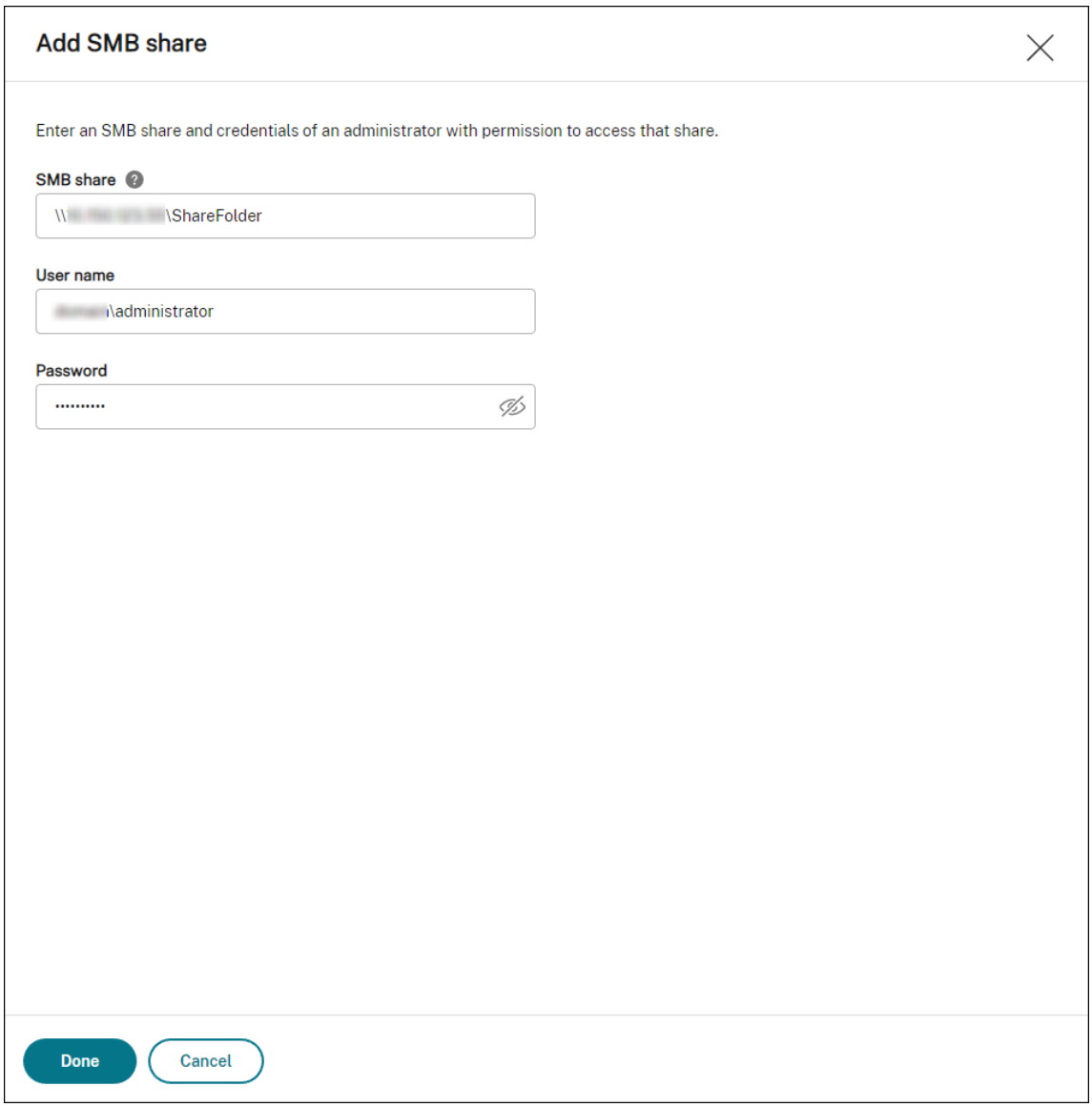
- Prepare a file share that the WEM agent can access.

Configure SMB shares

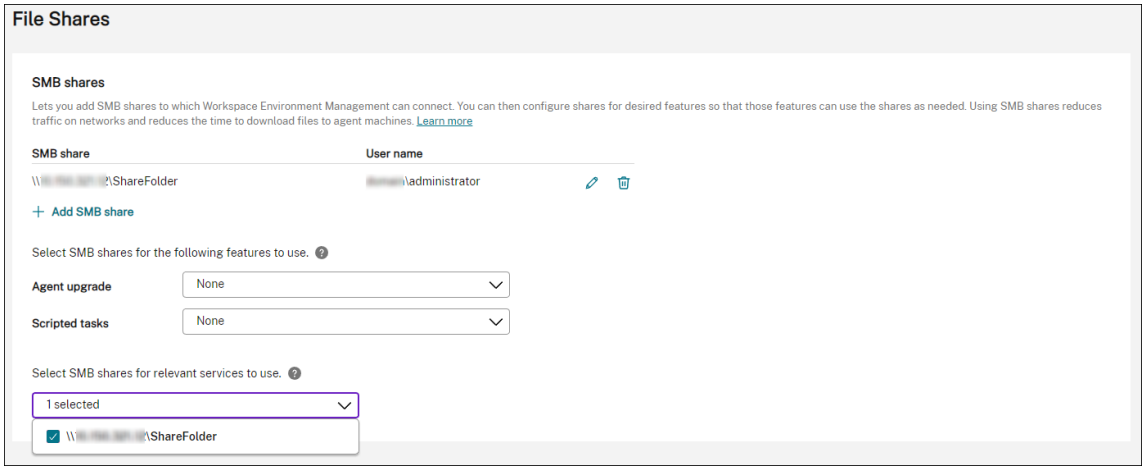
The following information is supplemental to the guidance in SMB shares. Follow the general guidance in that article and mind the details below.

1. In the web console, go to **Advanced Settings > File Shares** under the relevant configuration set and add the SMB share you prepared.

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



2. Select the SMB share that you want the Profile Management service to use.

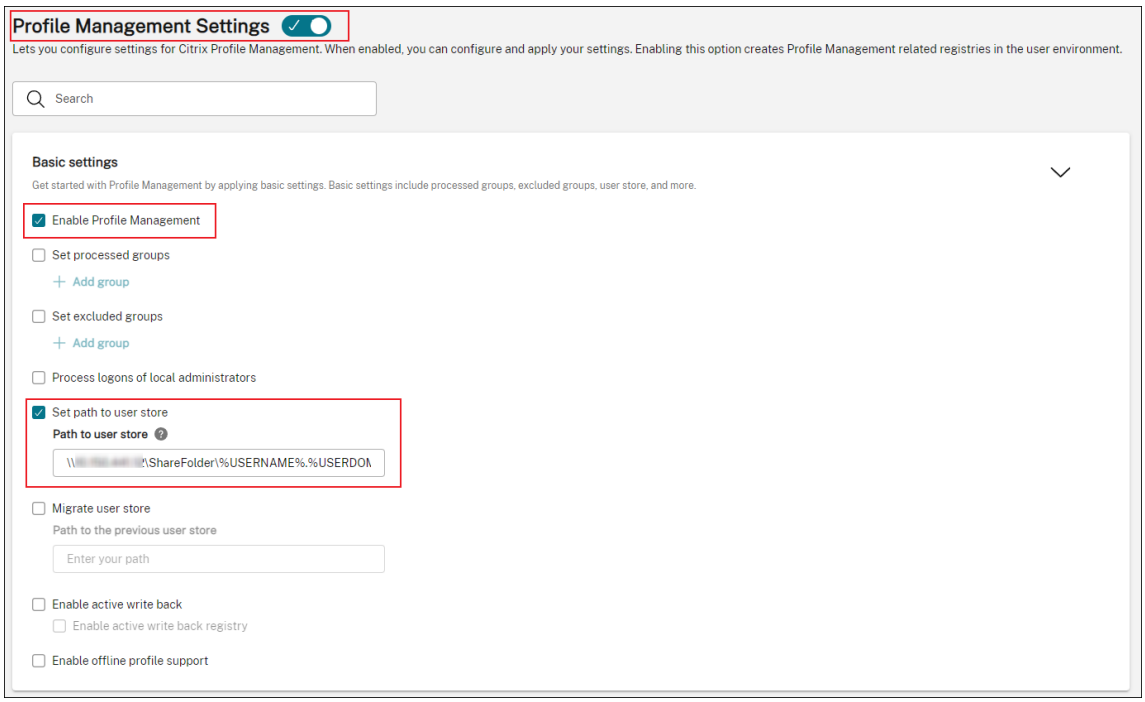


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Profile Management

The following information is supplemental to the guidance in Citrix Profile Management Settings. Follow the general guidance in that article and mind the details below.

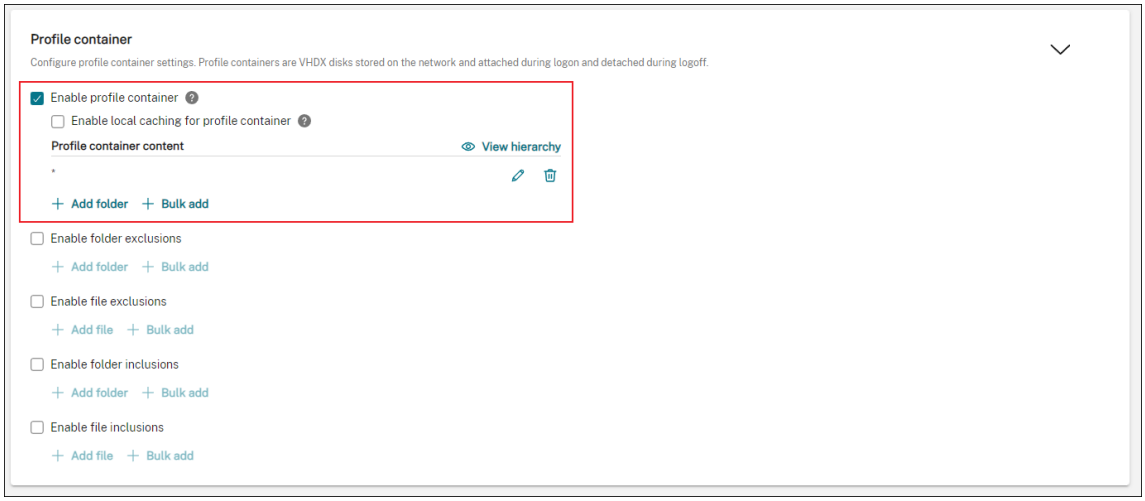
1. In the web console, go to **Profiles > Profile Management Settings** under the relevant configuration set and enable **Profile Management Settings**.
2. Go to **Basic settings**, enable Profile Management, and then set the path to the user store.



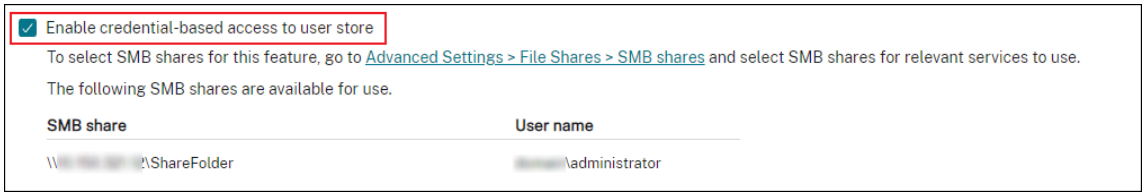
3. Go to **Profile container**, enable profile container, and then add an asterisk (*).

> **Note:**
>
> Adding an asterisk (*) puts the entire user profile in the profile container. This ensures that NTFS permissions are retained.

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



4. Go to **Advanced settings** and enable credential-based access to the user store.



For more information, see Enable credential-based access to user stores.

Configure startup and shutdown triggers for scripted tasks

September 7, 2025

As an administrator, you might want to perform system-level tasks such as configuration or cleanup tasks when the operating system starts or shuts down.

Workspace Environment Management™ (WEM) provides you with machine startup and shutdown triggers that you can associate with scripted tasks. The tasks are triggered to run when the operating system starts or shuts down.

A general workflow to achieve the goal is as follows:

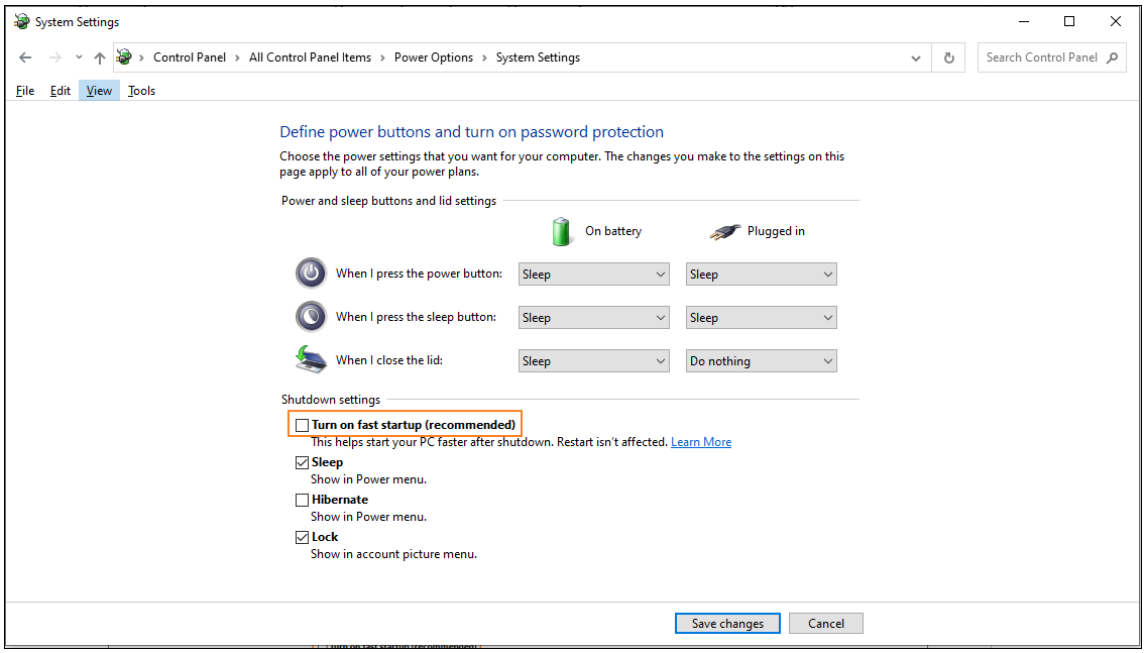
1. Add scripted tasks
2. Associate startup and shutdown triggers with scripted tasks
3. View task execution reports

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

Prerequisites

Before you start, make sure that:

- Fast startup is turned off for the target machines. Example: for Windows 10 machines, go to **Control Panel > All Control Panel Items > Power Options > System Settings** and disable the **Turn on fast startup** option. The option affects only startup processing.



- The scripted tasks are signed with trusted certificates and the certificates are installed on the target machines.

Recommendation

We recommend that you sign the scripted tasks with trusted certificates.

Add scripted tasks

The following information is supplemental to the guidance in Scripted Tasks. Follow the general guidance in that article and mind the details below.

This example adds two scripted tasks:

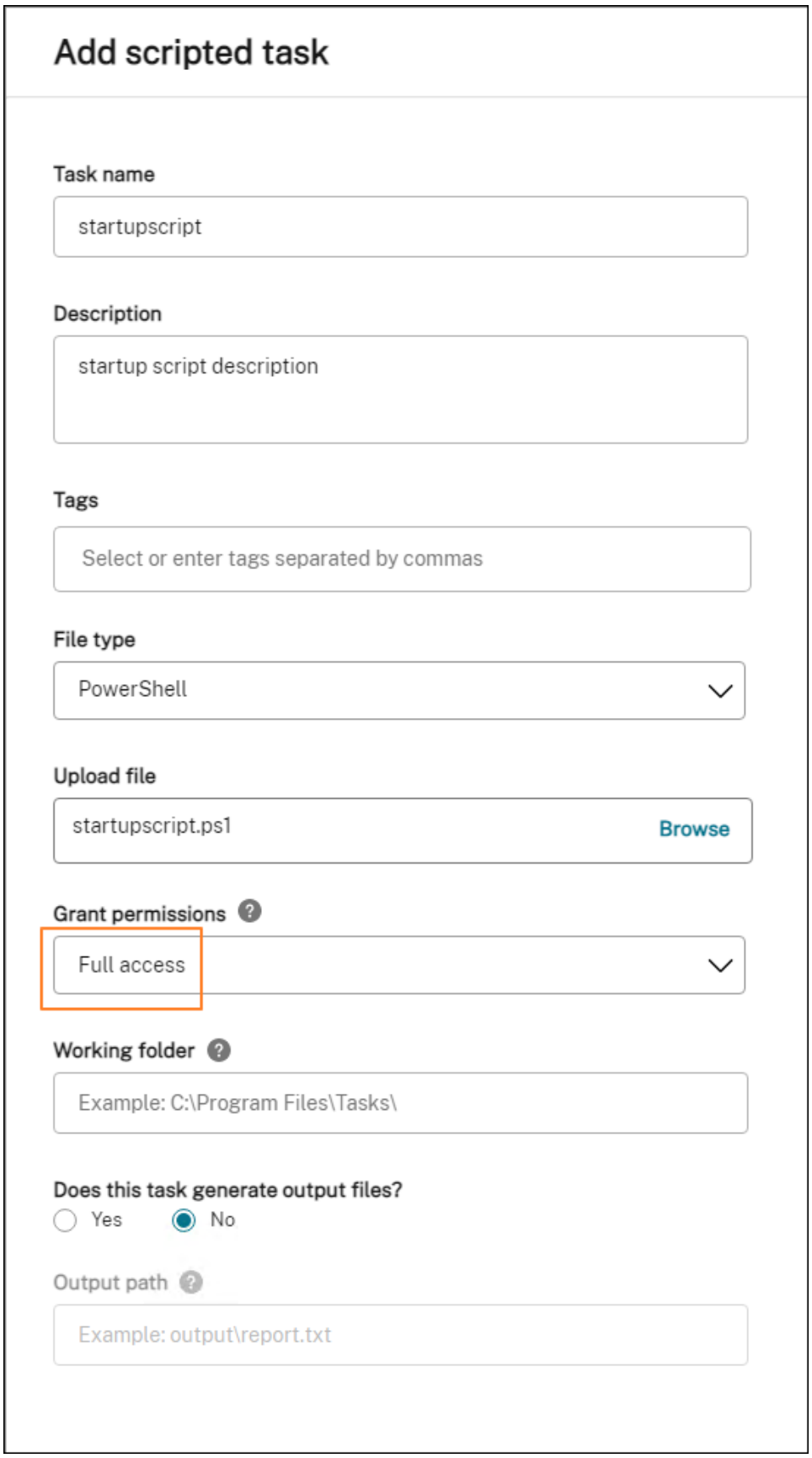
- Task 1: `startupscript` - Includes scripts to run on startup.
- Task 2: `shutdownscript` - Includes scripts to run on shutdown.

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

> **Tip:**
>
> You can combine the two scripts into one so that you just need to add a single task.

1. In **Web Console > Scripted Tasks**, first add the `startupscript` task as follows:

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



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

In this example:

- For **File type**, select **PowerShell**.
- Browse to the PowerShell file to upload it.
- For **Grant permissions**, select **Full access**.

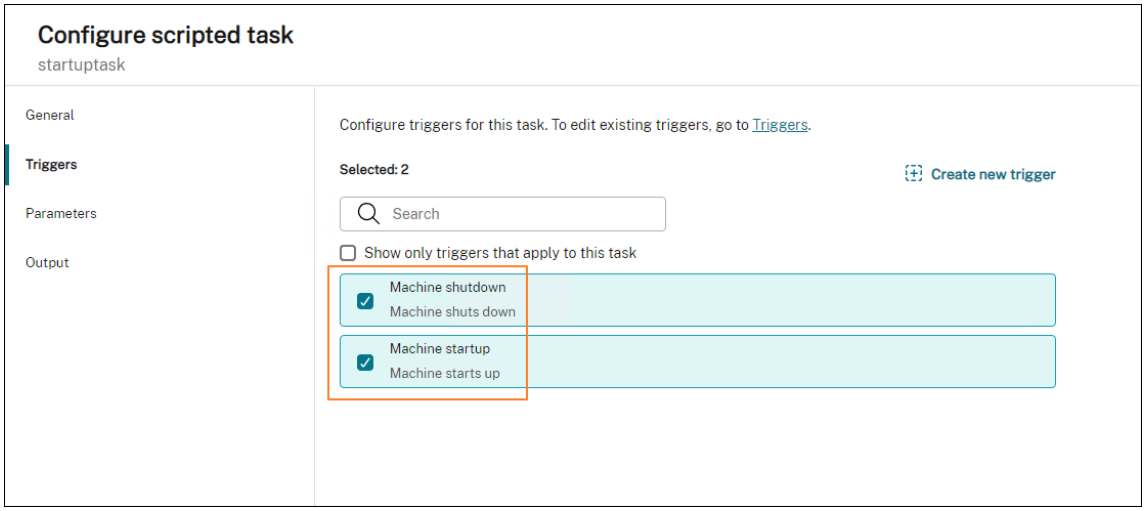
2. Repeat step 1 to add the `shutdownscript` task.

Associate startup and shutdown triggers with scripted tasks

The following information is supplemental to the guidance in Scripted Task Settings. Follow the general guidance in that article and mind the details below.

Go to the relevant configuration set, navigate to **Scripted Tasks Settings,** and configure the two tasks as follows:

- In **Triggers**, select **Machine startup** for the `startupscript` task and select **Machine shutdown** for the `shutdownscript` task.

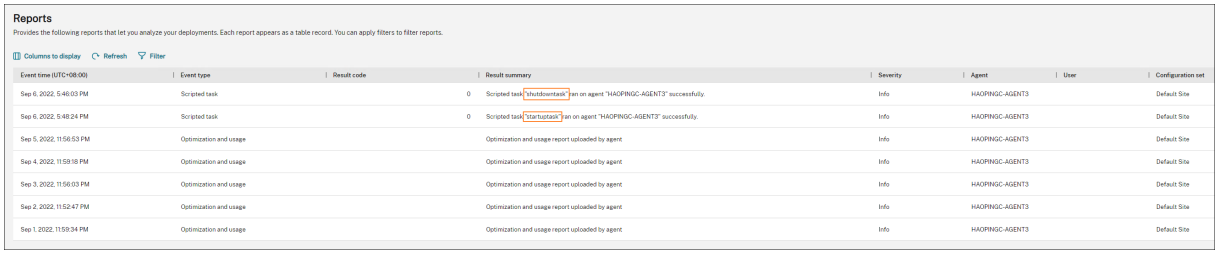


For your changes to take effect immediately, go to **Monitoring > Administration > Agents** and select **Refresh agent host settings**.

View task execution reports

After the tasks run successfully, you can view the results by checking the reports. For more information, see Reports. In this example, you can see the following two reports: One for shutdown and the other for startup.

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



Manage DaaS-provisioned non-domain-joined machines using WEM

September 7, 2025

You can use Workspace Environment Management™ (WEM) to manage non-domain-joined-machines provisioned in Citrix DaaS.

To achieve the goal, do the following:

1. Go to **DaaS > Manage > Full Configuration > Machine Catalogs** to locate the catalog you want to manage using WEM.
2. Select the catalog and then select **Manage Configuration Set** in the action bar.
3. Select a configuration set to which you want to bind the catalog.
4. In WEM, apply settings to the machines by configuring the configuration set.

Prerequisites

Before you start, verify that the following prerequisites are met:

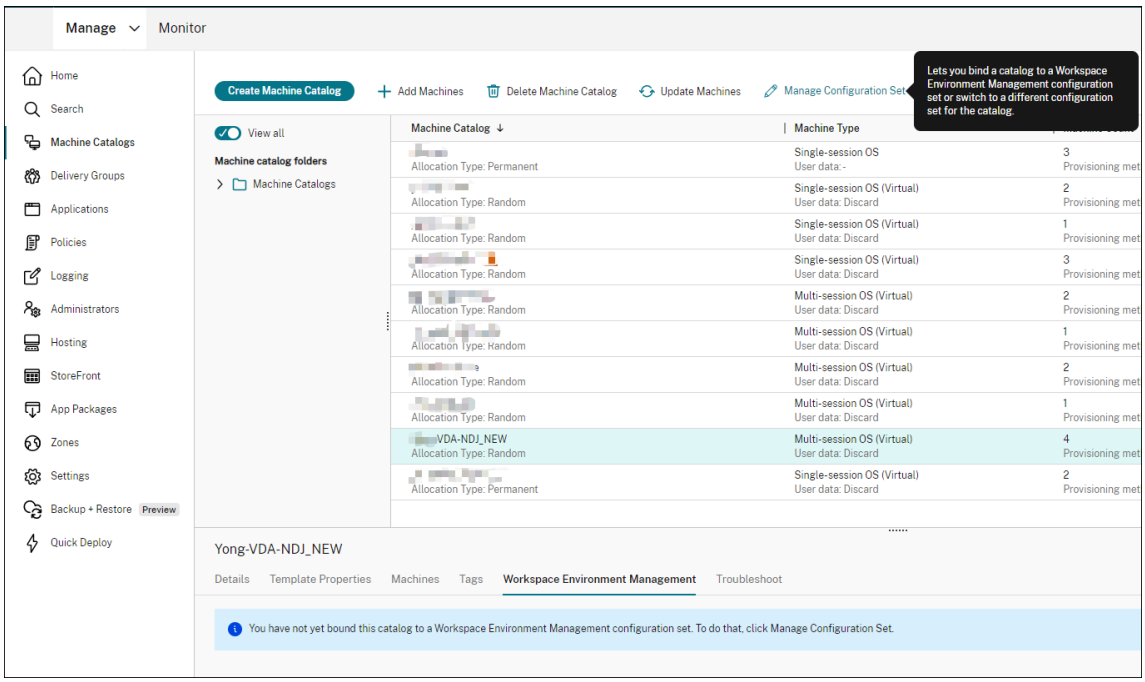
- WEM agent version 2103.2.0.1 or later.
- Agents installed with **Skip Configuration** selected. See Install agents.

Manage configuration set for a catalog

To manage configuration set for a catalog, do the following:

1. Sign in to Citrix Cloud.
2. Navigate to **My Services** > **DaaS > Manage > Full Configuration > Machine Catalogs**.
3. Select the catalog and then select **Manage configuration set** in the action bar. The **Manage configuration set** blade appears.

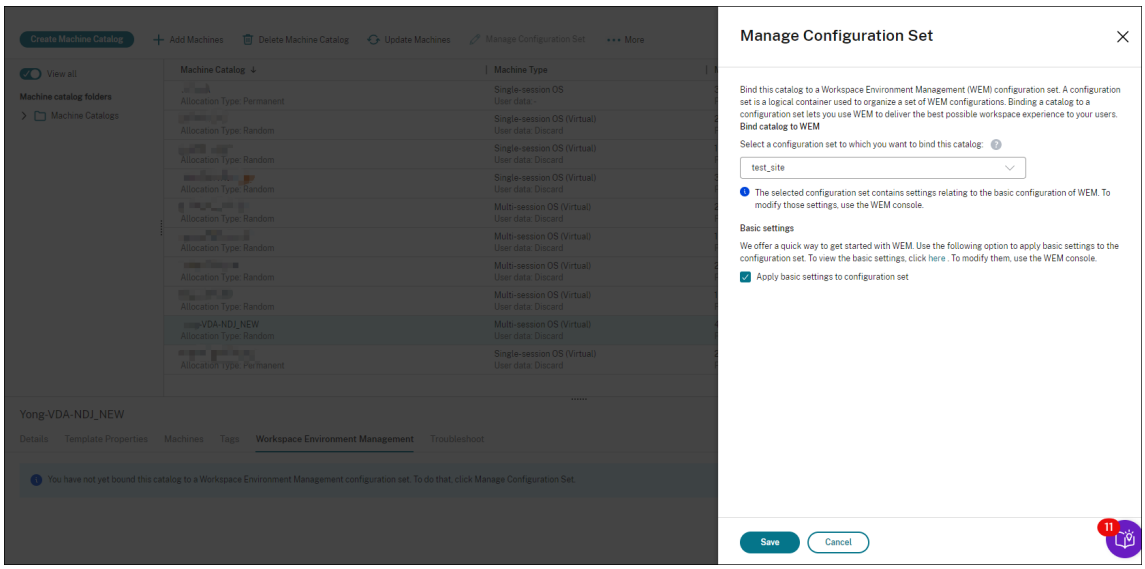
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Select a configuration set to which you want to bind the catalog.

> **Note:**
>
> If the selected configuration set has not been configured to include settings relating to the basic configuration of WEM, the **Apply basic settings to configuration set** option appears. We recommend that you select the option to apply basic settings to the configuration set.

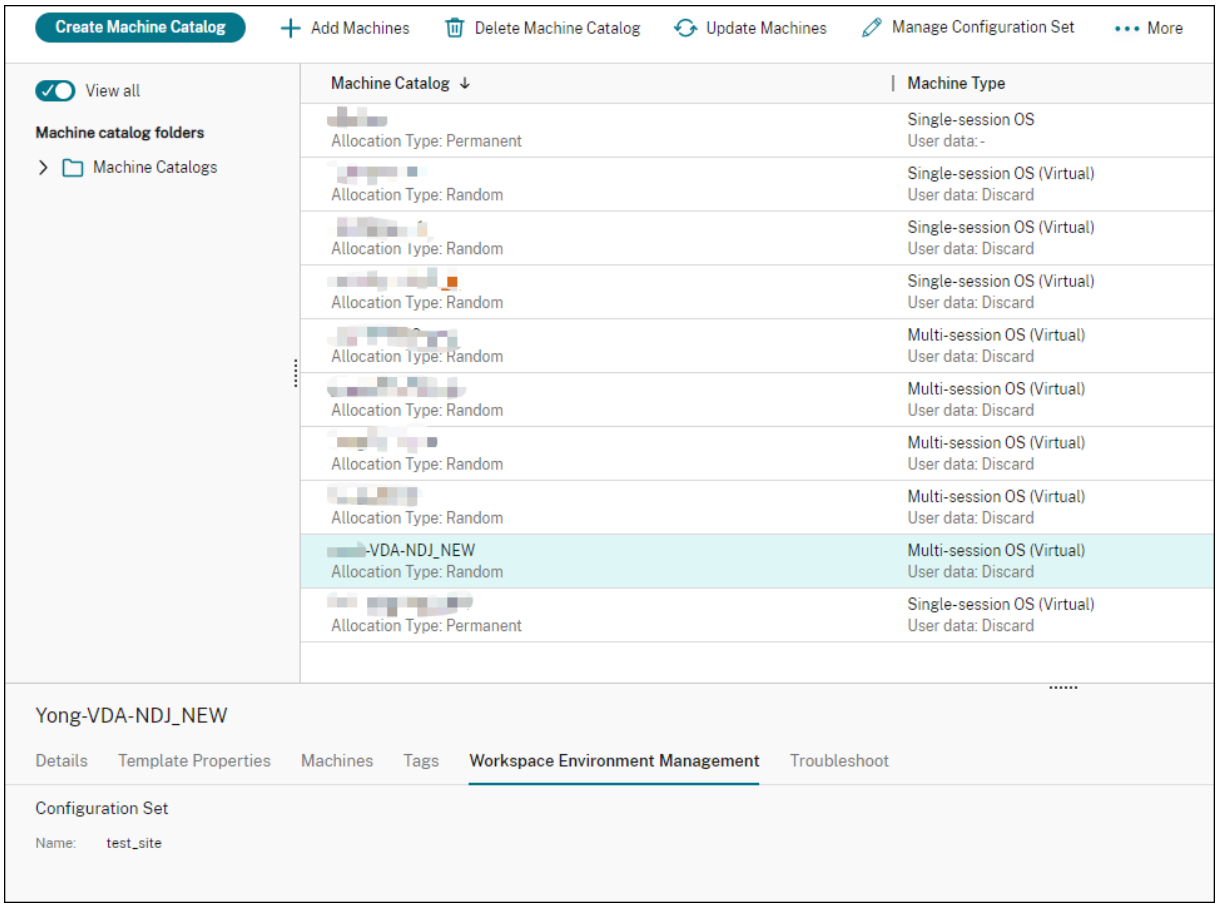
5. After you have finished, click **Save** to save your change and exit the blade.



To verify which configuration set the catalog is bound to, select the catalog and check the **Workspace Environment Management** tab in the lower pane. The tab shows the configuration set to which the

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

catalog is bound.

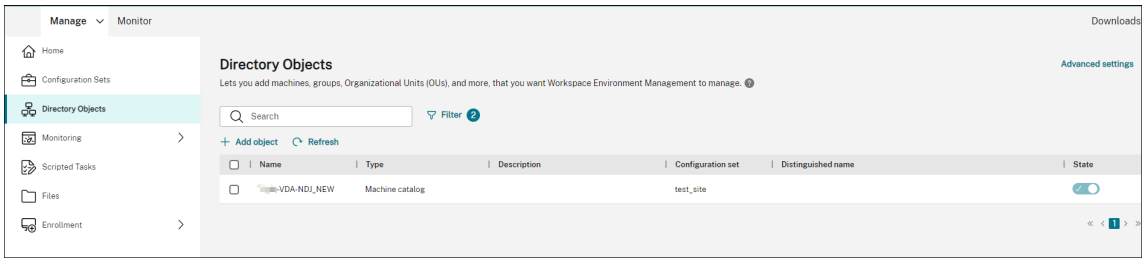


For more information, see Manage configuration set for a catalog in the DaaS documentation.

Apply settings to non-domain-joined machines

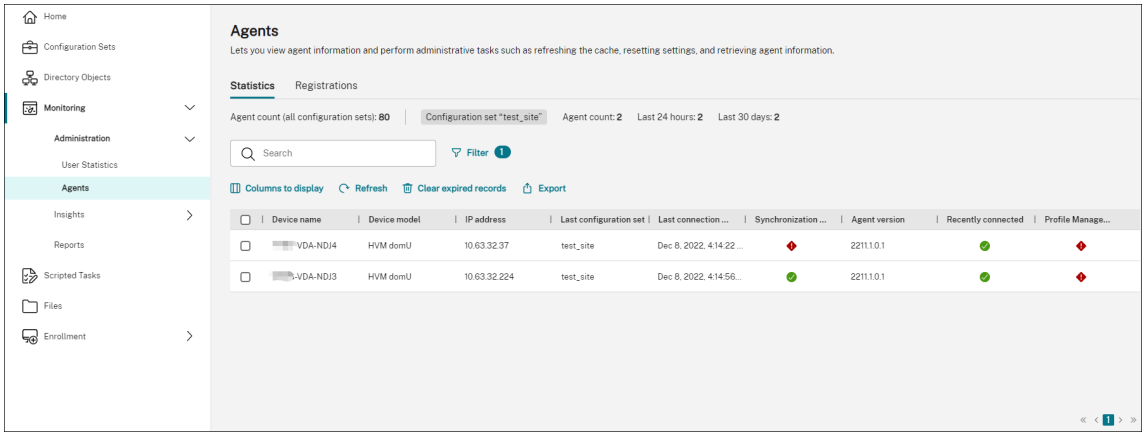
Before configuring settings, you can first view relevant information in WEM:

- In DaaS, go to **Manage > Environment Management (Web)**.
- In **Directory Objects**, check the non-domain-joined machines and the configuration set to which those machines are bound.

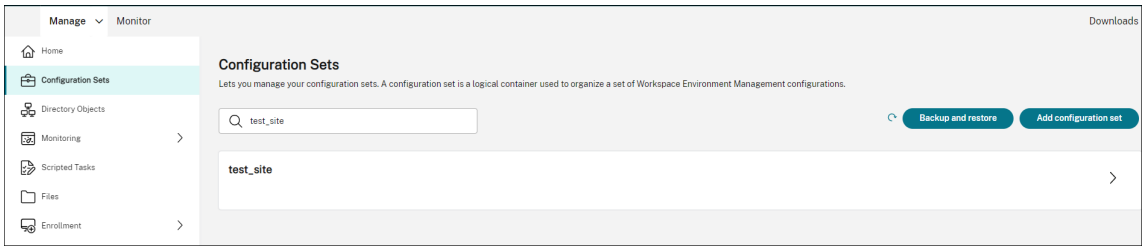


- In **Monitoring > Agents**, view the non-domain machines.

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

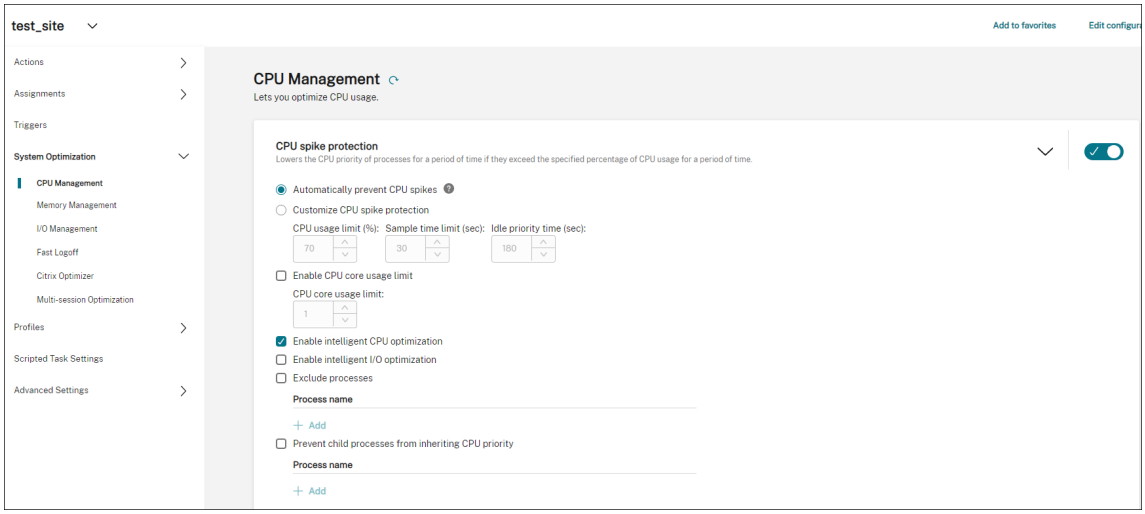


- In **Configuration Sets**, click the target configuration set.



- In **System Optimization**, adjust and apply settings as needed.

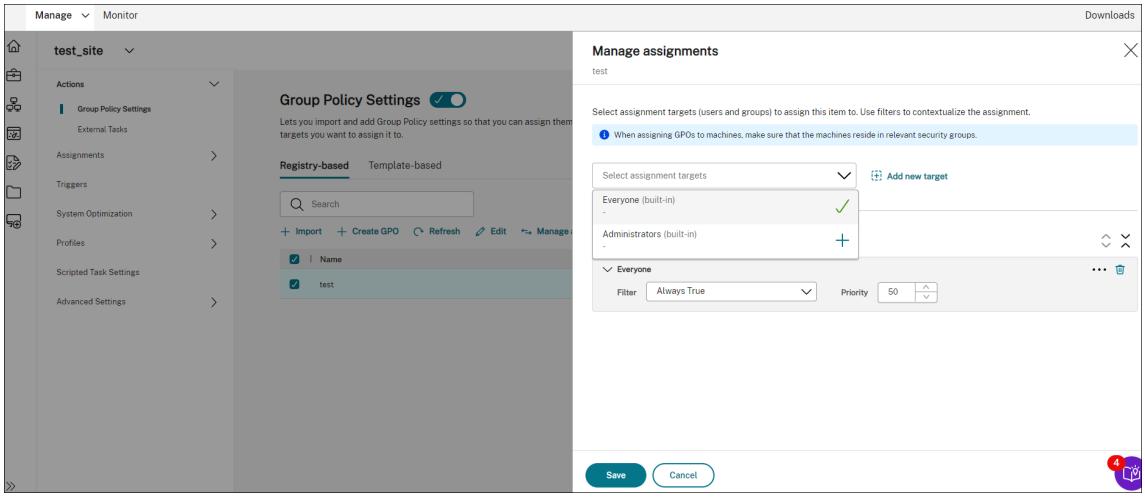
  In this example, some settings are enabled. Those settings are configured automatically because the **Apply basic settings to configuration set option** was selected in DaaS.



You can then apply settings to the non-domain-joined machines by configuring the configuration set. For example, you can apply policies to them:

- In **Actions > Group Policy Settings**, select a GPO, click **Manage assignments**, and then select **Everyone**.

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



You can go to a non-domain-joined machine to verify that the policy has taken effect. You can also assign other actions if needed. For settings to be applied to non-domain-joined machines, be sure to select **Everyone**.

More information

- Create non-domain-joined catalogs
- Manage configuration set for a catalog

Migrate FSLogix profiles to Citrix Profile Management

October 16, 2025

This article shows you how to migrate user profiles from FSLogix Profile Containers to Citrix Profile Management by using the Profile Migration Tool in Citrix Environment Tool Hub.

About the Profile Migration Tool

The **Profile Migration Tool** simplifies moving user profiles from different sources into the Citrix Profile Management format. It automates profile conversion and copying so that user settings are preserved.

The tool is included in the **Citrix Environment Tool Hub**, a set of utilities that help you configure and manage Citrix environments. For more information, see Profile Migration Tool.

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

Prepare for migration

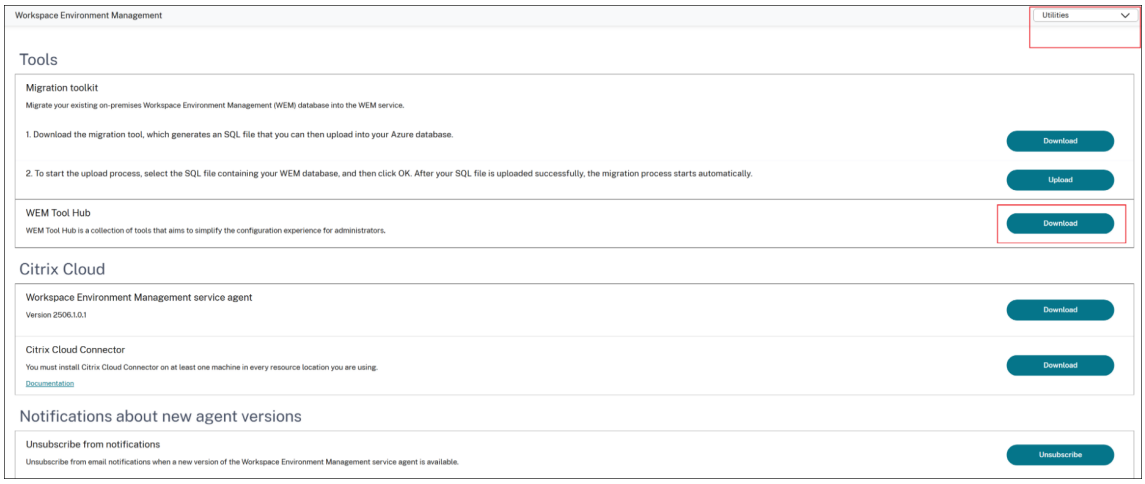
Before you start:

1. Download Citrix Environment Tool Hub to your machine
2. Prepare the Citrix Profile Management user store

Download Citrix Environment Tool Hub

Download Citrix Environment Tool Hub from the Citrix Cloud™ WEM service console.

1. Sign in to **Citrix Cloud**.
2. Open the **Workspace Environment Management™** service.
3. From the upper-right drop-down list, select **Utilities**.
4. Under **Citrix Environment Tool Hub**, select **Download**.



Prepare the Citrix Profile Management user store

Set up the destination profile store (Citrix Profile Management user store) and confirm that it's accessible. You can perform this task in one of two ways:

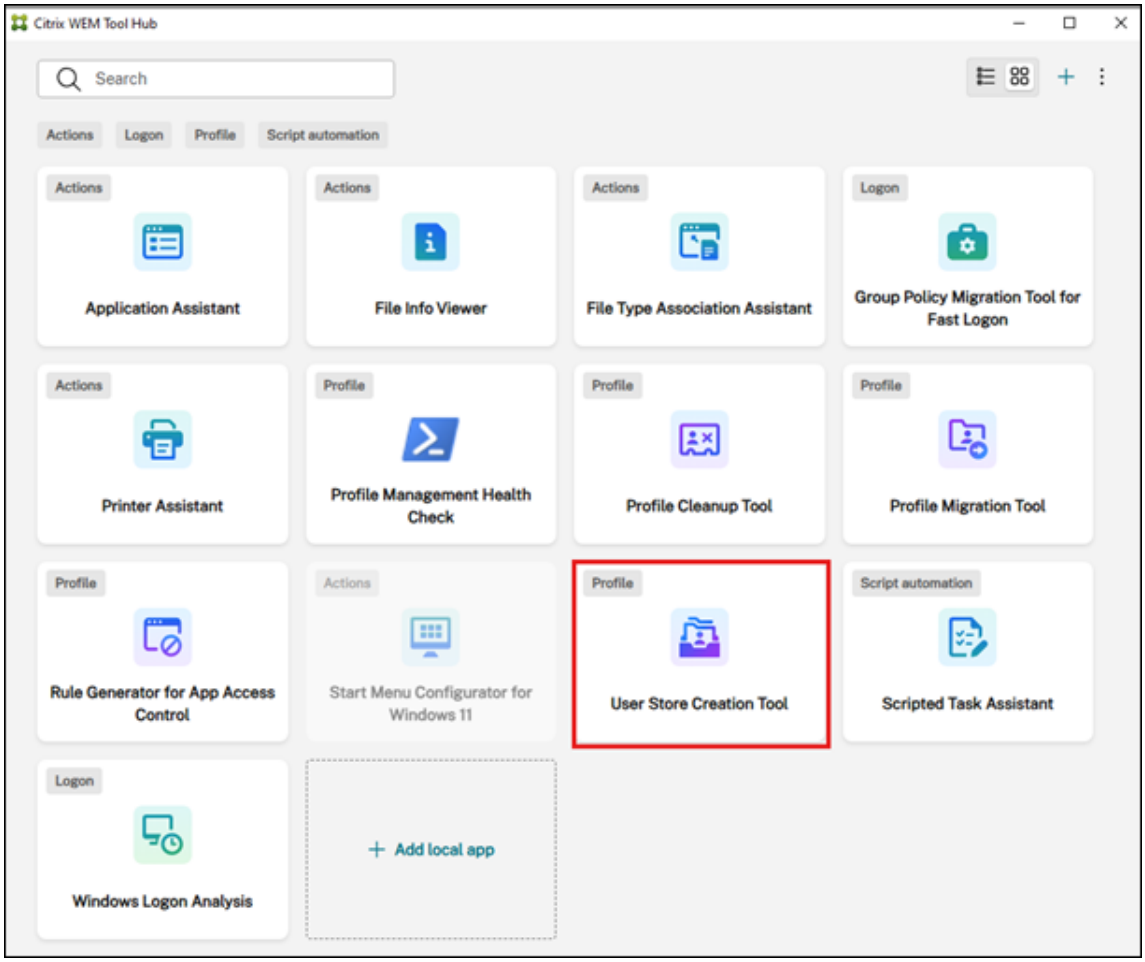
- **Create a user store manually.**

  For instructions, see Create a user store.

- **Use the User Store Creation Tool.**

  This tool, also available in Citrix Environment Tool Hub, automatically creates the folder structure and sets permissions.

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



For more information, see User Store Creation Tool.

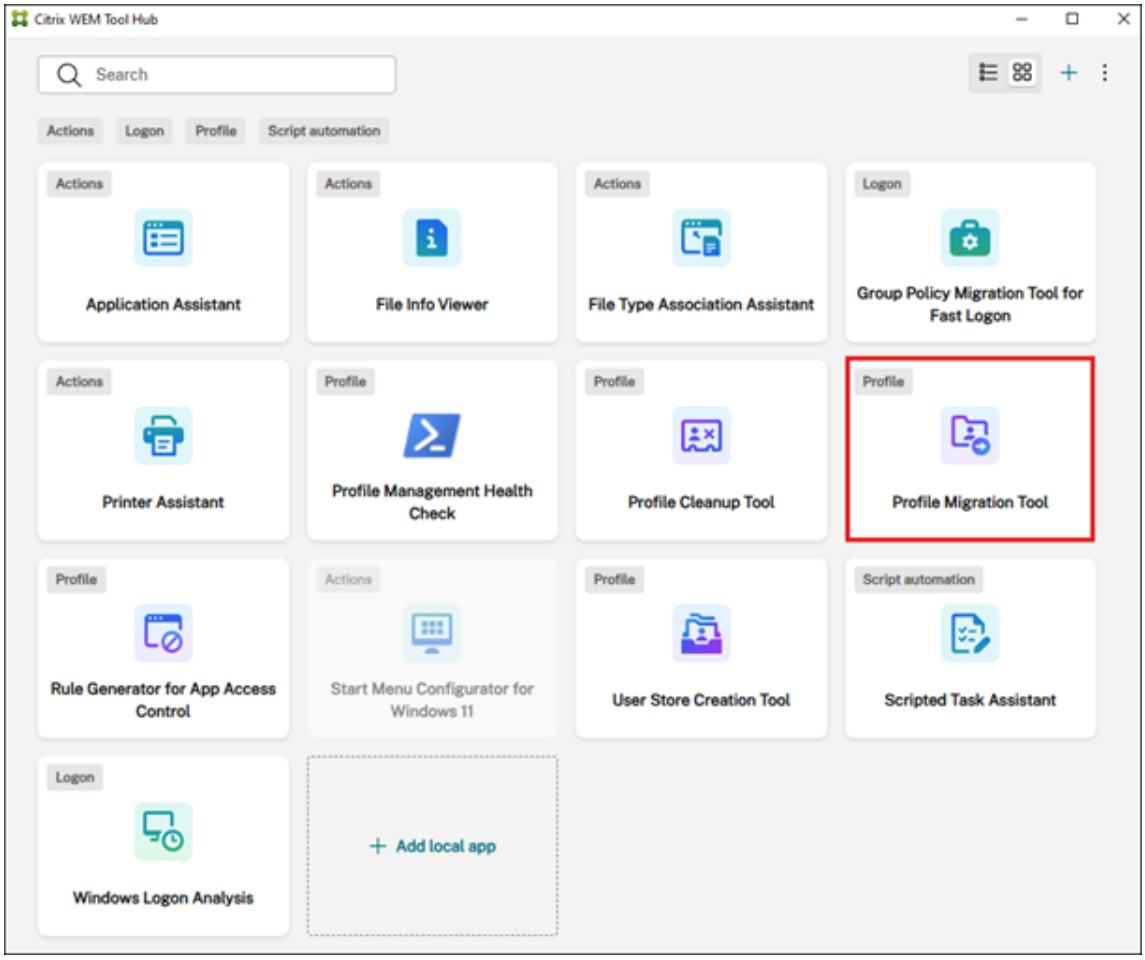
Migrate profiles

Follow these steps to migrate profiles:

1. Open the Profile Migration Tool.

   Start Citrix Environment Tool Hub and select **Profile Migration Tool**.

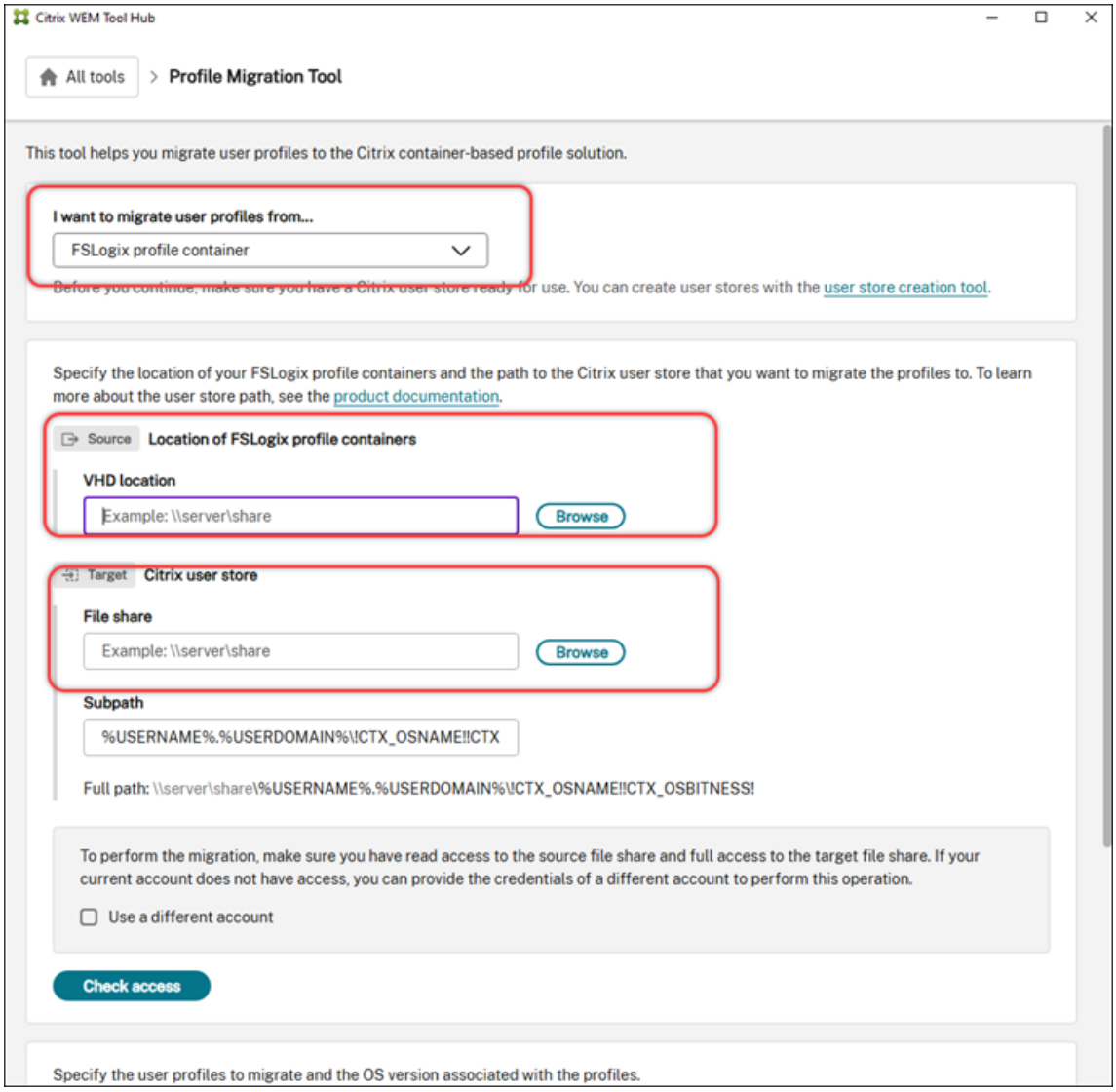
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Select the migration type.

   From the **I want to migrate user profiles from…** list, select **FSLogix profile container**.

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



3. Enter the FSLogix VHD location.

   In the **Source** section, select **Browse** and choose the UNC path of the network share that contains the FSLogix VHD or VHDX files.

4. Enter the Citrix user store location.

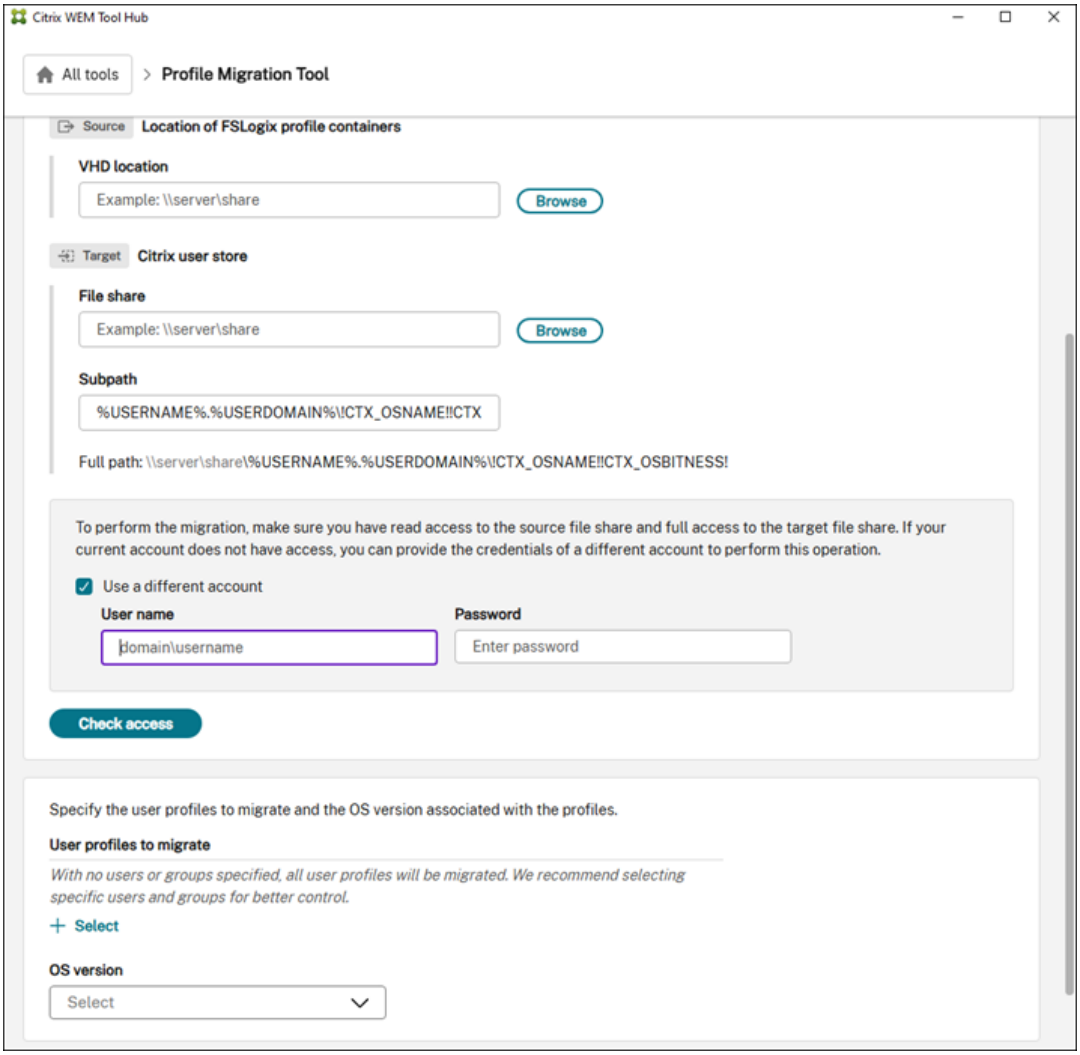
   In the **Target** section, select **Browse** and choose the UNC path for the Citrix Profile Management user store.

5. Verify access.

   a) Select **Check access** to confirm that your account has **Read** access to the source and **Full control** access to the target.

   b) If your current account lacks the necessary permissions, select **Use a different account** and enter credentials with the required permissions.

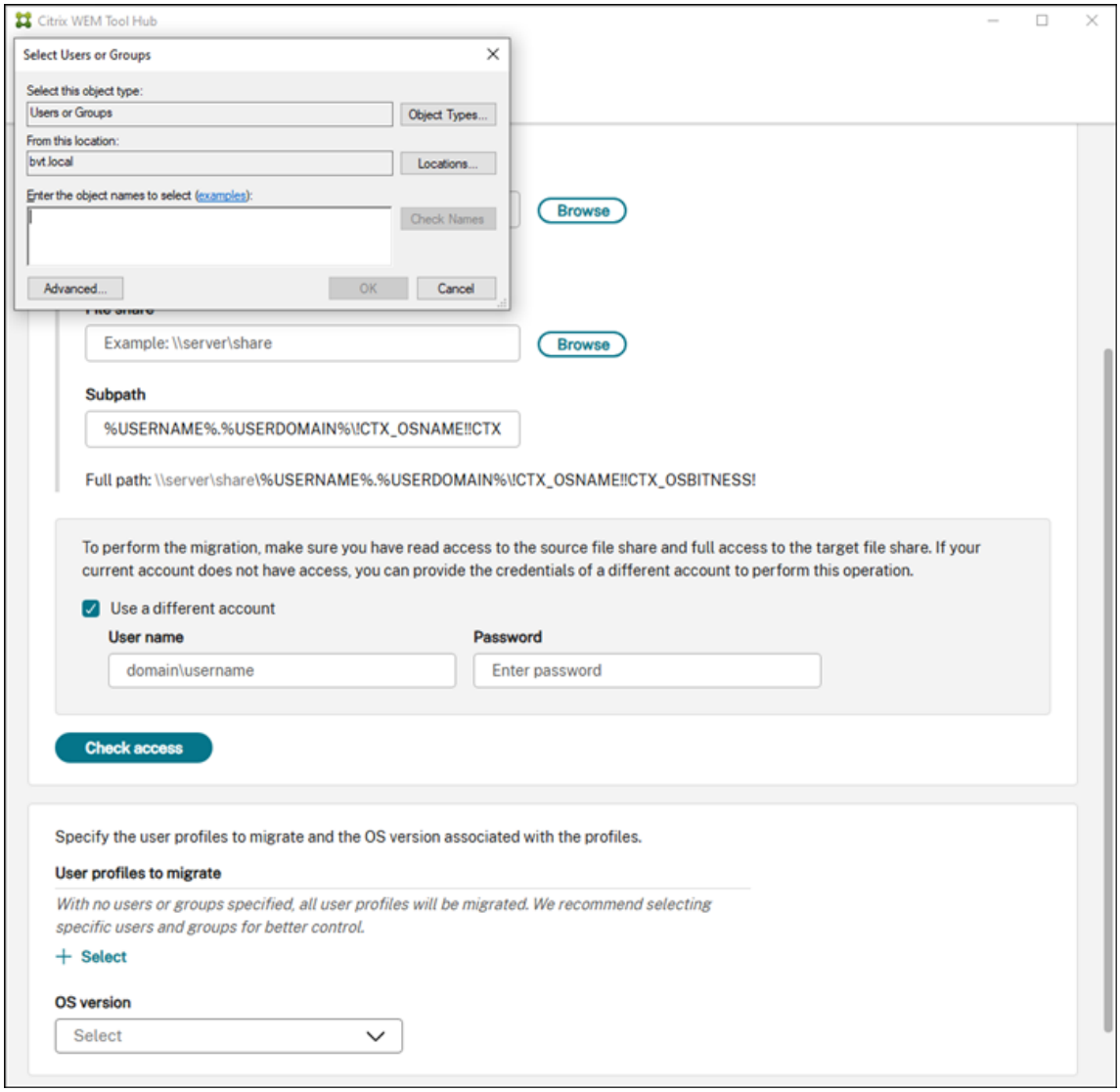
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Specify users and groups.

   In the **User profiles to migrate** section, select **+ Select** and use the Windows object picker to add users or groups.

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



7. Select the OS version.

   From the **OS version** list, select the Windows version of the source profiles (for example, Windows 10 or Windows Server 2022).

8. Start the migration.

   Click **Start migration**. Use the progress bar and logs to monitor status.

Configure after migration

After migration completes:

1. Install Citrix Profile Management on your machines. See Install and set up.
2. Set up the container-based profile solution by configuring specific Profile Management policies:

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

a) Enable Profile Management.

b) Specify the user store path.

c) Enable profile containers for the entire user profile.

For advanced container settings, see Citrix Profile Management profile container.

3. Disable FSLogix Profile Container on your machines. Otherwise, the Citrix container-based solution can't work properly. Detailed steps are as follows:

a) In **Registry Editor**, go to `HKEY_LOCAL_MACHINE\SOFTWARE\FSLogix\Profiles`.
b) Set **Enabled** to `0`.

Known issues

TEMP environment variable redirection

Issue: FSLogix redirects `TEMP` variables to a local path. This setting is saved in the profile and isn't automatically reverted during migration.

Solution: After migration, reset the `TEMP` variables to the default location (for example, `%USERPROFILE%\AppData\Local\Temp`) by using Group Policy, WEM, or a script.

Protect Citrix Workspace™ environments using process hierarchy control

September 7, 2025

In a Citrix Workspace environment, some applications might be launched not as intended. This situation can pose security risks, especially if powerful Windows tools such as CMD and PowerShell are launched.

As an administrator, you might want to restrict your users only to launching allowed applications. Workspace Environment Management™ (WEM) provides you with the process hierarchy control feature, which helps prevent end users from launching child processes.

You can control whether certain child processes can be started from their parent processes in a Citrix Workspace environment. The feature is useful in scenarios where you want to prevent unintended processes from running through published applications.

This article uses CMD as an example. With process hierarchy control, you can protect against attacks launched through CMD in a Citrix® virtual app environment by preventing CMD from being started through the published app. A general workflow for using the feature is as follows:

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

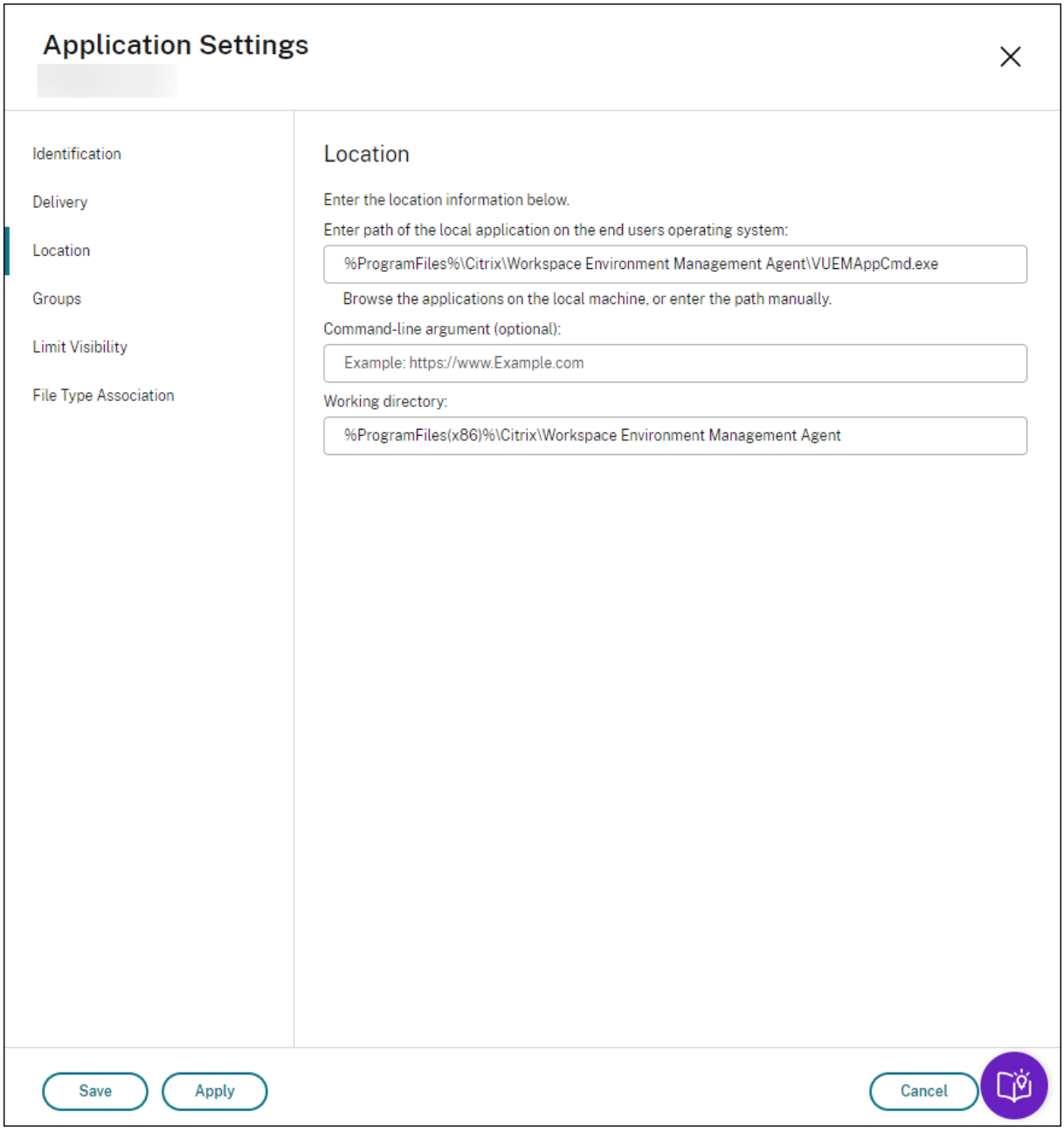
1. Enable process hierarchy control on the WEM agent
2. Configure process hierarchy control rules in the WEM console

Recommendation

We recommend that you use the WEM tool **VUEMAppCmd** to publish applications. The tool ensures that the WEM agent finishes processing process hierarchy control rules before published applications start.

Use the Full Configuration management interface to edit the application settings and then add an executable file path that points to **VUEMAppCmd.exe**. For more information, see Applications.

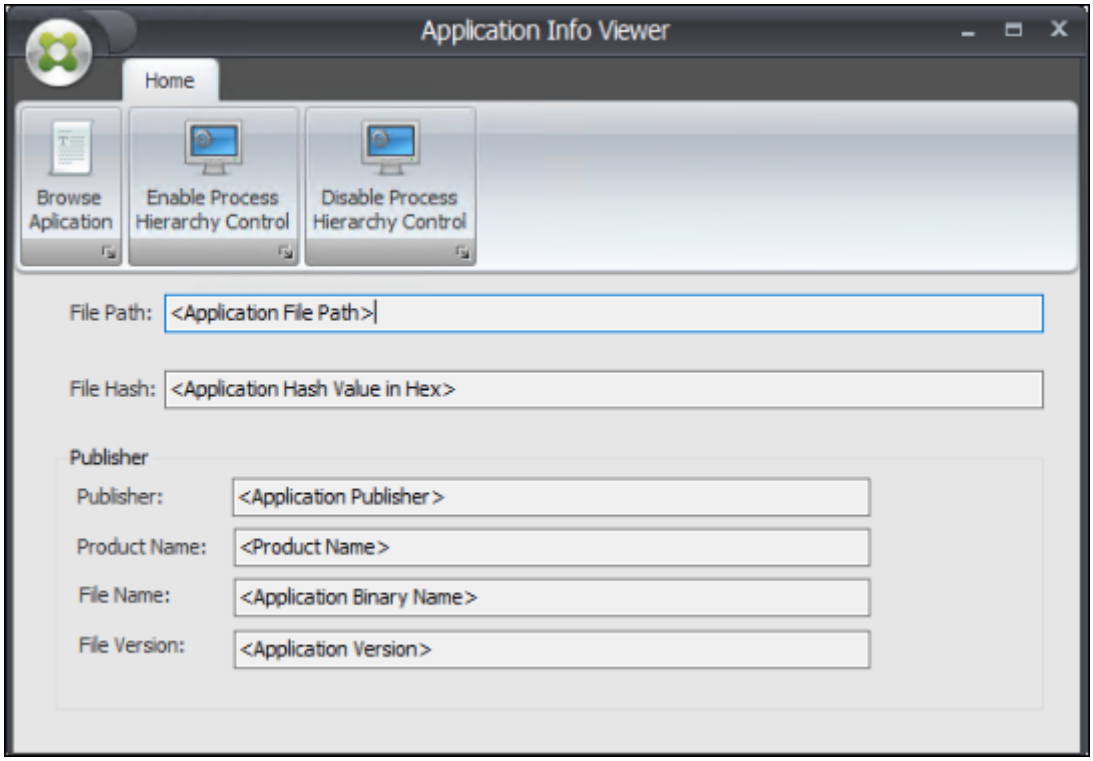
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enable process hierarchy control on the WEM agent

To enable the feature, use the **AppInfoViewer** tool on the agent machine. The tool is located in the agent installation folder. A machine restart is required after you enable or disable the feature.

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

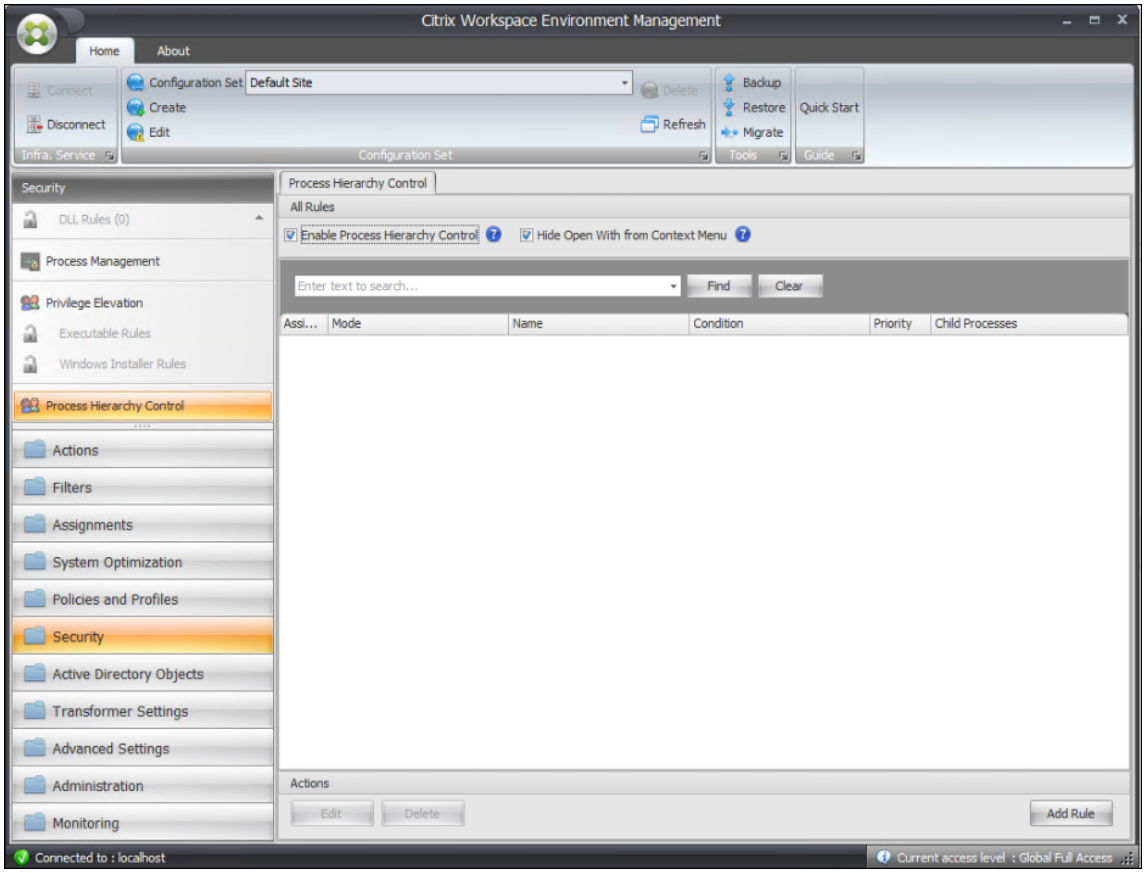


Configure process hierarchy control rules in the WEM console

Suppose you want to block CMD from launching through Notepad. To create process hierarchy control rules, complete the following steps:

1. Go to **Legacy Console > Security > Process Hierarchy Control** and select **Enable Process Hierarchy Control**.

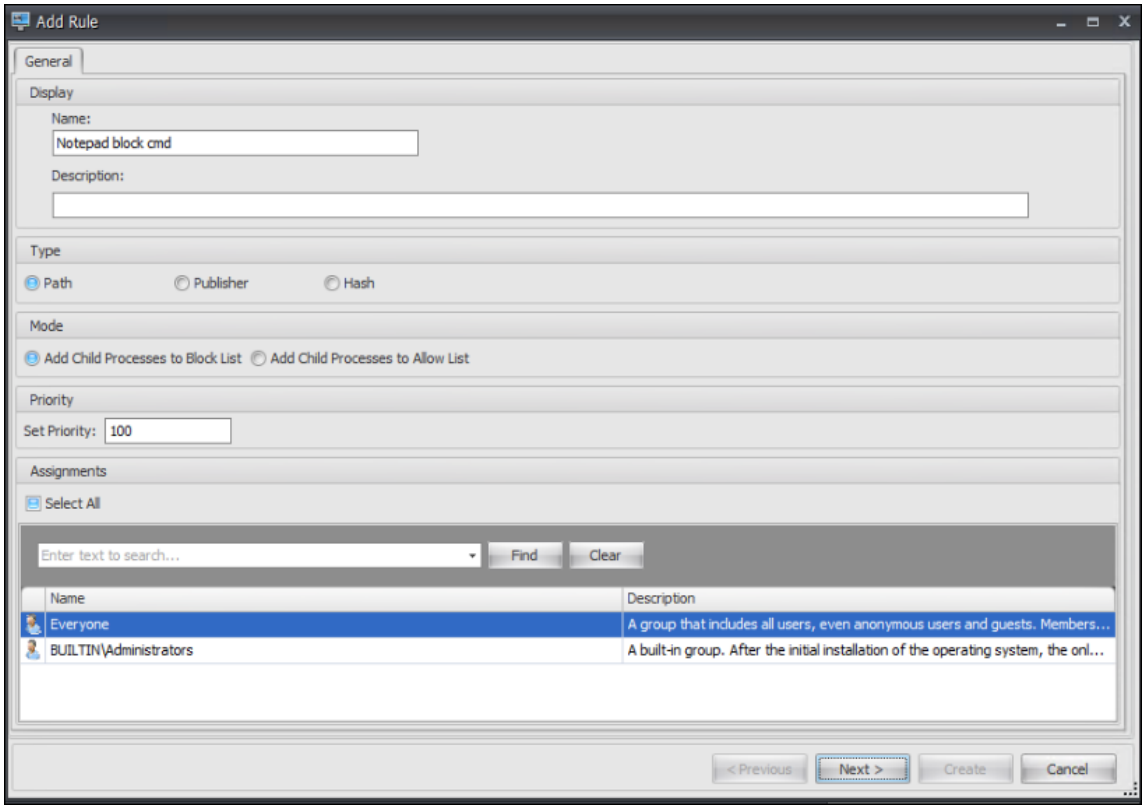
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Click **Add Rule**, configure settings as follows, and click **Next**.

> **Note:**
>
> In this example, you create a rule to prevent CMD from launching through Notepad. You can use one of the three rule types (Path, Publisher, and Hash) to specify parent and child processes. Under **Assignments**, you choose the users to which you want to apply the rule. For more information about the settings, see Process hierarchy control.

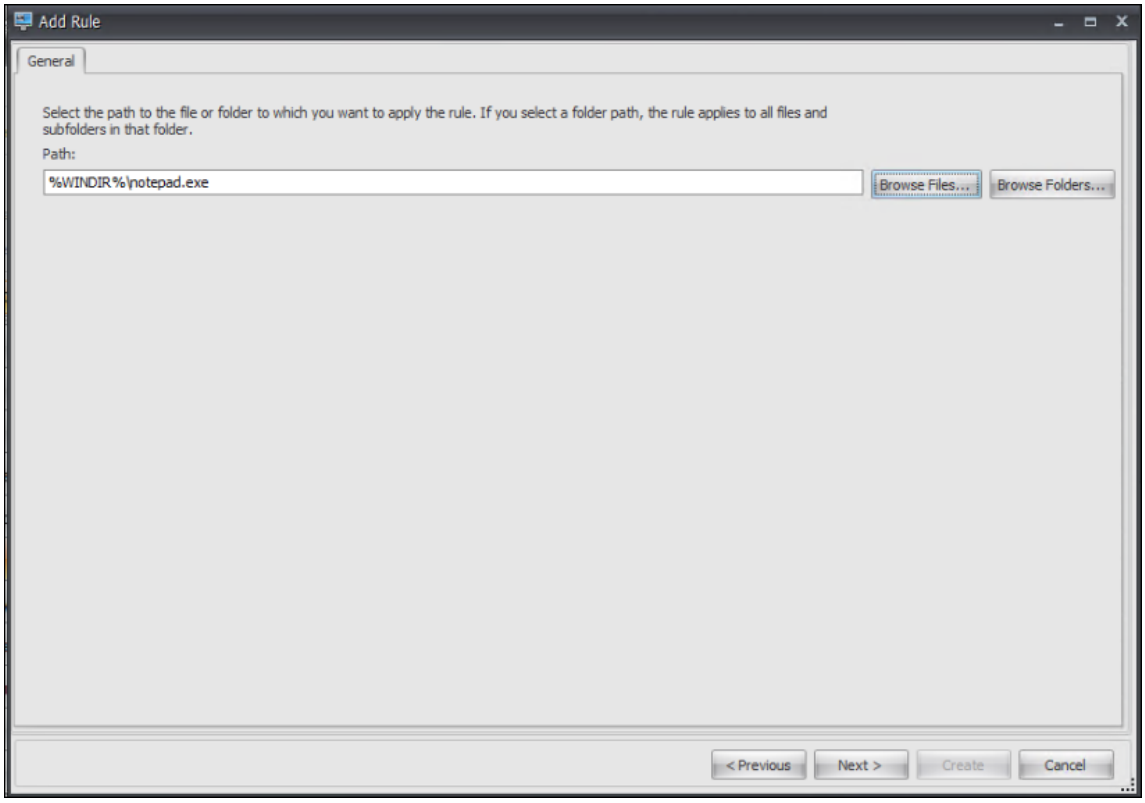
© 1997–2026 Citrix Systems, Inc. All rights reserved.



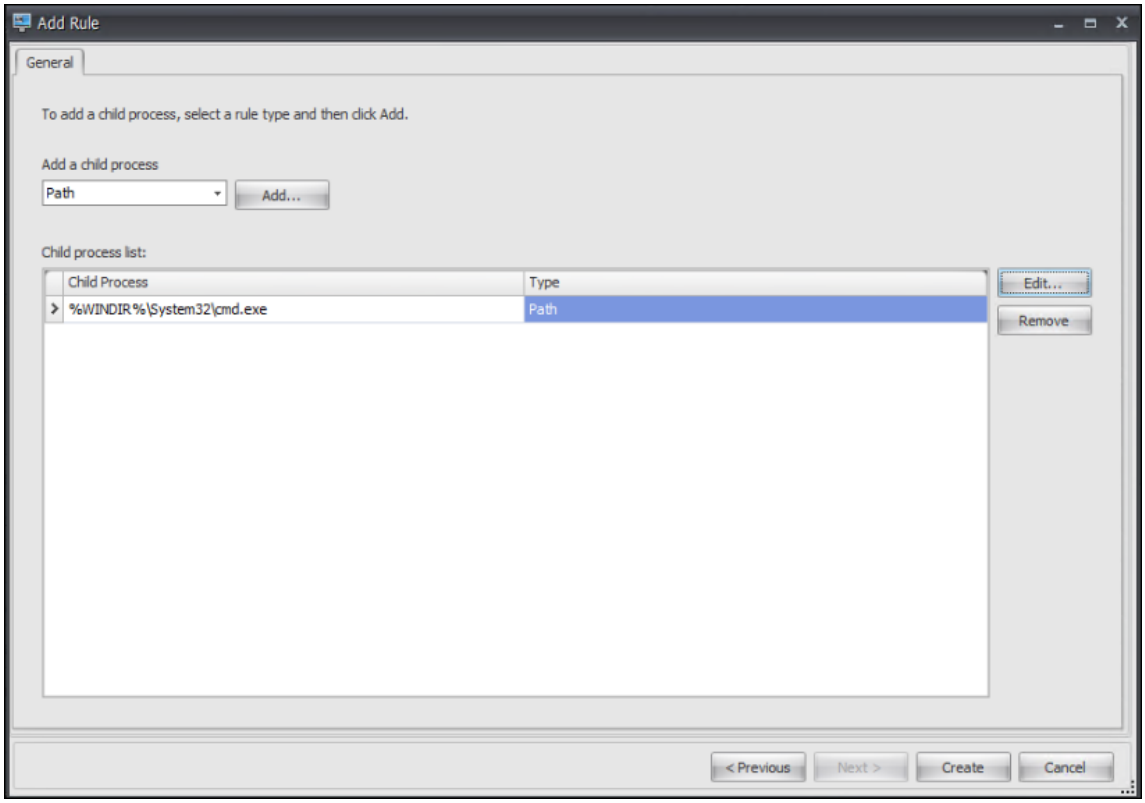
3. Configure Notepad as the parent process and click **Next.**

> **Note:**
>
> The user interface differs depending on which rule type you select in step 2.

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



4. Add multiple child processes in the rule as needed and click **Create**.



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

This completes creating the rule. The agent will prevent CMD from launching through Notepad in the Citrix Workspace environment.

Troubleshoot Login Time Issues Using Citrix Environment Tool Hub and WEM

October 16, 2025

This article serves as a guide for the Windows system administrators in troubleshooting login time issues using Citrix Environment Tool Hub. When you experience long login times, **Citrix Environment Tool Hub** provides a structured approach to efficiently diagnose and resolve the problems.

Prerequisites

The prerequisites are as follows:

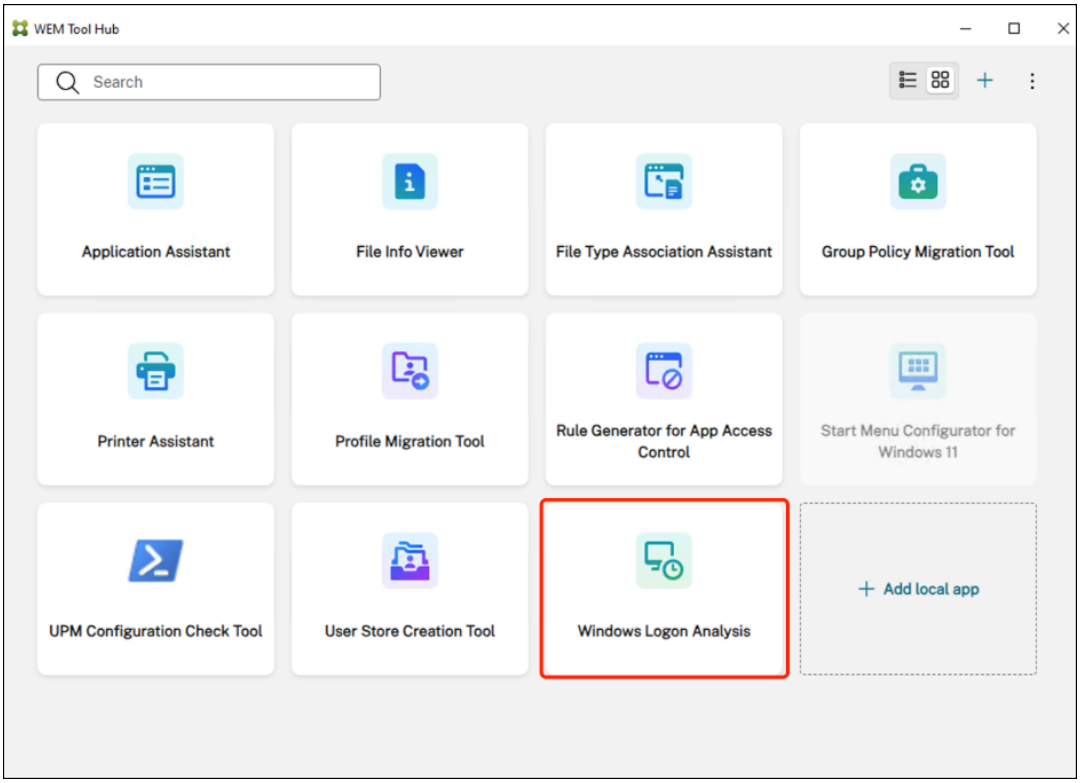
- Access to **Citrix Environment Tool Hub**
- Administrator privileges on the target Windows machine

Initial Analysis

When you experience long login times, perform your analysis using **Citrix Environment Tool Hub** by completing the following steps.

- Launch **Citrix Environment Tool Hub** with administrator privileges.
- Select **Windows Logon Analysis** on the home page.
- Select **Get Latest**, choose an appropriate time (ensure the selected time covers the login period) and click **Get Reports**.
- Wait for a while for the new report to be generated.
- Click the newly generated report to view detailed information. Use the charts or tables to identify which steps in the login process took longer durations.

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

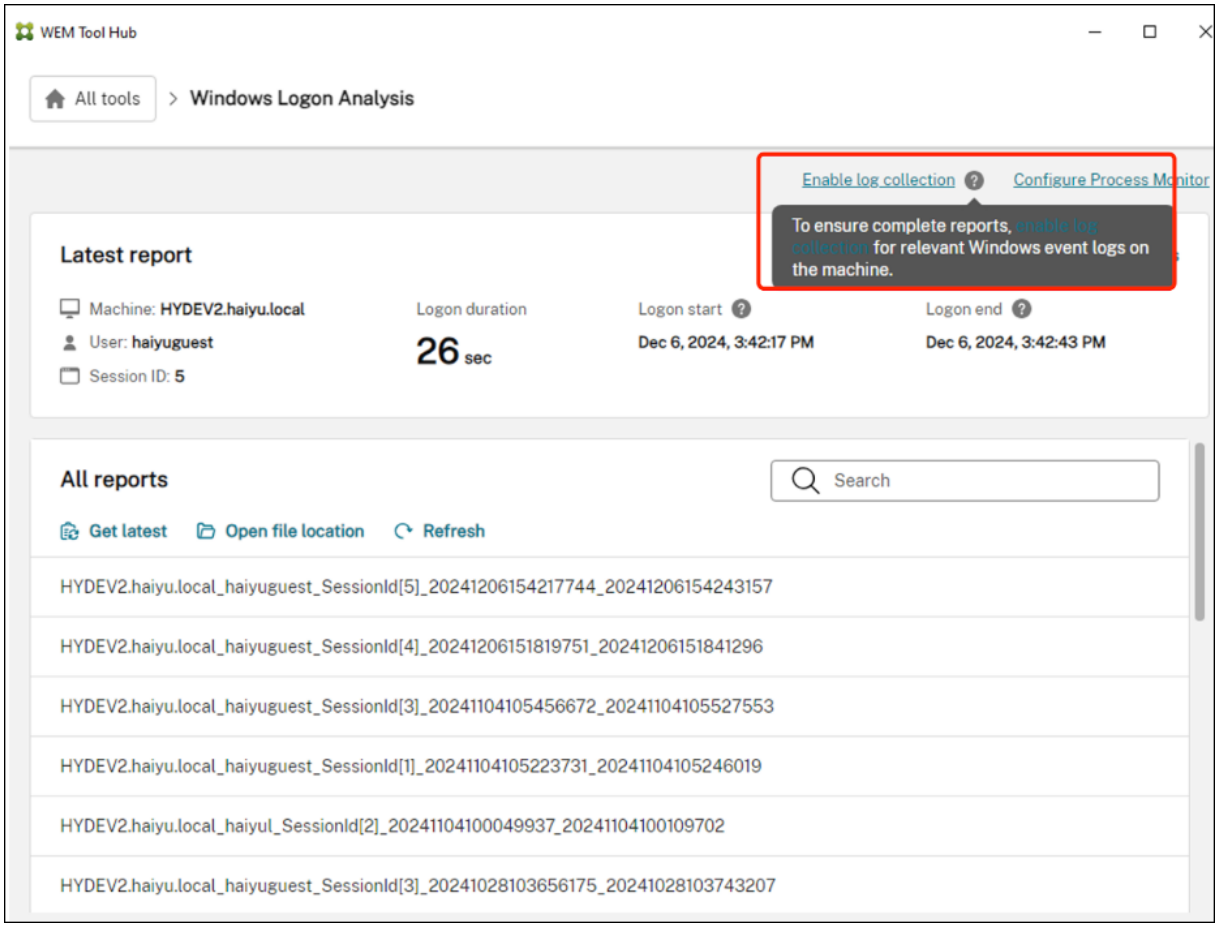
- 

Enable Log Collection

This is an optional step. If the initial analysis doesn't pinpoint the stages causing long login times, enable detailed log collection by completing the following steps.

- Select **Enable Log Collection** on the main page of the **Logon Duration Analysis** tool.
- Log off (ensure to perform a complete logoff and not disconnect) and then re-login.
- Perform the **Logon Duration Analysis** again by following the steps in the Initial Analysis section to check the new reports and logs.

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

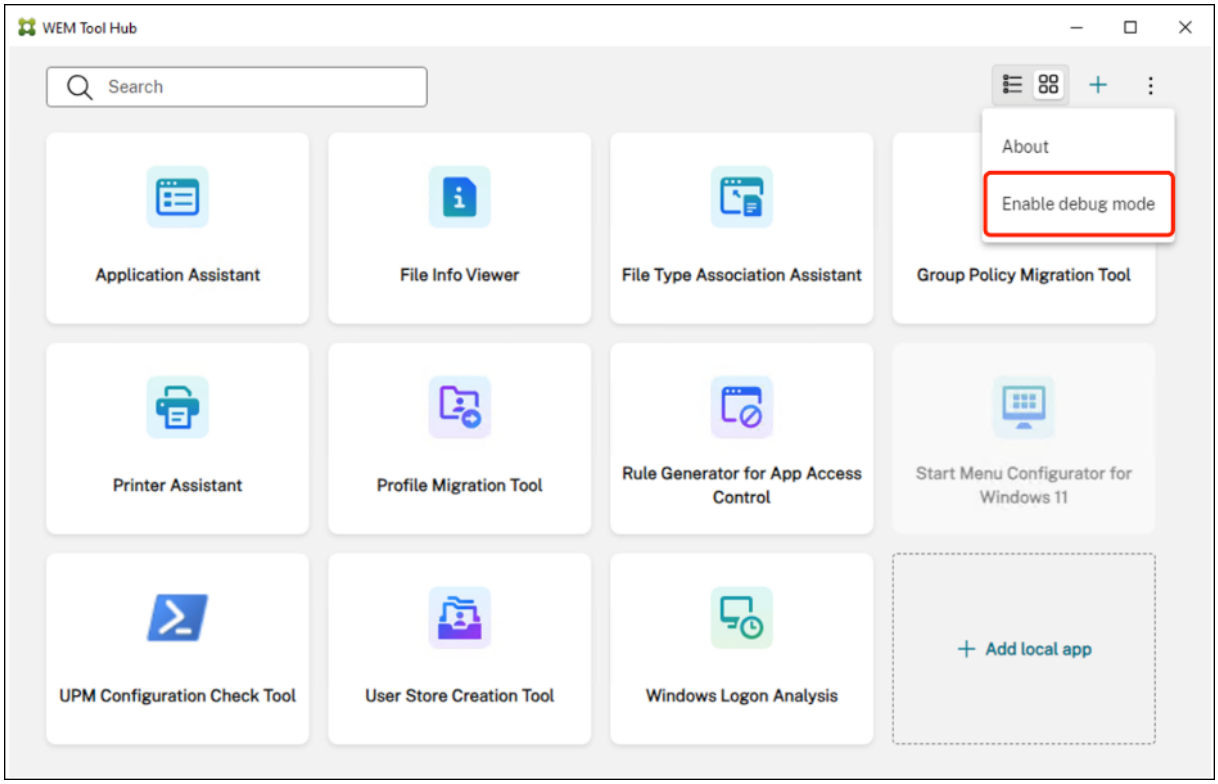


Enable Debug Mode for Analysis

If the preceding sections do not provide enough insights, select **Enable debug mode** for further analysis.

- Log off (ensure you perform a complete logoff, not disconnect) and then re-login.
- **Enable debug mode** from the three-dot menu at the top-right corner of Citrix Environment Tool Hub's main page.
- Perform the **Logon Duration Analysis** again by following the steps in the Initial Analysis section to check the new reports and logs.
- After the analysis is complete, you can select the **Open File Location** menu to see a `.CSV` file. This file contains all Windows event logs generated during the logon process. You can search these event logs to identify any events with abnormal timings.

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



Use Process Monitor Trace (Advanced Analysis)

If enabling the log collection and debug mode still doesn't trace the issue, use Process Monitor to trace the login process by completing the following steps.

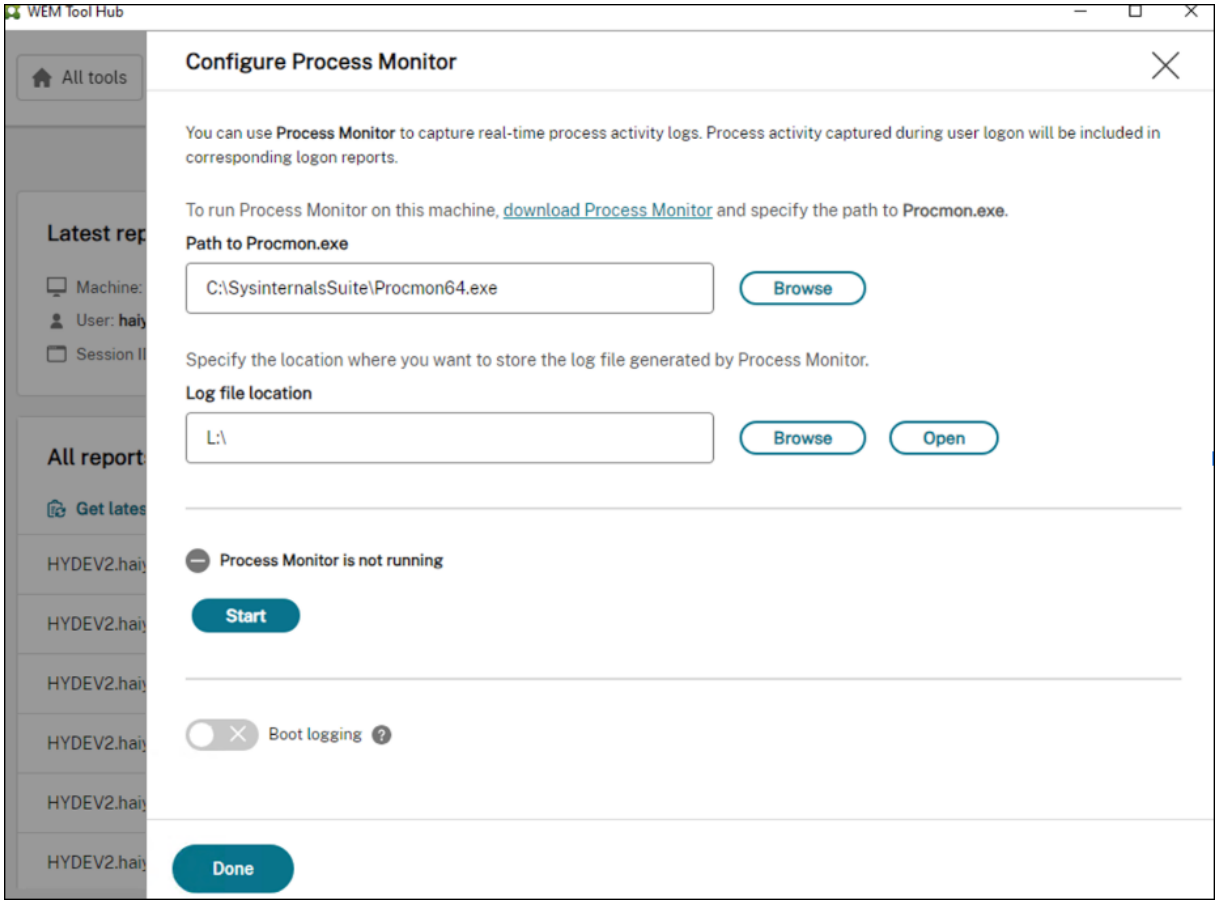
- Select **Configure Process Monitor** on the right corner of the **Logon Duration Analysis** main page to enter the Process Monitor configuration.
- If Process Monitor is not installed, download and configure its path in the **Citrix Environment Tool Hub**.
- Choose to begin the Process Monitor directly or use **Boot Logging** based on the scenario.
  - For multi-session, multi-user scenarios: Start with another user.
  - For single session or single user scenarios: Use Boot Logging, allowing **Citrix Environment Tool Hub** to automatically collect process traces during login.

    > **Note:**
    >
    > Don't leave the boot logging there for a long time after the machine startup, or it may take up much of your disk space.

- Logoff (Ensure you perform a full logoff, not disconnect) and then re-login, or reboot the machine (if using the boot logging way).

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

- Check that the Debug mode is turned on from the three-dot menu at the top-right corner of **Citrix Environment Tool Hub**'s main page.
- After trace collection is complete, repeat the steps under Initial Analysis.
- In the report's detail view, click the **Process Monitor Logs** link at the top-right corner to open the Process Monitor logs. From these logs, identify which processes are consuming significant time, CPU, memory, and so on.



Identify and Resolve Issues

Based on the data and reports collected, diagnose and resolve identified issues.

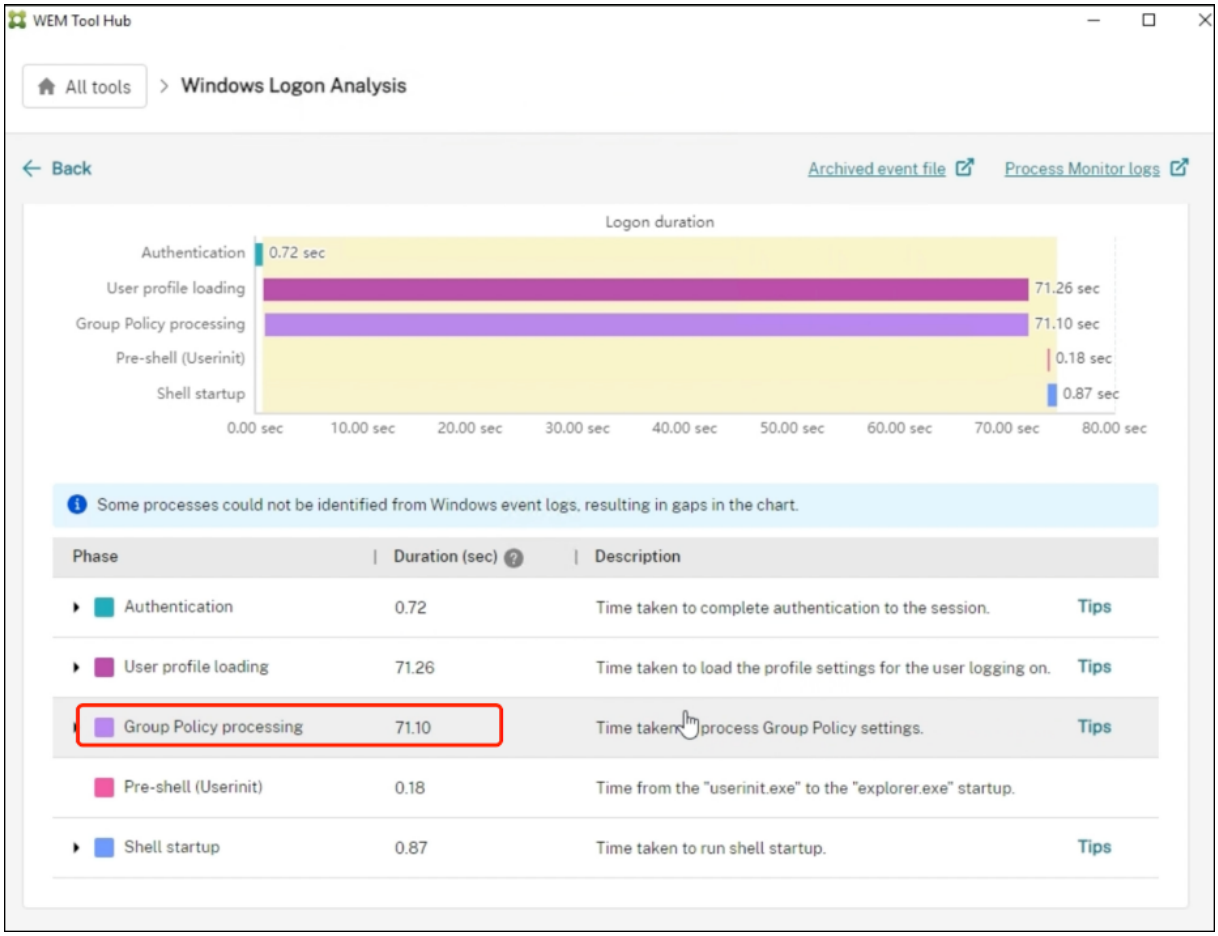
- Identify which metrics account for a higher proportion of the total login time in the report.
- Resolve issues based on tips and recommendations:
  - For example, configure and use **Citrix Profile Management** to address issues with long user profile load times.
  - Use the **Group Policy Migration Tool** in **Citrix Environment Tool Hub** to resolve issues with long group policy processing times.

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

Example Case Study: Troubleshooting Long Login Times

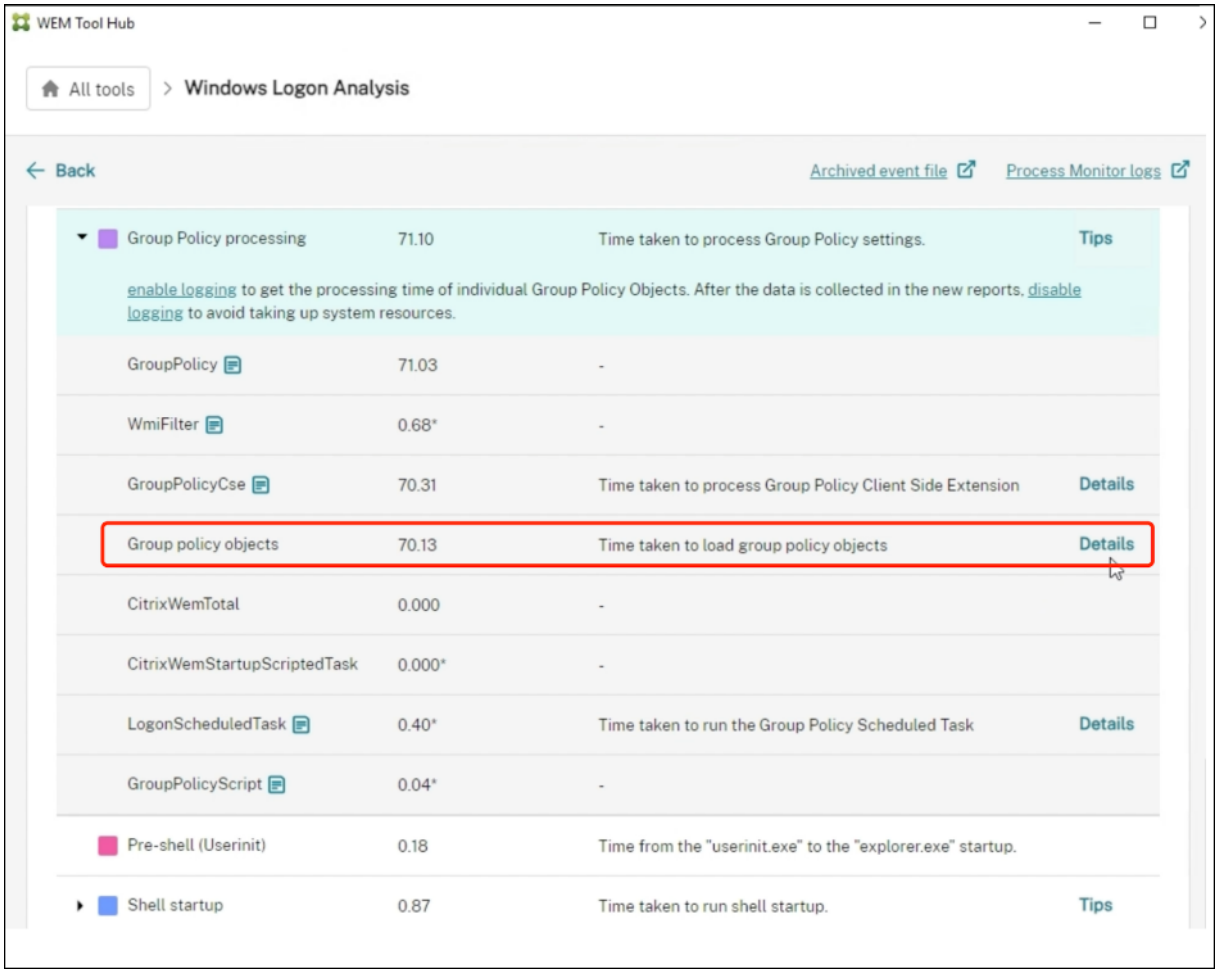
Background: Users experienced long login times on their Citrix environment, and asked the administrator for help.

Initial Analysis: Using **Citrix Environment Tool Hub**, the administrator conducted an initial analysis and noticed that the **Group Policy** processing stage took significantly longer.



Enable log collection: The administrator enabled log collection, performed a complete logoff and re-login, and then re-ran the analysis, confirming that Group Policy processing was the issue.

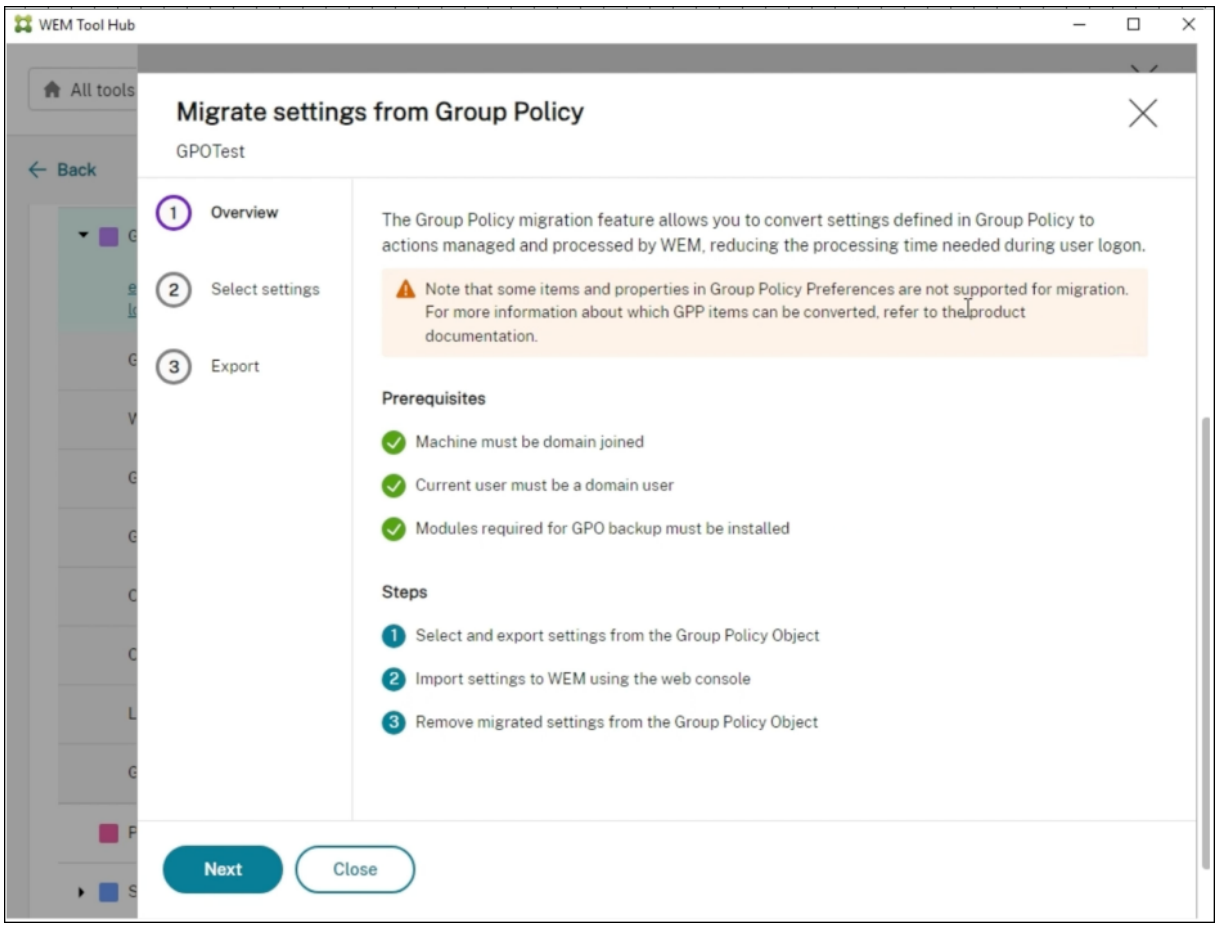
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Resolution: The administrator used the **Group Policy Migration Tool** in **Citrix Environment Tool Hub** to streamline the problematic GPO, significantly reducing its processing time.

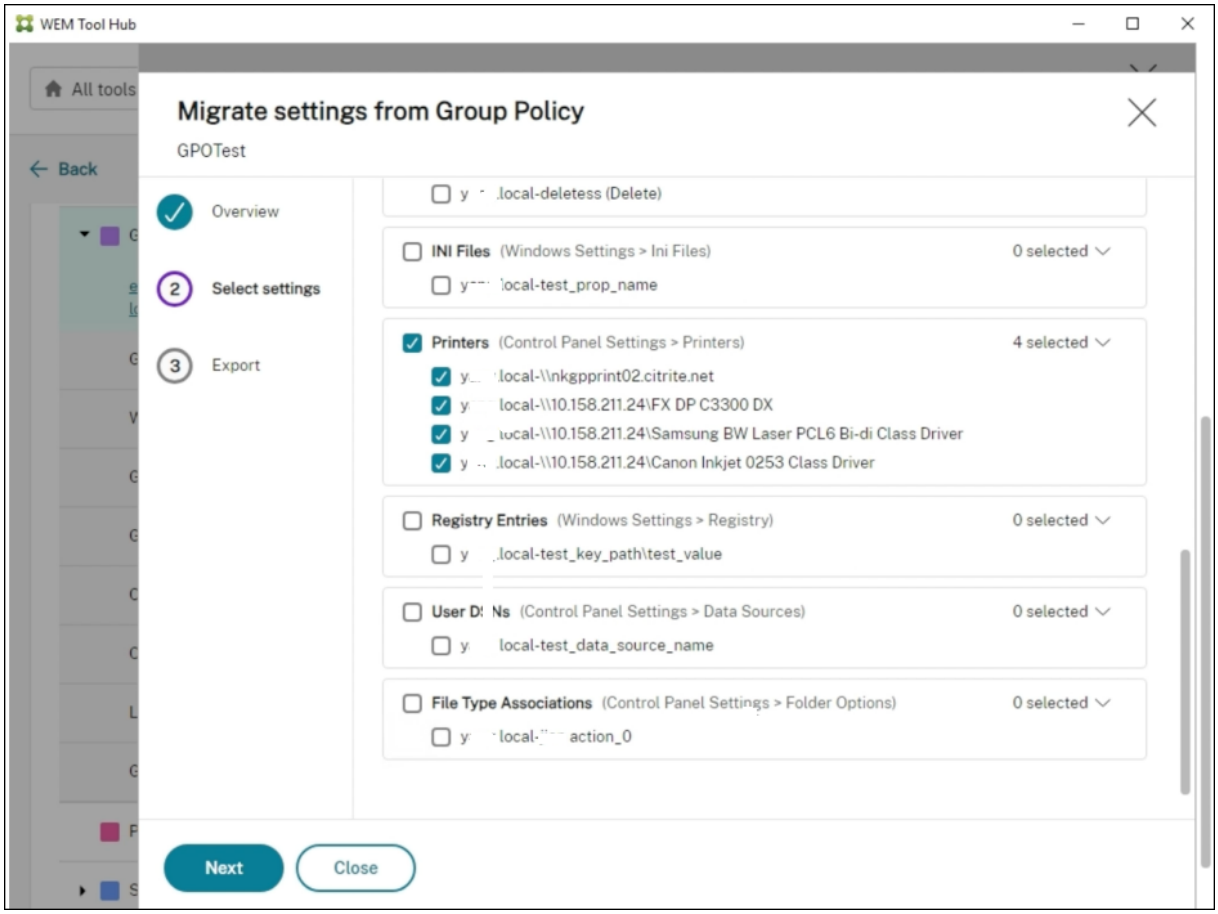
- Launch the **Group Policy Migration Tool**.

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

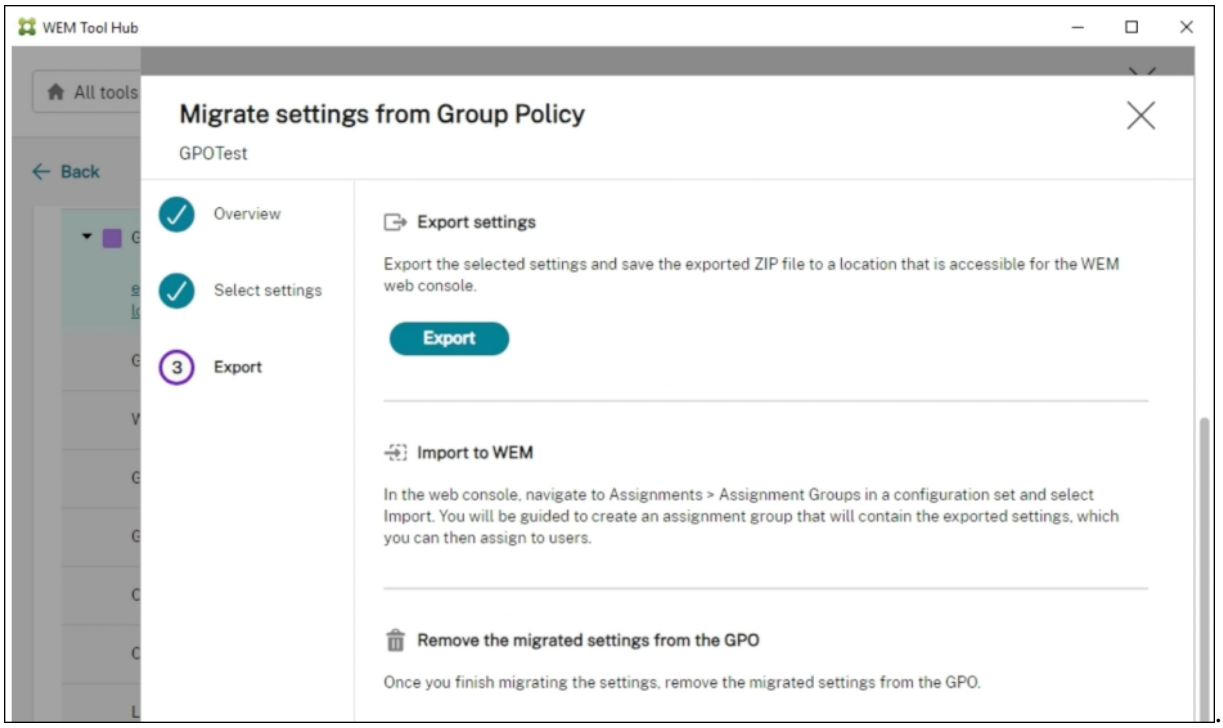


- Select Group Policy objects.

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

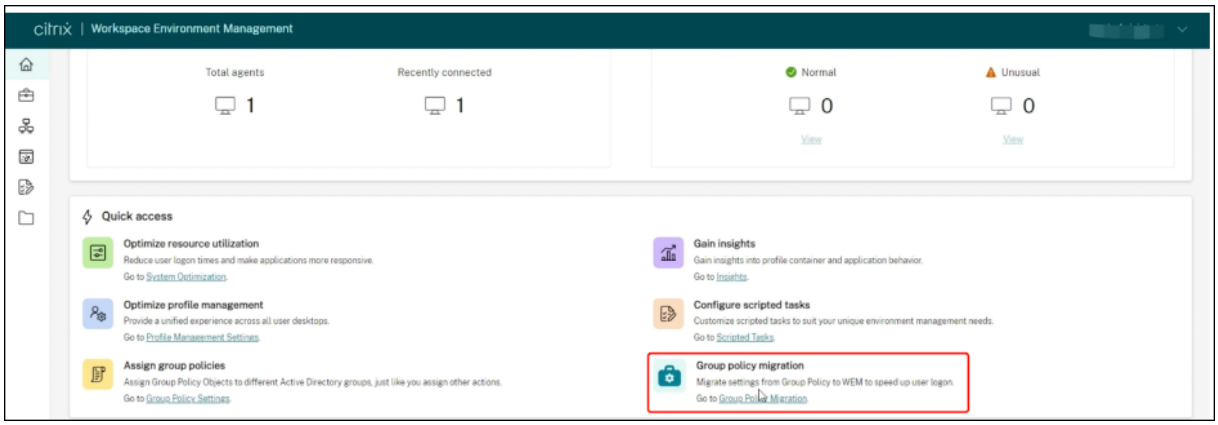


- Export the group policy to file.

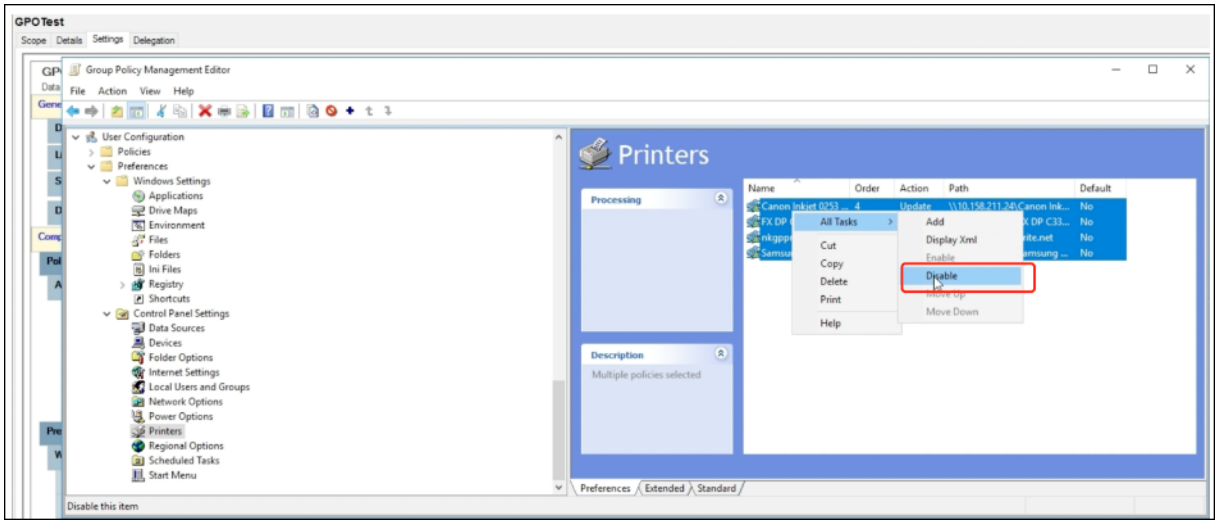


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Migrate the Group Policy to WEM.

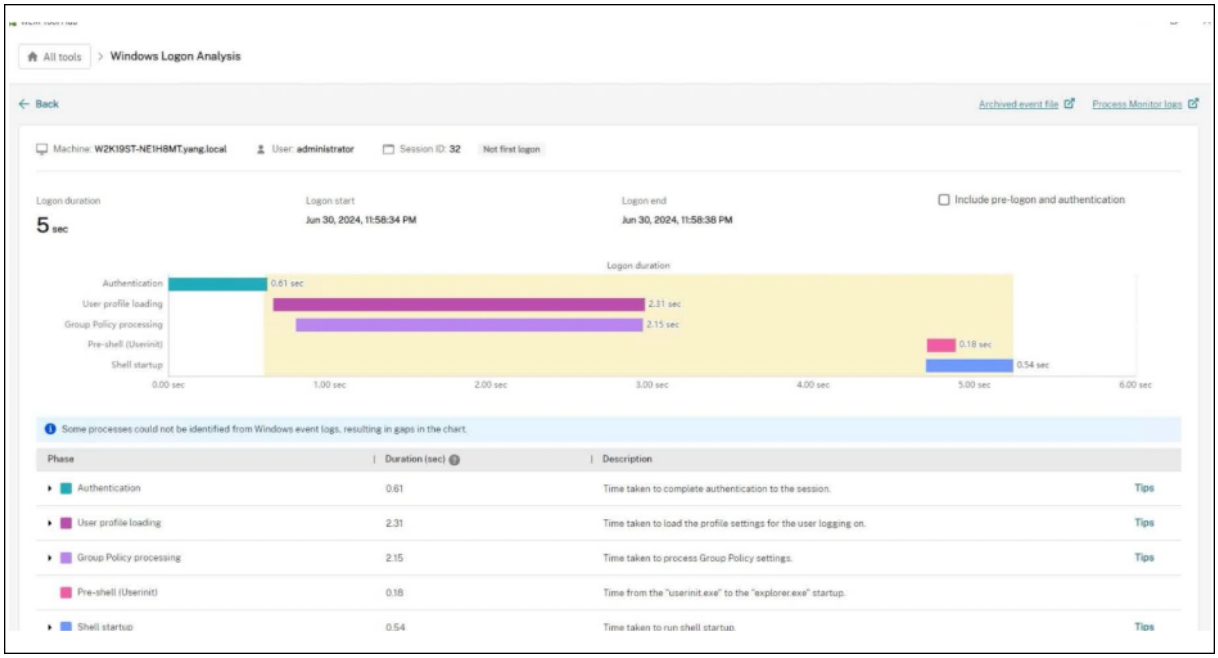


- Disable the Group Policy from the Active Directory side.



Outcome: After following these steps, the administrator saw a marked improvement in login times, and user satisfaction increased.

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



Further Analysis: If the preceding steps do not reveal the cause of long login times, collect all files generated during the analysis process in **Citrix Environment Tool Hub** and contact support for further analysis.

Conclusion: By following these steps, system administrators can systematically troubleshoot login time issues using **Citrix Environment Tool Hub**. This structured approach helps diagnose current problems and prepares for future login performance improvements.

Troubleshoot scripted task execution problems in Monitor

May 21, 2026

DaaS Monitor enables you to run scripted tasks from **Filters > Machines > Machine actions > Run scripted task**. However, you might encounter errors when attempting to run a scripted task, such as:

- `WEM Agent is not found`
- `WEM Agent is not recently connected`
- `WEM Agent version is not supported`

This article describes the common causes of these errors and how to resolve them.

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

WEM Agent not installed

Cause: The **Run scripted task** feature requires the WEM Agent to be installed. In Citrix Virtual Apps and Desktops 2507 LTSR and later, the WEM Agent is installed automatically on VDAs. In earlier versions, the agent must be installed manually.

Resolution: Verify that the WEM Agent is installed on the target machine. The default installation path is:

```
C:\Program Files (x86)\Citrix\Workspace Environment Management Agent
```

WEM Agent running in Basic Deployment mode

Cause: When the WEM Agent runs in the **Basic deployment** mode, it operates offline and does not connect to the network.

Scripted tasks require the agent to run in the **Cloud service deployment** mode and connect to the WEM service using AD-joined (or called *Cloud Connector* method) or Non-domain-joined method.

Resolution:

1. Use the **WEM Health Check Tool** to verify the agent mode. The tool is located at: `C:\Program Files (x86)\Citrix\Workspace Environment Management Agent\Health Check Tool`
2. To switch the agent to AD-joined method in the **Cloud service deployment** mode, complete one of the following actions:
   - Use the **Health Check Tool** to specify the Cloud Connector IP address or FQDN.
   - Use Group Policy to distribute Cloud Connector settings across multiple VDAs. For more information, see Configure group policies.

WEM Agent not registered to WEM service

Cause: The WEM Agent must be registered to a configuration set in the WEM service. Scripted tasks cannot run if the registration is incomplete.

Resolution:

Check the agent's registration status:

1. In the **WEM web console**, go to **Monitoring > Agents > Registrations**.
2. Verify whether the agent appears as **Registered** or **Unregistered**.

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

3. If the agent is unregistered or registration issues persist, review the following configuration set scenarios to further troubleshoot the issue:

    - Agent not bound to any configuration set
    - Agent bound to multiple configuration sets

Agent not bound to any configuration set

Cause: No configuration set is assigned to the agent.

Resolution: Assign a configuration set using one of the following methods:

- Configuring WEM options when creating or editing a machine catalog in Web Studio
- Creating Directory Objects (OU, group, or individual machine) in the WEM web console.

Agent bound to multiple configuration sets

Cause: Conflicting assignments exist. For example:

- A machine catalog is bound to **Configuration Set A**, and
- The Domain Computers group is bound to **Configuration Set B**.

Resolution: In the **WEM web console**, go to **Directory Objects**, review the bindings, and remove conflicting configuration set assignments.

WEM Agents not connected to the WEM service

Cause: The agent cannot connect to the WEM service due to network issues or firewall restrictions.

Resolution: Verify the network environment and ensure that all required connections to the WEM service are allowed.

WEM Agent version limitation for scripted tasks

Cause: WEM Agent versions earlier than **2207.1.0.1** do not support running scripted tasks.

Resolution: Upgrade the WEM Agent to a supported version.

WEM service upgrade in progress

Cause: The WEM service is temporarily unavailable during a WEM infrastructure service upgrade.

Resolution: Wait until the upgrade completes, and then retry the operation.

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

WEM database archived

Cause: The WEM database can be archived if no operations occur and no active agents connect for 30 consecutive days.

Resolution: Unarchive the database by manually opening the WEM web console. This action automatically triggers the unarchive process.

WEM service is not ready

Cause: The WEM service is not yet provisioned.

Resolution: Ensure WEM provisioning is completed and all required services are running, then retry the operation.

Troubleshoot unregistered VDAs using scripted tasks in Monitor

July 8, 2026

When a Virtual Delivery Agent (VDA) is unregistered, published apps and desktops on it are unavailable to users. As administrators, you often need to connect to the machine, review logs, check services, and retry the launch. You can now run scripted tasks directly in Monitor to diagnose unregistered VDAs and restart an affected Windows service without opening a separate remote session to the VDA.

Use this article when you need to investigate a single unregistered VDA on demand. For recurring issues across multiple VDAs, consider using Windows event triggers to run health checks automatically. For more information, see Use Windows events as triggers to detect VDA registration issues.

Prerequisites

Before you start, make sure that:

- WEM is enabled for the site.
- The target VDA is bound to a WEM configuration set.
- The WEM Agent is installed and running on the target VDA.
- You have permission to run WEM scripted tasks on the target machine.

If the scripted task cannot start, see Troubleshoot scripted task execution problems in Monitor.

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

Symptoms

Use this procedure when one or more of the following symptoms occur:

- A user reports that a published app or desktop fails to launch.
- Monitor shows an **Unregistered** status in the **Failure Type** field for the affected VDA.

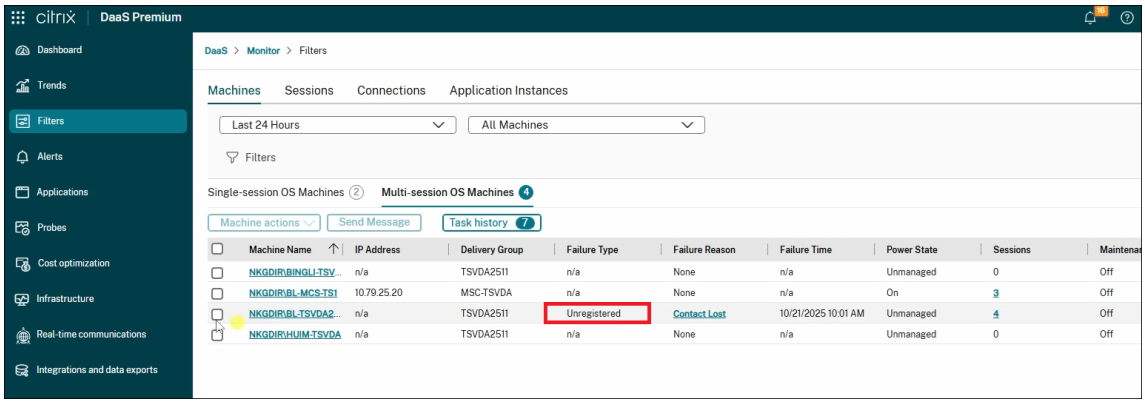
Workflow

Use the following workflow to diagnose and remediate the issue:

1. Locate the unregistered VDA in Monitor.
2. Run the **Diagnose VDA Unregistration** scripted task on the target VDA.
3. Review the scripted task result and identify the failed check.
4. If the result points to a stopped or unhealthy service, run the **Restart Windows Service** scripted task for that service.
5. Verify that the VDA registers and that the user can launch the app or desktop.

Step 1: Locate the unregistered VDA

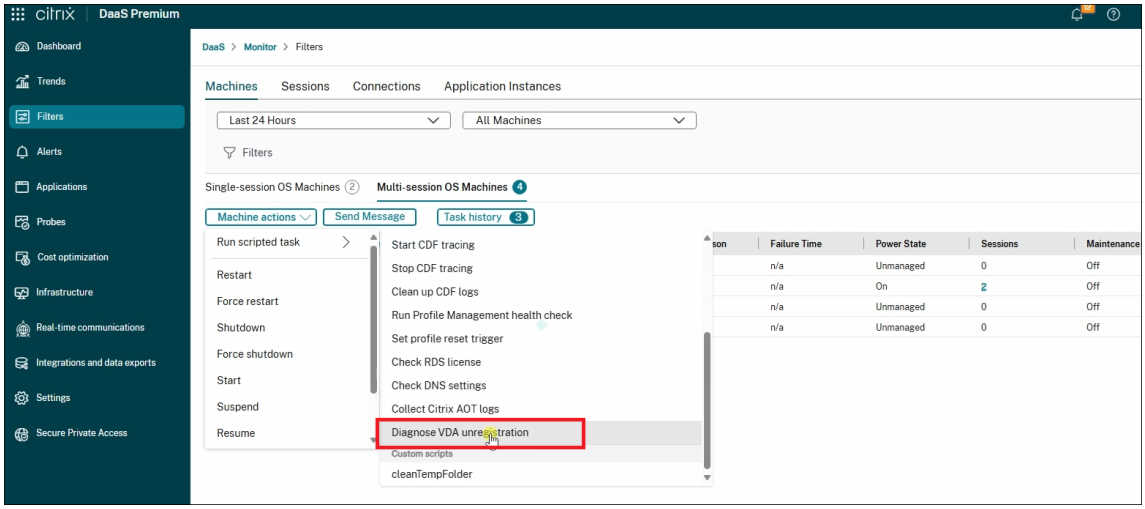
1. From **Monitor**, select **Filters** in the left pane.
2. Find the affected machine from the **Machines** view or search results.
3. Verify that the machine registration state is **Unregistered**.



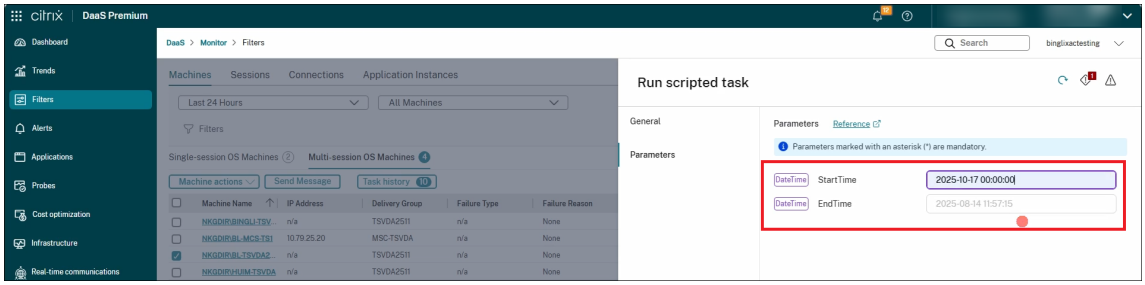
Step 2: Run the Diagnose VDA Unregistration scripted task

1. Select the affected machine.
2. Select **Machine actions > Run scripted task > Diagnose VDA Unregistration**.

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



3. Enter the time range for collecting Always On Tracing (AOT) failure logs.



4. Click **Run** to submit the task.

The task runs diagnostic checks on the target VDA and generates a result that summarizes passed, warning, and failed checks.

Checks included in the diagnosis

The **Diagnose VDA Unregistration** scripted task can check the following areas:

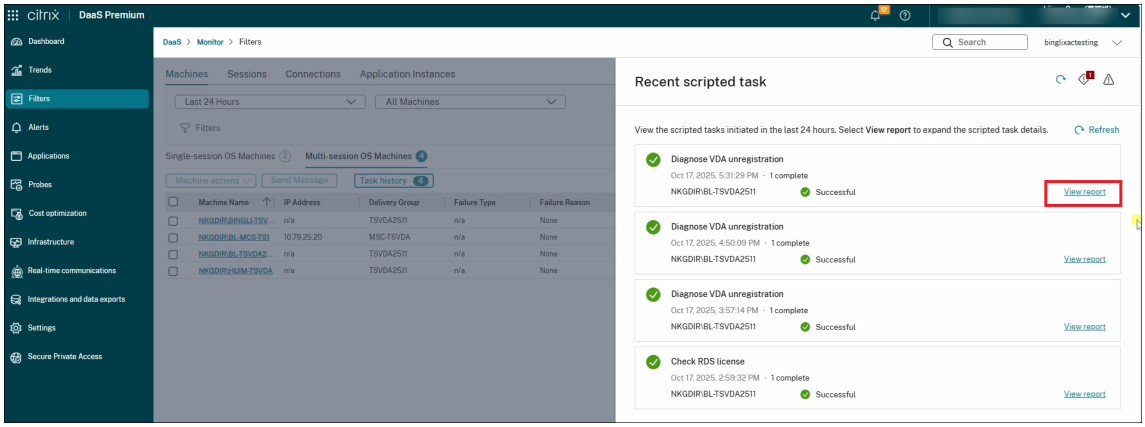
- **CHC (Citrix Health Check) check**. Validates common VDA registration prerequisites, including firewall rules, registry settings, Delivery Controller or Cloud Connector configuration, domain trust, certificates, TLS configuration, and time synchronization.
- **RDS check**. For multi-session VDAs, verifies that Remote Desktop Services is installed and running and that Remote Desktop Services licensing is configured correctly.
- **DNS check**. Verifies that the VDA can resolve configured Delivery Controllers or Cloud Connectors.
- **Delivery Controller / Cloud Connector connectivity check**. Tests whether the VDA can reach the Delivery Controllers or Cloud Connectors on the required broker ports, such as 80 or 443.
- **AOT failure log check**. Collects and filters Citrix AOT logs so that recent registration failure details are easier to review.

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

- **Event log scan**. Scans recent Windows Application and System event logs for known registration-related events, and lists the matches.

Step 3: Review the diagnosis result

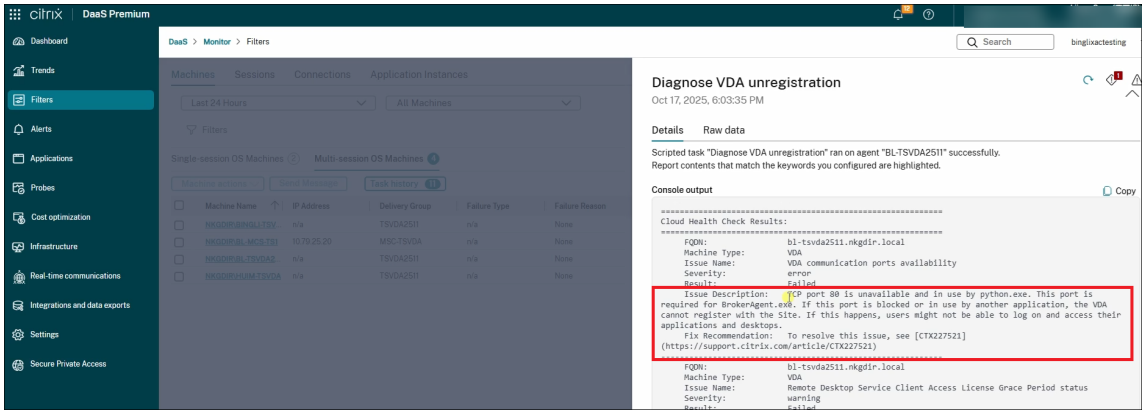
1. After the scripted task finishes, open the task result or output.



2. Review the summary in the **Summary** section and identify failed checks.
3. Use the details in the result to decide the next action.

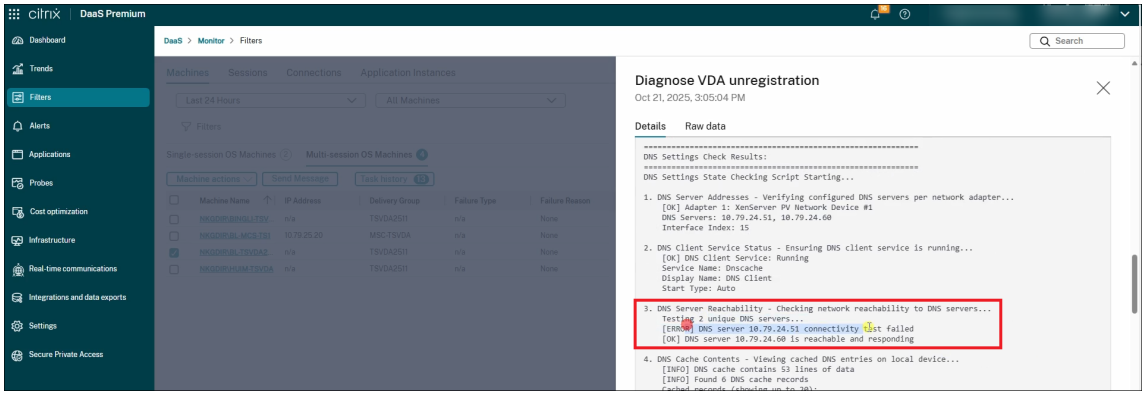
Common findings include:

- **TCP port errors**. The VDA cannot reach DaaS or Cloud Connector on the required port.

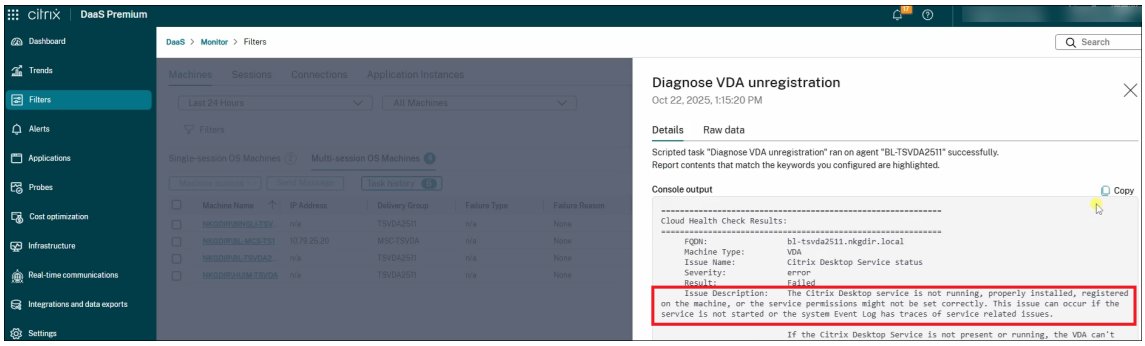


- **DNS errors**. The VDA cannot reach DNS servers.

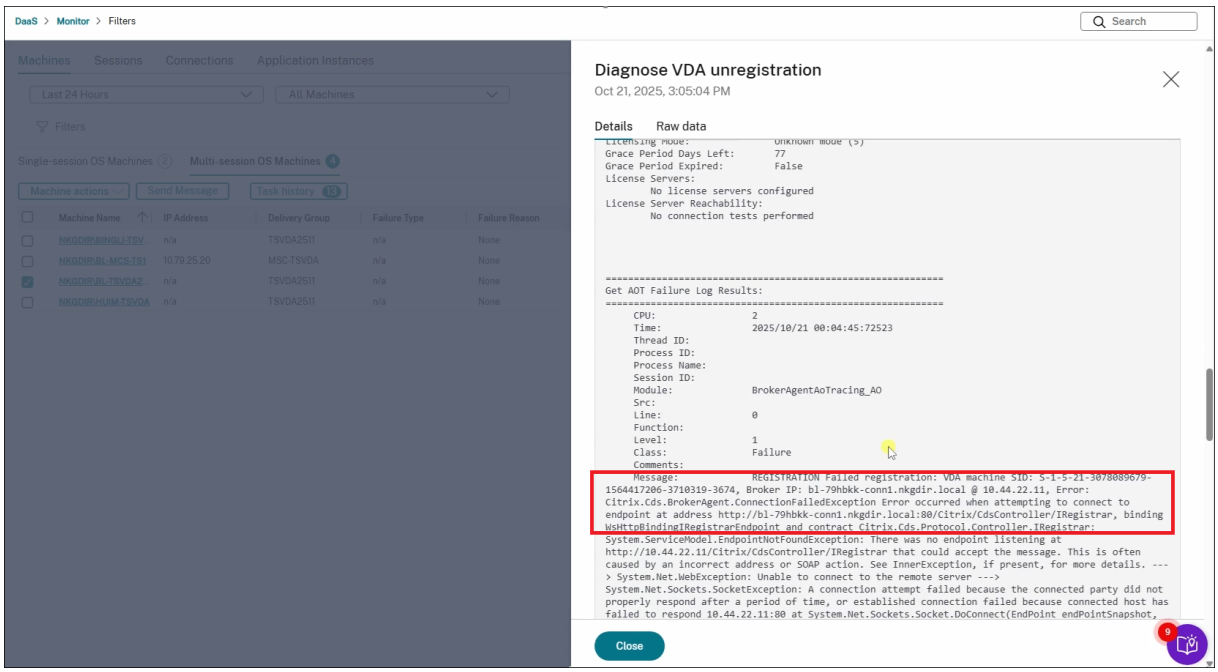
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Citrix Desktop Service errors**. The Citrix service that is required for registration is stopped or unhealthy.



These errors are typically associated with VDA unregistration.



If the result points to network, DNS, controller, domain trust, or certificate issues, resolve those issues based on the diagnostic details. If the result points to a stopped or unhealthy service, continue to the

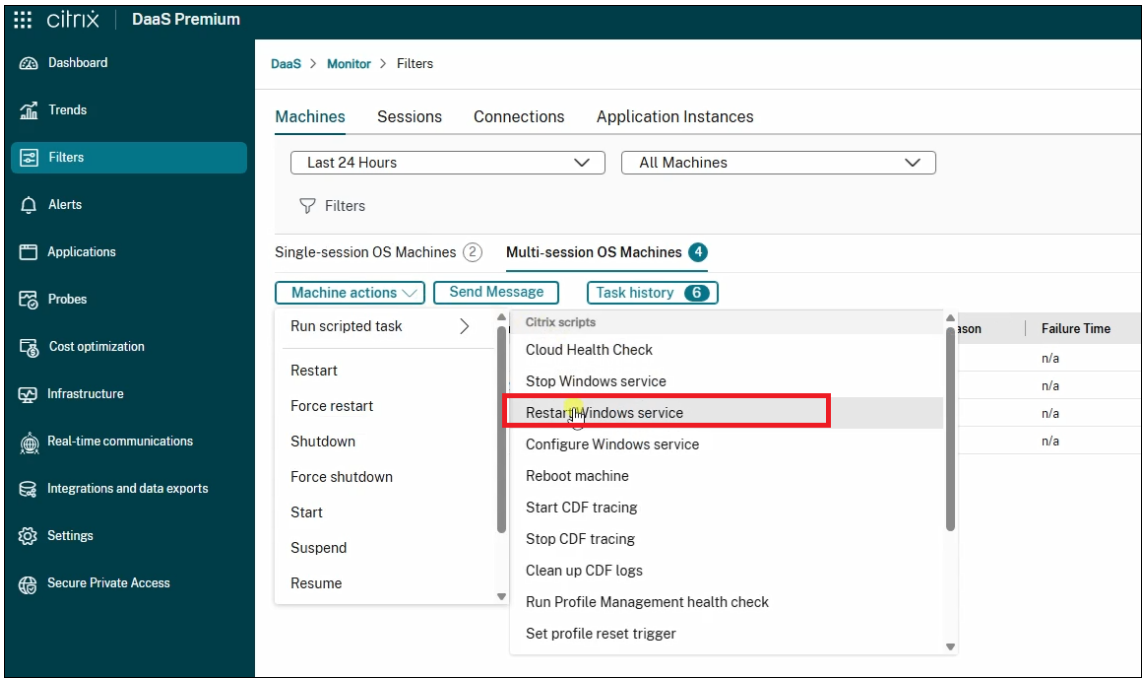
© 1997–2026 Citrix Systems, Inc. All rights reserved.

next step.

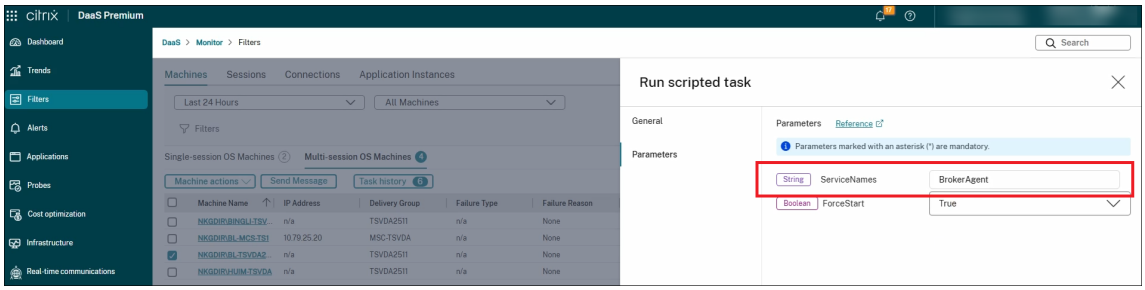
Step 4: Restart the affected Windows service

Run the **Restart Windows Service** scripted task only for *Citrix Desktop Service errors* reported by the diagnosis result.

1. Select the same VDA.
2. Select **Machine actions > Run scripted task > Restart Windows Service**.



3. Enter the service name from the diagnosis result. *For example*, if the result identifies the Broker Agent service, enter `BrokerAgent`.



4. Click **Run** to submit the task and wait for it to finish.

The task restarts the specified service and verifies that the service returns to the `Running` state.

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

Step 5: Verify the VDA registration state

1. In **Monitor**, refresh the machine view.
2. Verify that the VDA registration state changes to **Registered**.
3. Ask the user to launch the app or desktop again.

If the VDA remains unregistered, use the diagnosis result as evidence for further troubleshooting or support escalation. Include the failed checks, related event IDs, and AOT failure log details when you open a support case.

Related information

- Troubleshoot VDA registration and session launch issues using scripted tasks
- Use Windows events as triggers to detect VDA registration issues
- Troubleshoot scripted task execution problems in Monitor
- Scripted Tasks

Troubleshoot VDA registration and session launch issues using scripted tasks

September 7, 2025

As an administrator, you might want to proactively discover issues related to Virtual Delivery Agents (VDAs) in your deployment. This insight can help you resolve issues in time before your users are affected.

Workspace Environment Management (WEM) provides a built-in scripted task, Cloud Health Check, that lets you run checks to gauge the health of VDAs. Using the task, you can identify possible causes for VDA registration and session launch issues. Each time the task runs, a detailed health check report is generated. Based on the report, you can analyze and resolve issues accordingly.

A general workflow to configure the task is as follows:

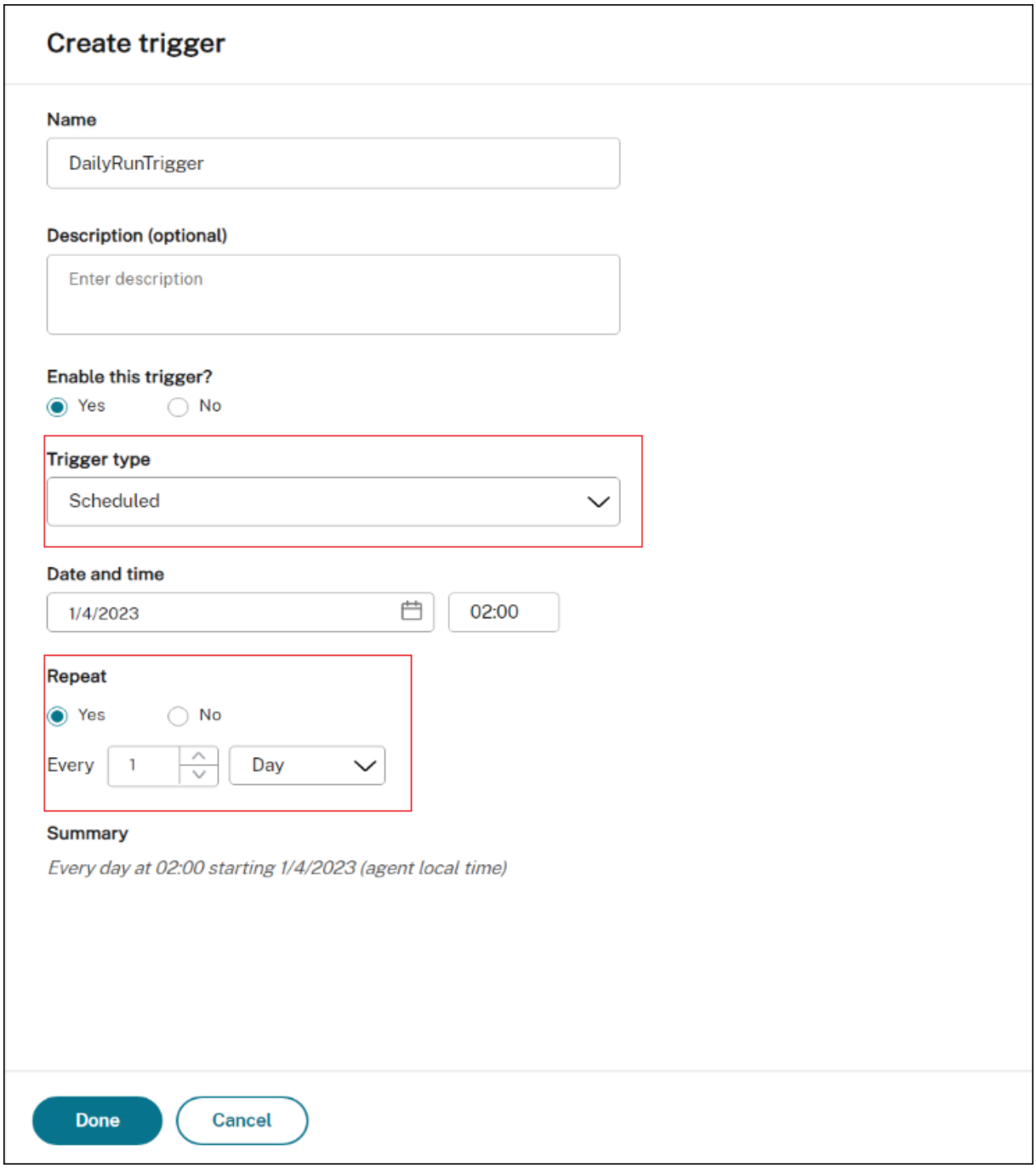
1. Create a scheduled trigger.
2. Associate the trigger with the Cloud Health Check task.
3. View the health check report.

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

Create a scheduled trigger

The following information is supplemental to the guidance in Create a trigger. To add a scheduled trigger, follow the general guidance in that article, minding the details below.

Go to the relevant configuration set, navigate to **Triggers**, and create a trigger as follows:



In this example:

- Name the trigger `DailyRunTrigger`.

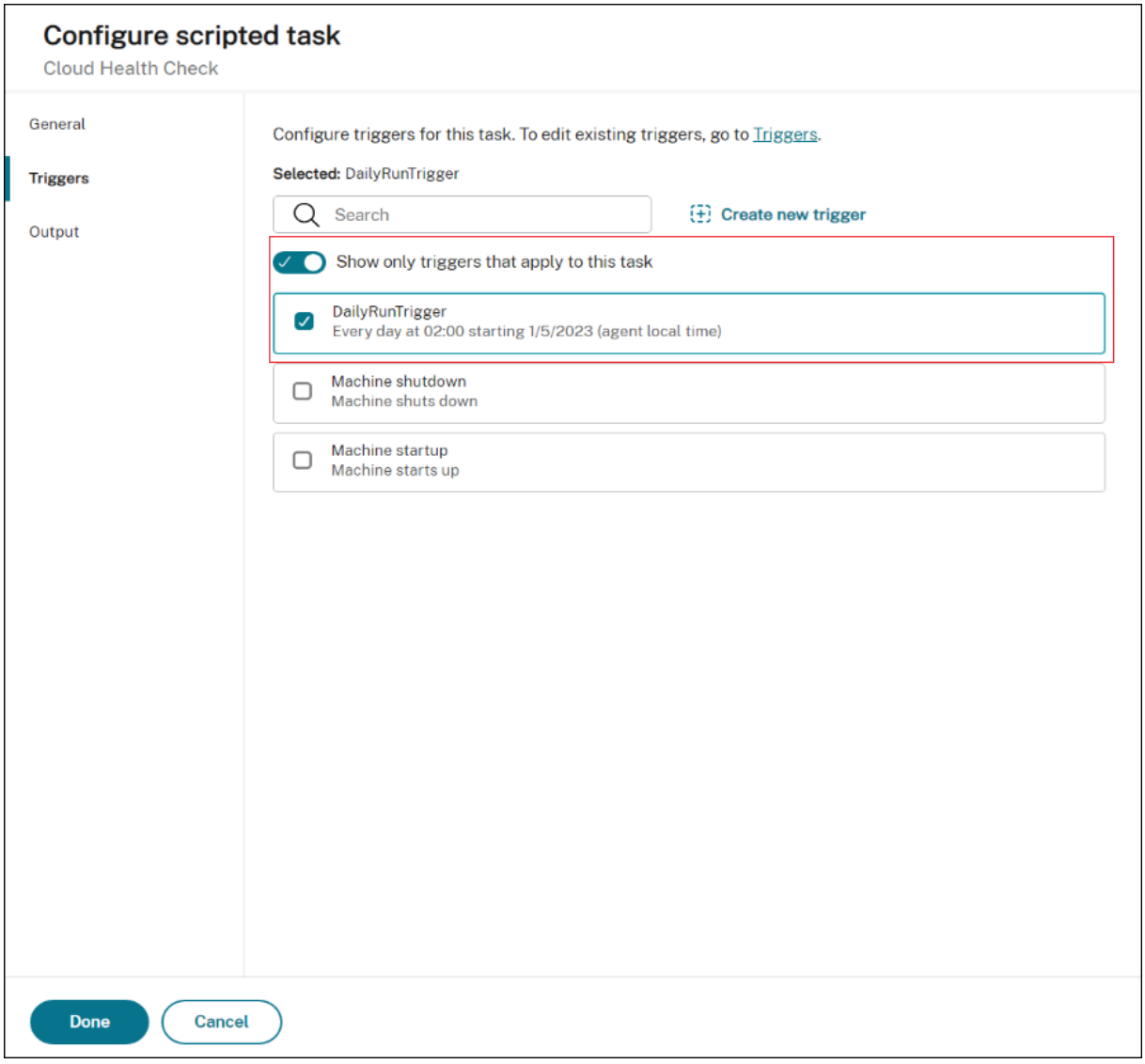
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For **Trigger type**, select **Scheduled**.
- For **Date and time**, configure the task to run at 02:00, April 4, 2023.
- For **Repeat**, configure the task to run every day.

Associate the trigger with the Cloud Health Check task

The following information is supplemental to the guidance in Configure a scripted task. To configure the Cloud Health Check task, follow the general guidance in that article, minding the details below.

Go to the relevant configuration set, navigate to **Scripted Task Settings**, and configure the Cloud Health Check task as follows:

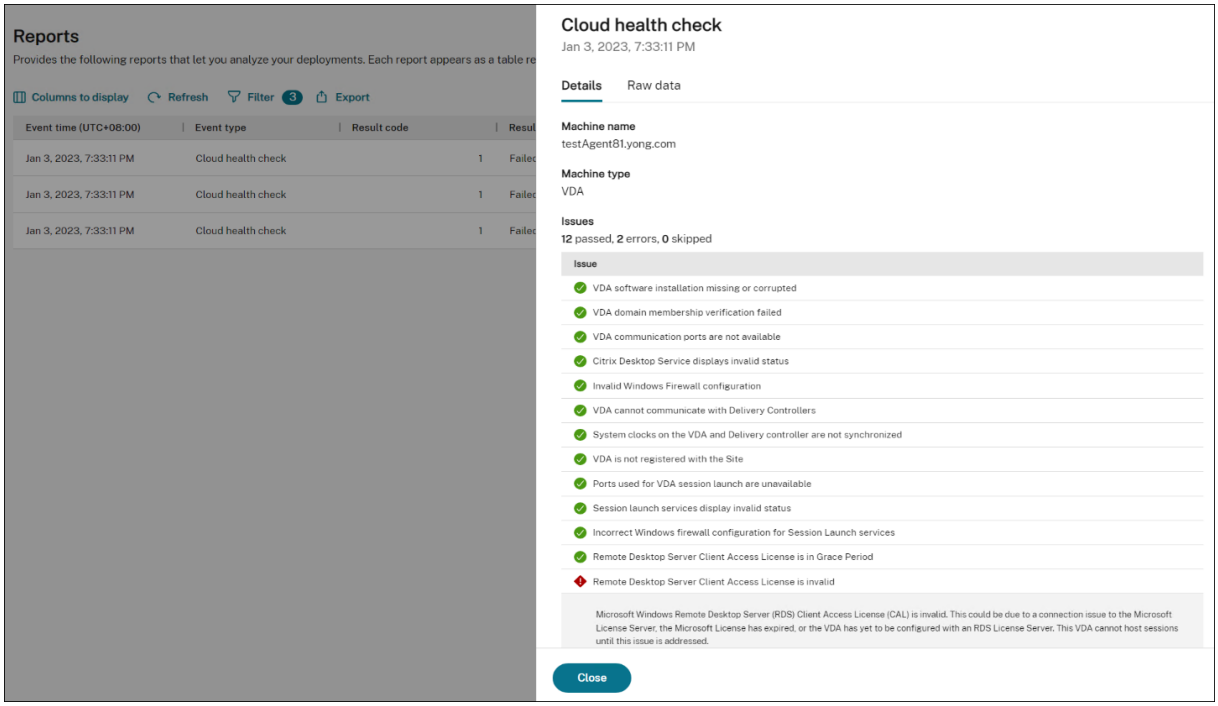


In this example, select the scheduled trigger `DailyRunTrigger` to associate it with the Cloud Health Check task.

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

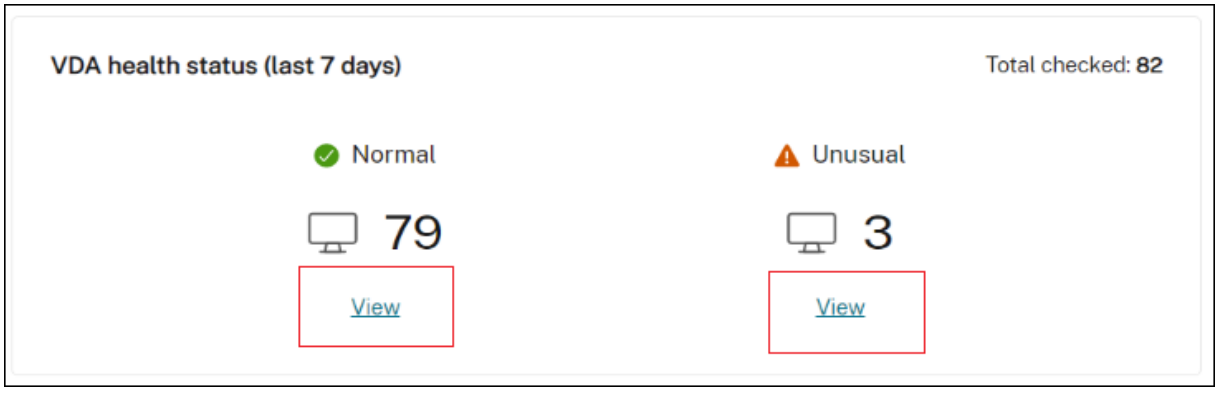
View the health check report

The Cloud Health Check task runs at the scheduled time. After it completes, you can view the health check results by checking the reports. For more information, see Reports.



In **Web Console > Home > Overview**, you can get an overview of VDA health status. To view VDA health status in detail:

- Click **View** under **Normal** to see reports about VDAs in normal state.
- Click **View** under **Unusual** to see reports about VDAs in unusual state.



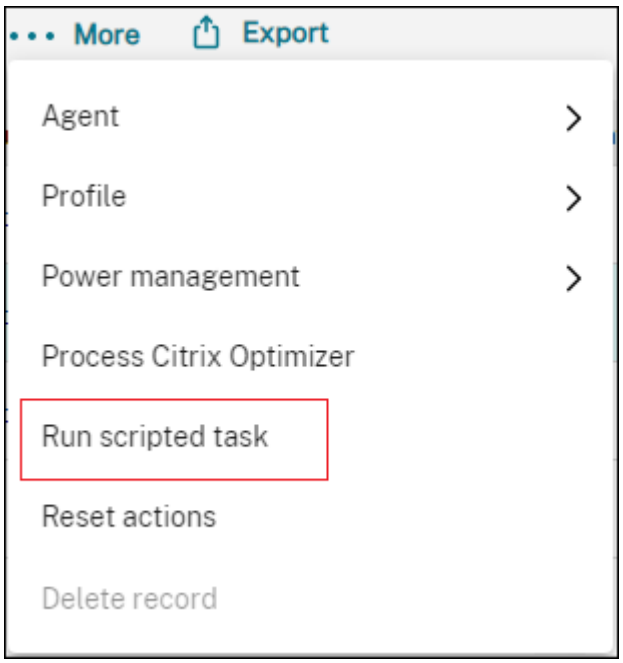
The reports about VDAs in unusual state include issues found and fix recommendations. You can resolve the issues accordingly.

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

Run the Cloud Health Check task on demand

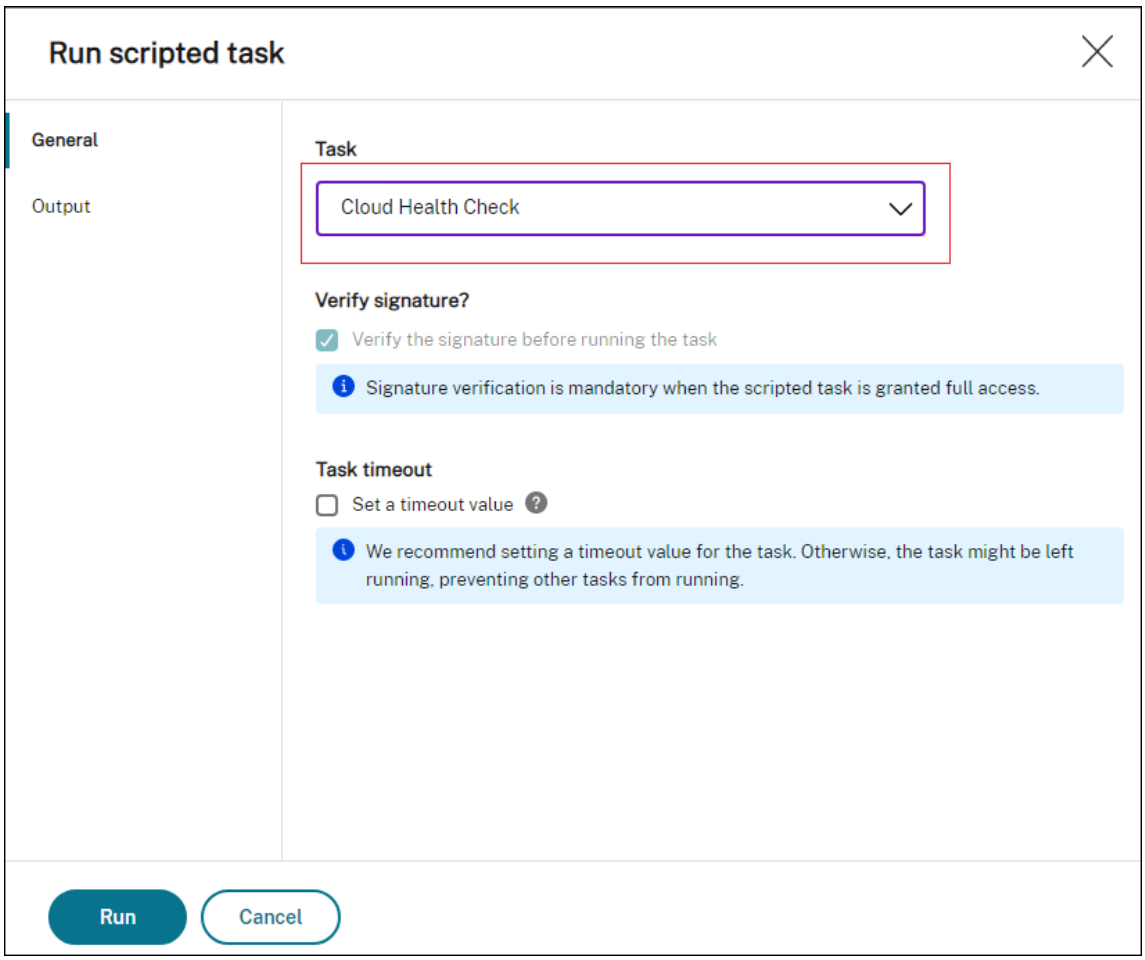
WEM also provides a method to run the task on an agent machine on demand. To do that, perform the following steps:

1. Go to **Monitoring > Administration > Agents**, select the agent, and select **More > Run scripted task**.



2. In the wizard that appears, select **Cloud Health Check** as the task and then click **Run**.

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



3. After the task completes, you can view the health check results by checking the reports. For more information, see Reports.

Use Windows events as triggers to detect VDA registration issues

September 13, 2025

As an administrator, when you encounter VDA registration issues, you might need to log on to each VDA to run the Citrix Health Assistant to troubleshoot VDA registration issues.

With Workspace Environment Management (WEM), you can use Windows events as triggers to detect VDA registration issues. You then associate the triggers with the scripted task, Cloud Health Check. The task is then triggered to run to identify possible causes. Finally, you can use the task report to resolve issues accordingly. This enables you to stay on top of any VDA registration issues and resolve them in time before more users are impacted.

A general workflow to achieve the goal is as follows:

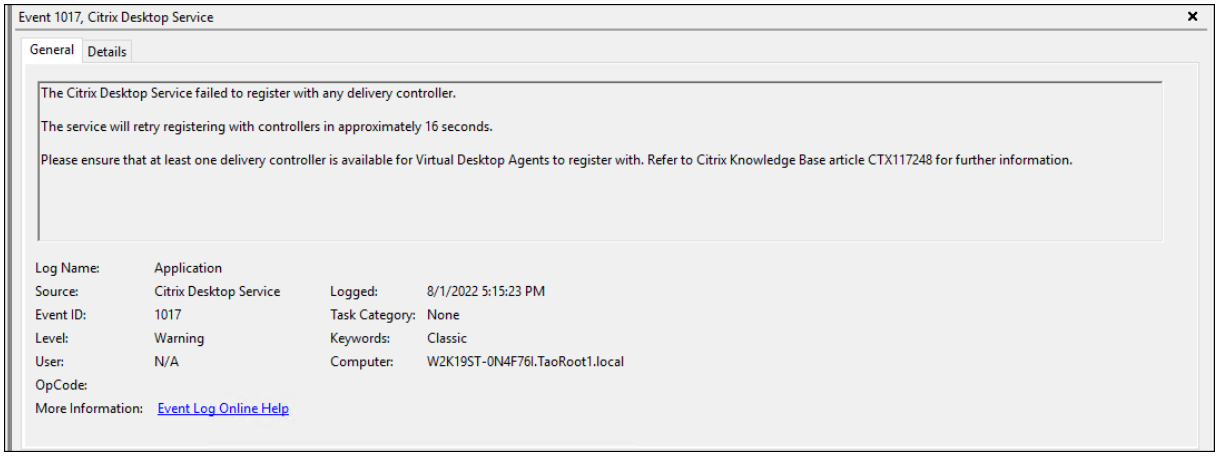
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Get Windows event logs relating to VDA registration issues.
2. Create a Windows event trigger to detect VDA registration issues.
3. Associate the Windows event trigger with the task, Cloud Health Check.
4. View the task execution report.

Get Windows event logs

You need to collect Windows event logs resulting from unregistered VDAs. The information provides clues to understanding the reasons VDAs are unregistered.

The following is an example message in Windows Event Log relating to an unregistered VDA.

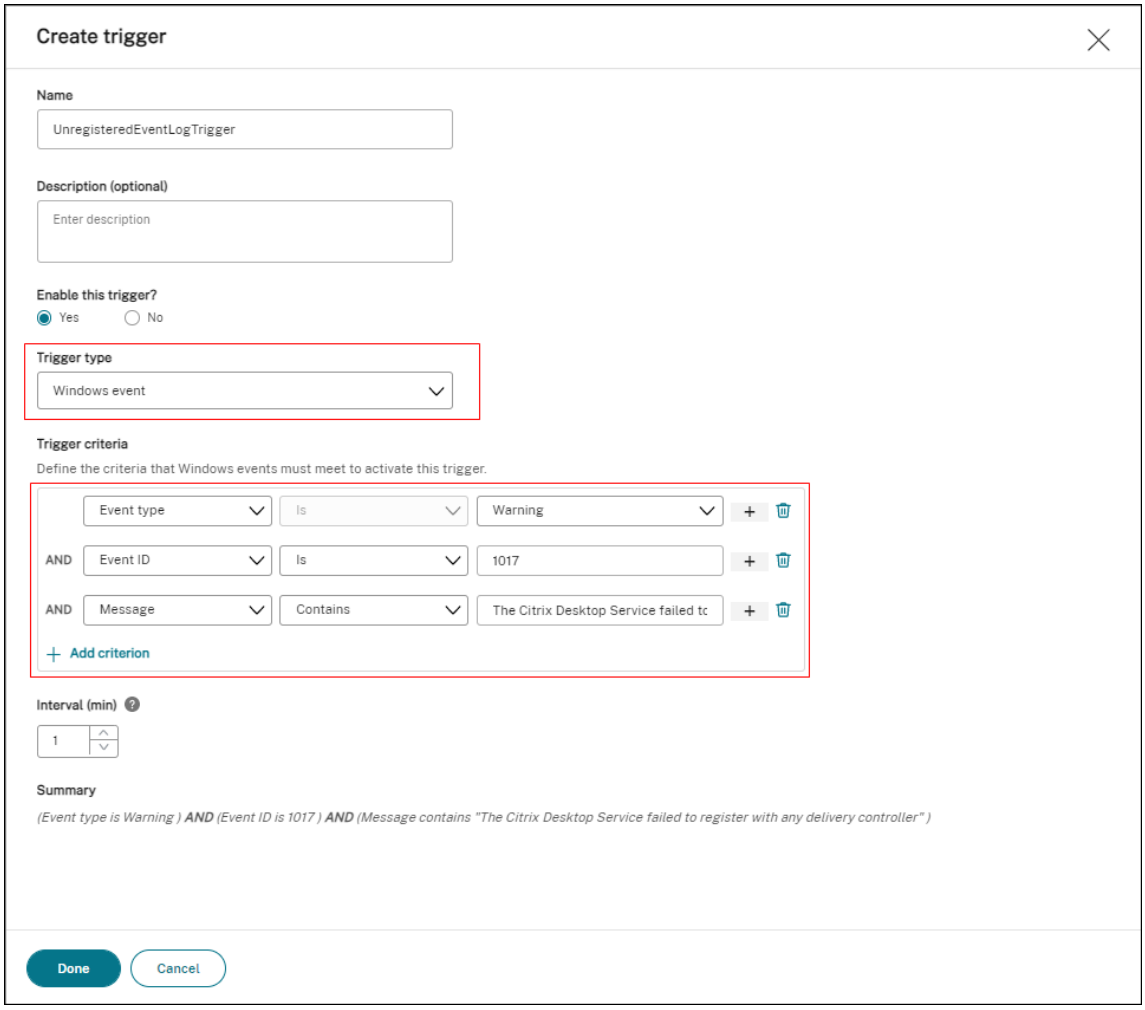


Create a Windows event trigger

The following information is supplemental to the guidance in Create a trigger. To add a Windows event trigger, follow the general guidance in that article, minding the details below.

- Go to the relevant configuration set, navigate to **Triggers**, and create a trigger named `UnregisteredEventLogTrigger`.

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



In this example, configure settings as follows:

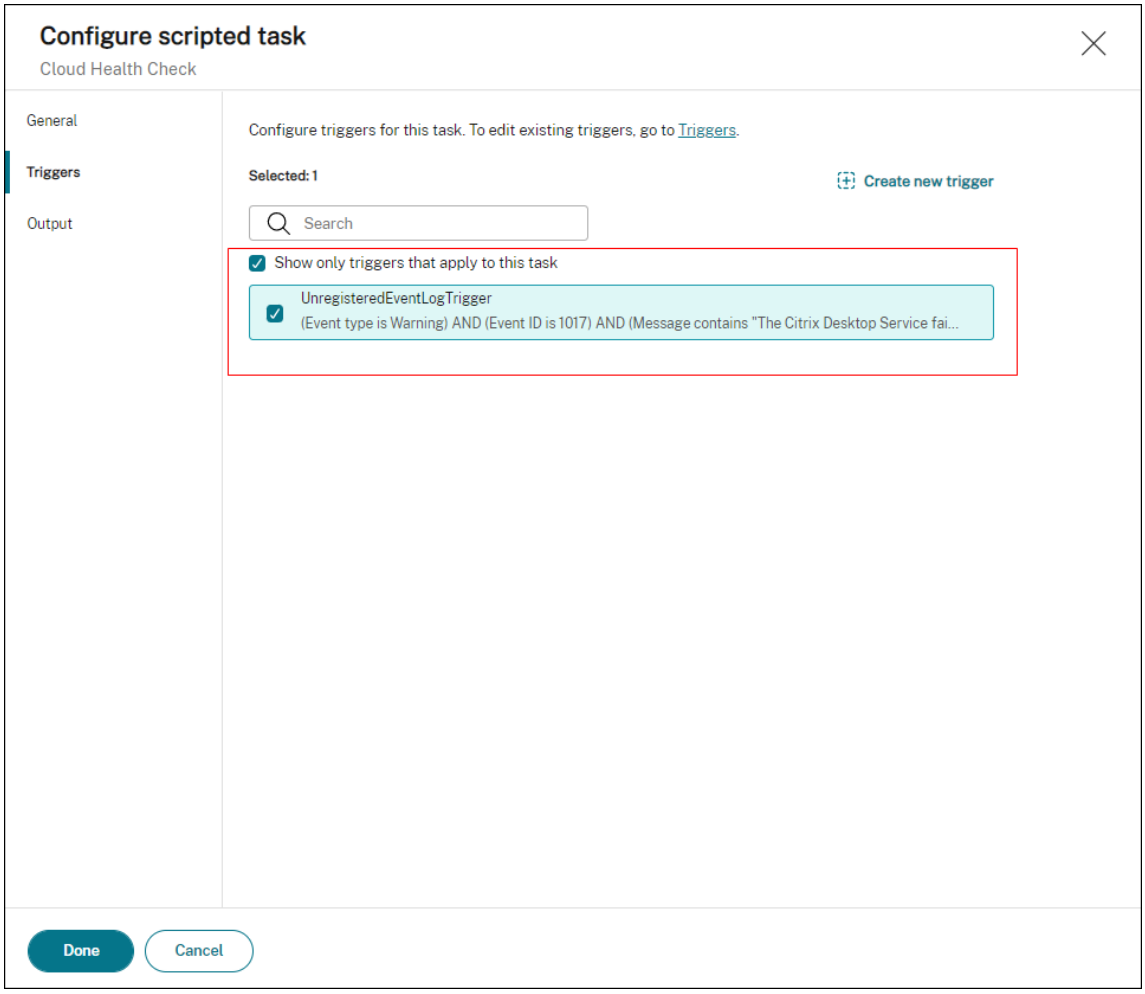
- For **Trigger type**, select **Windows event**.
- For **Trigger criteria**:
  - **Event type**: Warning
  - **Event ID:** `1017`
  - **Message:** `The Citrix Desktop Service failed to register with any Delivery Controller`

Associate the Windows event trigger with Cloud Health Check task

The following information is supplemental to the guidance in Configure a scripted task. To configure the Cloud Health Check task, follow the general guidance in that article, minding the details below.

- Go to the relevant configuration set, navigate to **Scripted Task Settings**, and configure the Cloud Health Check task.

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



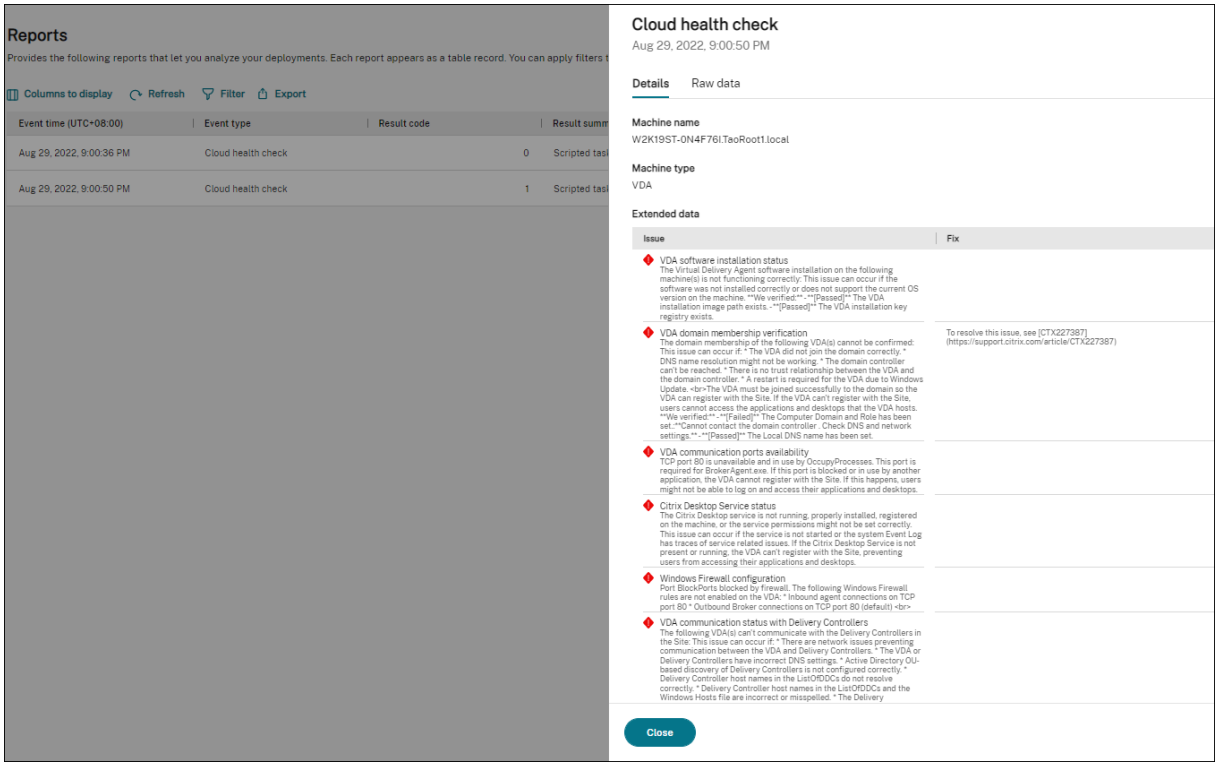
In this example, configure settings as follows:

- In **Triggers**, select the `UnregisteredEventLogTrigger` trigger to associate it with the Cloud Health Check task.

View the task execution report

When VDAs are in an unregistered state, the WEM agent detects the corresponding Windows event log. The Cloud Health Check task runs automatically. You can view the results by checking the reports. For more information, see Reports. In this example, you can see the following report:

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



Based on the report, you can analyze and resolve the issues accordingly.

Agent event logs

April 27, 2026

This article provides a comprehensive list of WEM event logs, along with their corresponding, and distinct event IDs.

WEM configuration set

Event ID	Level	Message
1001	Info	Agent successfully registered with configuration set: name: `configuration set name` (ID: `configuration set ID`).

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

Event ID	Level	Message
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
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

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

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
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

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

Event ID	Level	Message
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`
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

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

Event ID	Level	Message
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
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 }`

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

Event ID	Level	Message
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 }
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

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

> **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` (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`.

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

Event ID	Level	Message
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` (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`.

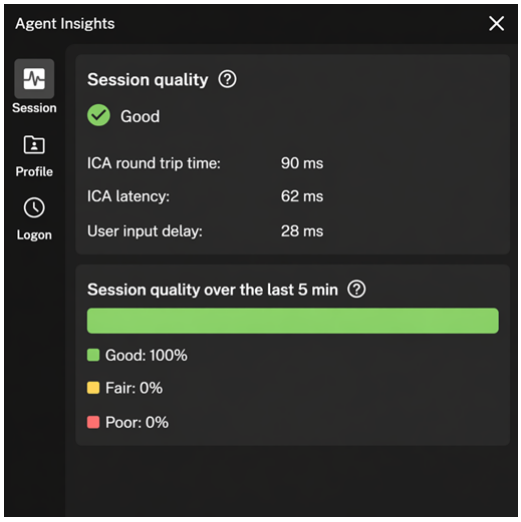
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Level	Message
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

June 11, 2026

Agent Insights is a tool provided with the WEM service agent that helps you monitor and troubleshoot session performance, user profile usage, and logon activity in real time.



> **Note:**
>
> Agent Insights is available only for WEM service agent versions 2511 and later.

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.

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

- **Profile**: User profile details, including profile type, profile size, a list of large files, and (for profile containers) capacity.
- **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 logon data is 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.

If the agent runs in **Basic mode**, use Group Policy to enable this Agent Insights setting: `enableAgentInsightsM`
.

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

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

Reference

The following tabs in the Agent Insights panel provide detailed metrics to help troubleshoot session performance, user profile usage, and logon activity:

- Session
- Profile
- Logon

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

The **Profile** tab displays:

- Profile type
- Profile size
- Capacity (for profile containers only)
- List of large files

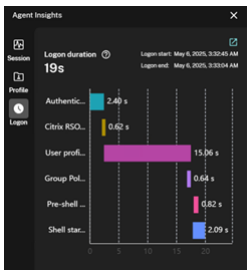
> **Note:**
>
> Profile data is updated when Agent Insights loads. Select **Refresh** to rescan.

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.



> **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.

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

Agent in CMD and UI mode

September 7, 2025

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:

- 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.

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

- **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.

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.

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

> **Note:**
>
> You cannot run the CMD agent and the UI agent at the same time in a session.

Agent-side refresh operations

October 15, 2020

On the agent side, you can perform the following refresh operations:

- Refresh cache. Use a command line to run *AgentCacheUtility.exe* in the agent installation folder, for example:
  - `AgentCacheUtility.exe -RefreshCache`
- Refresh agent host settings. Use a command line to run *AgentCacheUtility.exe* in the agent installation folder, for example:
  - `AgentCacheUtility.exe -RefreshSettings`
- Refresh workspace agents. When the agent is in UI mode, navigate to the agent menu and then click **Refresh**.

	If infrastructure service is online	**If infrastructure service is offline**
Refresh cache	Refreshing the cache synchronizes the agent local cache with the infrastructure service.	The agent local cache cannot be refreshed.

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

	If infrastructure service is online	If infrastructure service is offline
Refresh agent host settings	If the **Use Cache Even When Online** option is enabled, the agent applies the settings that it retrieves from the agent local cache rather than from the infrastructure service. In this case, refresh the cache before refreshing the settings. If the **Use Cache Even When Online** option is not enabled, the agent applies the settings that it retrieves from the infrastructure service.	The agent applies the settings that it retrieves from the agent local cache.
Refresh workspace agents	If the **Use Cache Even When Online** or the **Use Cache to Accelerate Actions Processing** option is enabled, the agent applies the settings that it retrieves from the agent local cache rather than from the infrastructure service. In this case, refresh the cache before refreshing the settings. If the **Use Cache Even When Online** and the **Use Cache to Accelerate Actions Processing** options are not enabled, the agent applies the settings that it retrieves from the infrastructure service.	If the **Enable Offline Mode** option is enabled, the agent applies the user-assigned actions that it retrieves from the agent local cache. If the **Enable Offline Mode** option is not enabled, the agent does not work.

Citrix Environment Tool Hub

April 16, 2026

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

Citrix Environment Tool Hub is a collection of tools that aims to simplify the configuration experience for Workspace Environment Management™ (WEM) administrators. To download it, go to **Citrix Cloud > WEM service > Utilities** 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
- Local administrator privilege

Currently, the following tools are available:

- Application assistant
- File Info Viewer
- File Type Association Assistant
- Group Policy Migration Tool
- Printer Assistant
- Profile Migration Tool
- Rule Generator for App Access Control
- Profile cleanup tool
- Start menu Configurator for Windows 11
- Windows Logon Analysis
- User Store Creation Tool
- WEM Health Check
- Scripted Task Validator
- Migration Tool for Ivanti Workspace Control
- Profile Management Log Parser
- Profile Management Health Check

> **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

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

- 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.
2. Click **Browse resources** to browse your resources. Resources are then enumerated 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.

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

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.
- You can copy the configured FTA data by clicking the **Copy** button.

For more details, see File Type Associations.

Group Policy Migration Tool

This tool enables you to migrate settings from Group Policy to WEM by converting policies and preferences into WEM actions, which you can then manage and assign using the web console.

WEM *Actions* handle user configuration through the WEM agent after the Windows sign-on is finalized. Unlike Windows GPPs, WEM *Actions* do not cause delays in the Windows sign-in process.

This feature allows you to convert settings in Group Policy to actions managed and processed by WEM, reducing the processing time needed during user sign-on.

To migrate settings from Group Policy, consider the following prerequisites:

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

- Machine must be domain joined
- The current user must be a domain user
- Modules required for GPO backup are installed

During the process of Group Policy migration, when the logon scripts are converted into WEM external tasks, an additional optimization for script execution parameters is added. The logon scripts to be migrated must meet the following two requirements:

1. The script file type must be one of the following: `cmd`, `bat`, `ps1`, or `vbs`.
2. The script file must be stored in the built-in shared path on the Domain Controller (DC) (`\\\{ $domainName } \SysVol\\{ $domainName } \Policies\\{ GP_Id } \User\Scripts\Logon`).

You can configure the Group Policy migration by completing the following steps.

1. Export GPPs to the local machine using Citrix Environment Tool Hub: Export the selected settings and save the exported ZIP file to a location that is accessible for the WEM web console.
2. Import GPPs to WEM as actions using the WEM web console: In the web console, navigate to **Assignments > Assignment Groups** in a configuration set and select **Import**. You can create an assignment group with the settings exported, which you can then assign to the users. For more details, see Create an assignment group using the exported settings.
3. Remove migrated settings from the GPO: Once you finish migrating the settings, remove the migrated settings from the GPO by setting the migrated options to **Disabled**. Sign out to verify.
4. Compare the sign-on times.

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.

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

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 romaing 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:

      - **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 if your current account or the alternate account has read access to the source file share and full access to the target file share. If your current account doesn't have access, select the **Use alternate credentials** checkbox to enter the alternate user name and password.

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.

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

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**.

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

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.

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

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:
   - **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.

   > **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**

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

> **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`

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\`

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

- \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.

   > **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.

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

> **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 FXLogix rule sets

Import FSLogix rule sets to reuse existing configurations and quickly create equivalent App Access Control rules.

> **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.

1. 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.
2. 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**.

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

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.
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.

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

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.
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.

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**.
3. You can change the order of the applications by dragging the applications as needed under the **Pinned** layout section.

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

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. You can also integrate this feature/tool into the WEM agent and analyze the logon duration just after you log in.

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 Hello is a biometric authentication feature that allows you to log in to your PC using your face or fingerprint.	Session Arbitration	-	-
			Network Provider	-	-
			Windows authentication	-	-
			VDA authentication	-	-
Citrix RSOP	Time taken to complete Citrix RSOP(Resultant Set of Policy).	-	-	-	-

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

Base-metric	Base-metrics description	Tips	Sub-metrics	Sub-metrics description	Details
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 login process. Make sure that 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 I/Os inside user	Temp File Traverse	-	This metric is available only when a PML exists.
			User profile	Time taken to load Windows user profile files and settings.	-
			SMB client	Time taken to initialize the SMB client for remote connections.	-
			Citrix Profile Management	Time taken to process Profile Management setting.	-
			Citrix Layering Service	-	-
			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.	-

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

Base-metric	Base-metrics description	Tips	Sub-metrics	Sub-metrics description	Details
Group Policy Processing	Time taken to process Group Policy settings.	• **Disable the GPO cache:** Run gpedit.msc and locate to path: **Computer Configuration > Administrative Templates > System > Group Policy** then disable the GPO cache. • **Decrease the number of GPOs:** Decrease the number of GPOs that are processed at once: Group Policy processing is done in	Folder redirection	Time taken to apply folder redirection policies and link user folders to the network location.	-
			Wmi Filter	-	-
			Winlogon notification packages	-	-
			Logon scheduled task	Time taken to run the Group Policy Scheduled Task.	-
			Single Logon Scheduled Task	-	-
			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	-	-

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

Base-metric	Base-metrics description	Tips	Sub-metrics	Sub-metrics description	Details
			Citrix WEM User Group Policy	-	-
			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	-	-
			Group policy objects	Time taken to load group policy objects.	-
			Citrix WEM Query LDAP User Info	-	-
Shell startup	Time taken to run shell startup.	• **Disable startup programs:** You can disable the programs that automatically launch when you turn on your PC. To disable	Shell Start	Time taken to run the shell after loading the windows user profile	-
			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
			Active setup	-	-
			Appx associations	-	-
			Appx load packages	Time taken to load AppX packages.	-
			Pre-shell (Userinit)	Time from the “userinit.exe” to the “explorer.exe”	-
			User Logon Script	-	-
			Logon script processing	Time taken to run logon scripts.	-
			App Readiness tasks	Time taken to complete App Readiness tasks.	-

To integrate the WEM logon duration feature with the WEM agent and analyze logon duration, follow these steps:

1. On the agent machine, run Citrix Environment Tool Hub to monitor logon duration.
2. Log on to the agent machine. The WEM agent analyzes the logon duration and automatically generates a report.
3. Refresh Citrix Environment Tool Hub to view the latest report.
4. Review the logon duration report for the current session. Before proceeding, verify the report history.

Process activity and details

The process activity data captured with Process Monitor during user logon can provide additional information and help you identify issues that cause slow logons. This feature incorporates the process data into the logon reports and allows you to examine the process activity in the context of user logon.

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

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, follow these steps.

1. In the main session, Click **Configure Process Monitor** in the Windows Logon Analysis tool. The session automatically starts the Process Monitor application with predefined settings. You can also configure the session to stop Process Monitor automatically when data collection completes.
2. In the sub-session, trigger the target user logon.
3. In the main session, generate and analyze the logon report, which includes the captured process activity details.

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.

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

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.

- 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.

Profile Management Log Parser

Use this tool to analyze Citrix Profile Management logs. The tool helps you identify and troubleshoot profile-related issues.

To analyze logs, follow these steps:

1. Select logs:

   - Click **Select file** to select a single Citrix Profile Management log file.
   - Click **Select folder** to select a directory containing multiple logs for batch parsing.

   Parsing starts automatically after you make a selection.

2. Select a session:

   After parsing completes, a list of sessions appears. Click a specific session to view its details.

3. Review analysis results:

   - **Summary** tab: View the session duration, profile loading and logoff times, and system information. The **Issues identified from logs** section highlights any detected errors.
   - **Logs** tab: View the formatted log entries related to the selected session.
   - **Applied settings** tab: View the Profile Management policies that were active during that session.

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

Profile Management Health Check

Use this tool to perform a health check on the Citrix Profile Management environment. The tool collects local Profile Management configuration, Profile Management policy settings, event logs, and log file data, and then presents the results with health status indicators and remediation recommendations.

To run the health check, click **Run again**. The report displays the check timestamp and tool version at the top.

The report includes the following tabs:

- **General** tab: Shows environment information and recent session alerts.
    - **Service and driver status**: Shows the running status and version of the Profile Management service, JIT driver, and Action driver.
    - **Profile info**: Shows the profile type, path to the user store, and total folder and file counts.
    - **Machine info**: Shows the machine name and operating system version.
    - **User session alerts during the last 24 hours**: Lists recent session alerts grouped by user, including slow logon and slow logoff detections with profile loading time and logoff duration. Expand **Logs with time gaps** to see consecutive log entries where significant time gaps were detected.
- **Configuration** tab: Shows Profile Management policy settings organized into collapsible sections.
    - **Essential settings**: Shows key configuration values such as path to the user store and multi-session write-back settings.
    - **Log settings**: Shows logging configuration including verbose logging sub-options (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) and maximum log file size.
    - **Other settings**: Shows additional Profile Management settings displayed as label-value pairs.

WEM Health Check

The WEM Health Check tool checks the status of the WEM components and helps you identify and resolve configuration issues with your WEM deployment. The placement of this tool within Citrix Environment Tool Hub directs you to the WEM web console to proceed with the health check process. This tool required a minimum agent version of 2401 or later.

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

Scripted Task Validator

The Scripted Task Validator tool lets you:

- Validate scripted tasks by running them on a WEM Agent machine and reviewing the 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 the signature before running the script
    - Working folder
    - Output files
    - Input parameters
    - 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**.

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

Migration Tool for Ivanti Workspace Control

Use the **Migration Tool for Ivanti Workspace Control** to convert Ivanti Workspace Control configurations for use in WEM. The tool guides you through preparing source files, converting settings, reviewing results, and exporting the converted configuration for import into WEM.

To complete the migration, follow these steps:

1. Open the tool from the Tool Hub.
2. Prepare your files.
    a) Export XML configuration files from Ivanti Environment Manager.
    b) (Optional) Export the Administrative Roles XML file.
3. Convert configuration files.
    a) Select the XML configuration files that you want to convert.
    b) (Optional) Import the Administrative Roles file.
    c) Select **Convert** to start the conversion.
4. Review conversion results.
    a) Review the results across the following tabs:
        - **Converted**: View all settings that were successfully converted.
        - **Unsupported**: View items that can't be converted and were filtered out.
    b) Select the configuration items that you want to export.
    c) Specify a name prefix to apply to exported items.
5. Export converted settings.
    a) Select **Export selected**.
    b) Choose a location to save the file.
    The tool generates a ZIP file containing the exported configuration.
6. In the WEM web console, import the exported file into WEM.
    a) Sign in to the WEM Web console
    b) Import the ZIP file to your configuration set. For more information, see Create an assignment group using the exported settings.

Limitations

Some Ivanti Workspace Control configurations can't be converted. These items appear in the **Unsupported** tab during review.

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

OU assignments Access control based on Organizational Units (OUs) in Ivanti can't be mapped to WEM. We recommend recreating those access control rules manually in WEM.

Empty or invalid configurations The tool filters out configuration items that are missing required information. Examples include:

- Network drives without a path
- Applications without a command line

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.

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

September 7, 2025

The following Control Panel applets are common in Windows:

Applet name	Canonical name

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

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
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

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

Notification Area Icons	Microsoft.NotificationAreaIcons
Pen and Touch	Microsoft.PenAndTouch
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
Windows Update	Microsoft.WindowsUpdate
Work Folders	Microsoft.WorkFolders

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

Customer data management

September 7, 2025

This article describes the customer data associated with Workspace Environment Management™ (WEM) service. It provides information concerning the collection, storage, and retention of customer data involved.

Overview

WEM service uses intelligent resource management and Profile Management technologies to deliver the best possible performance, desktop logon, and application response times for Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) and Citrix Virtual Apps and Desktops deployments. It is a software-only, driver-free solution.

Data location

The following data sources are aggregated in a Microsoft Azure Cloud environment located in the United States (US) or the European Union (EU), depending on the WEM service UI URL.

- For organizations that onboard to WEM service before the enablement of EU-based instances, their storage locations reside in the US.
- For organizations that onboard to WEM service after the enablement of EU-based instances, their storage locations can be different, depending on the home region that the administrators select when onboarding their organizations to Citrix Cloud.
    - If the home region is EU, their storage locations reside in the EU.
    - If the home region is not EU, their storage locations reside in the US.

Data collection

WEM service involves three types of customer data:

- Logs collected from the WEM management console and from the WEM infrastructure services
- WEM service agent actions and policies defined by the administrator
- Statistics associated with end-user activity reported by WEM service agent

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

Data control and storage

Log files. You can use the WEM management console (**Manage** tab) to control the log settings associated with WEM service at any time. You can also enable or disable the log function. The "Citrix WEM Database Management Utility Debug Log.log"log file is located in the WEM infrastructure service installation directory.

WEM service agent actions and policies. All the actions and policies you set up are saved and stored in the back-end Azure database and are accessible only to you through the WEM management console (**Manage** tab).

Statistics on end-user activity. All statistics you monitor in the WEM management console (**Manage** tab) are saved and stored in the back-end Azure database and are accessible only to you through the WEM management console.

Data retention

The customer data associated with WEM service is retained in an identifiable form during the entire service period. Retention periods differ for different types of data:

- Log files are retained for 90 days by default and deleted thereafter. Retaining those log files for a custom time period is not supported.
- WEM service agent actions and policies are kept long term.
- Statistics on end-user activity are retained for 30 days by default and deleted thereafter. Retaining those statistics for a custom time period is not supported.

Dynamic tokens

September 7, 2025

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: Data**
  - With **Action** set to **Set value** and **Type** set to **REG_EXPAND_SZ: Data**
  - With **Action** set to **Set value** and **Type** set to **REG_MULTI: Data**

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

> **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
  - ##FullUserName##
  - ##UserInitials##
  - ##ClientName##
  - ##ClientIPAddress##
  - ##UserLDAPPath##
  - ##ClientRemoteOS##
- ADAttribute
  - [ADAttribute:attrName]
  - [UserParentOU: 1]
- 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**

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

- 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.

- 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**

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

> **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:

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`

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

Modal	Description	Example
#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`
!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\W
##UserStartMenu##	Returns the actual path of the special folder - StartMenu	C:\Users\Jill\AppData\Roaming\Microsoft\W Menu
##UserStartMenuPrograms##	Returns the actual path of the special folder - Programs	C:\Users\Jill\AppData\Roaming\Microsoft\W 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

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

Modal	Description	Example
##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
##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.

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

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 **[ADAttribute:attrName]** value with the related Active Directory attribute. [ADAttribute:attrName] is the dynamic token for any Active Directory attributes. There is a related filter that checks the value of the specified attributes.

For user organizational unit (OU) structures, WEM replaces the **[UserParentOU:level]** value with the related Active Directory OU name. The Active Directory path is the complete user path (LDAP) in Active Directory and [UserParentOU:level] 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 [UserParentOU:level] in the network drive path to resolve the users'OU dynamically. There are two ways to use the dynamic token:

- Use the [UserParentOU:level] 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 [UserParentOU:0]. 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 [ADAttribute:attrName].
There is no dynamic token available for Active Directory Group Match because that condition type is

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

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:

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:

- [RegistryValue:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Agent Host\AgentLocation]

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

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

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]

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
No XenApp Farm Name Match	-	Yes
No XenApp Zone Name Match	-	Yes

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

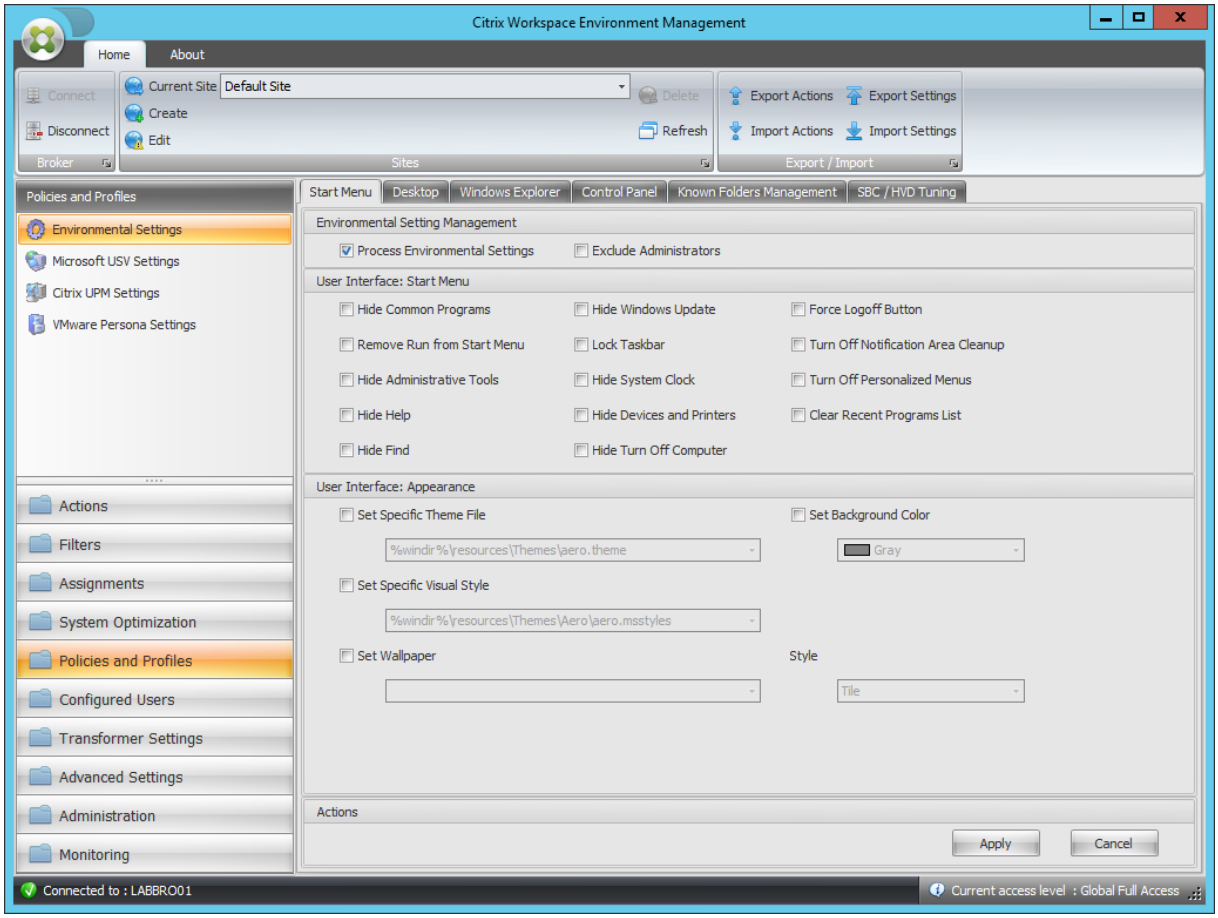
Condition type	Tested value	Matching result
No XenDesktop Farm Name Match	-	Yes
No XenDesktop Desktop Group Name Match	-	Yes
No Active Directory Attribute Match	Yes	Yes
Name or Value is not in List	Yes	Yes
Dynamic Value Match	Yes	Yes
No Dynamic Value Match	Yes	Yes
File Version Match	Yes	Yes
No File Version 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

September 7, 2025

This article describes the registry values associated with Environmental Settings in Workspace Environment Management™ service.

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



Hide Common Programs

Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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\
Value Name	NoRun
Value Type	DWORD

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

Remove Run from Start Menu	
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Hide Administrative Tools	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\
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\E
Value Name	NoSMHelp
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Hide Find	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\E
Value Name	NoFind
Value Type	DWORD
Enabled Value	1
Disabled Value	0

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

Hide Find	
Processing	Service called by agent

Hide Windows Update	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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\
Value Name	LockTaskbar
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Hide System Clock	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	HideClock
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

Hide Devices and Printers	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\
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\
Value Name	NoClose
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\
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\
Value Name	NoAutoTrayNotify

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

Turn Off Notification Area Cleanup	
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Turn Off Personalized Menus	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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\
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

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

Set Specific Theme File	
Disabled Value	Value is absent
Processing	Service at logon

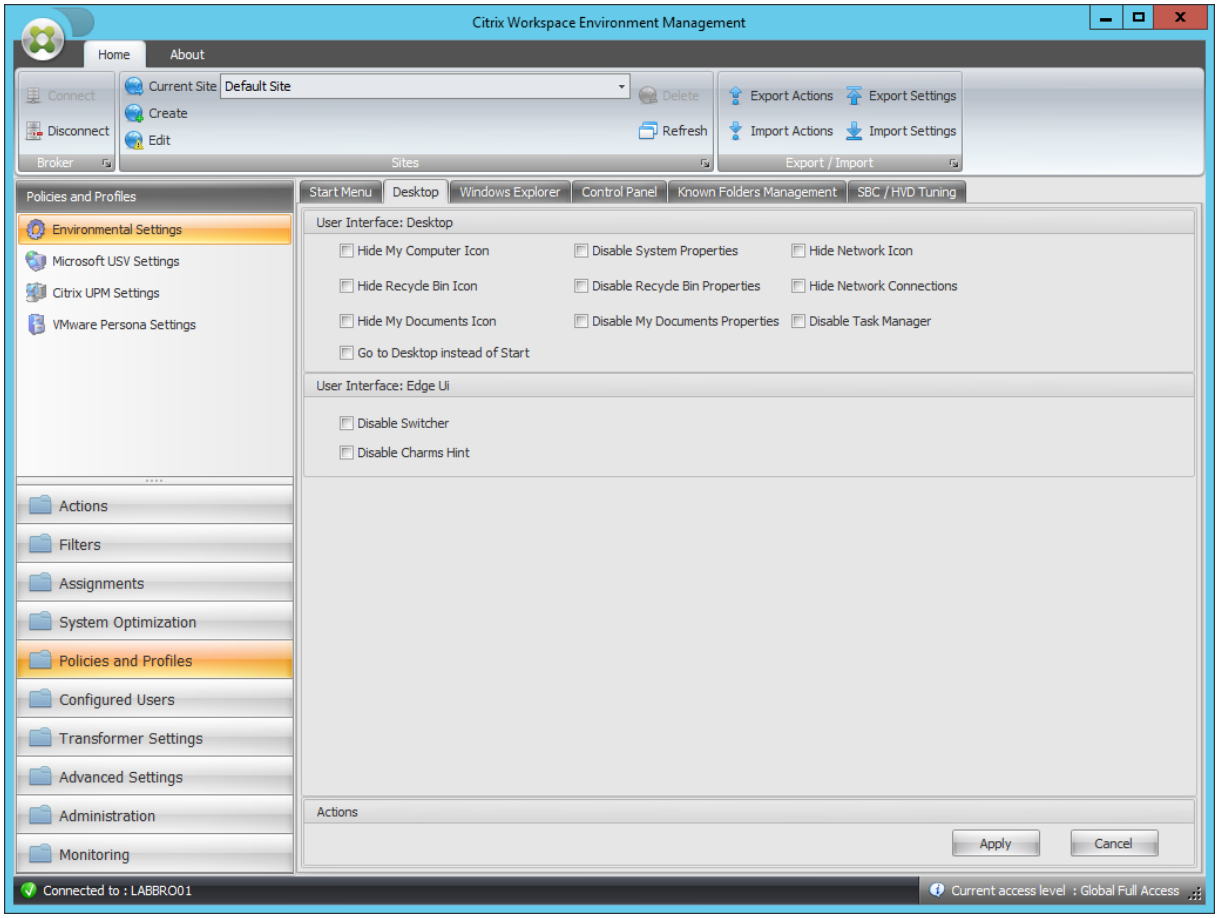
Set Background Color	
Parent Key	HKCU\Control Panel\Colors
Value Name	Background
Value Type	REG_SZ
Enabled Value	Configured color (R G B)
Disabled Value	Value does not exist or 0 0 0 if previously configured value
Processing	Service called by agent

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\
Value Name	Wallpaper
Value Type	REG_SZ
Enabled Value	Path specified in console
Disabled Value	Value is absent
Processing	Service at logon

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

Set Wallpaper	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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\
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\
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\
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\
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\
Value Name	OpenAtLogon

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

Go to Desktop instead of Start	
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service at logon

Disable System Properties	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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\
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\
Value Name	NoPropertiesMyDocuments
Value Type	DWORD
Enabled Value	1

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

Disable My Documents Properties	
Disabled Value	0
Processing	Service called by agent

Hide Network Icon	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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\
Value Name	NoNetworkConnections
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

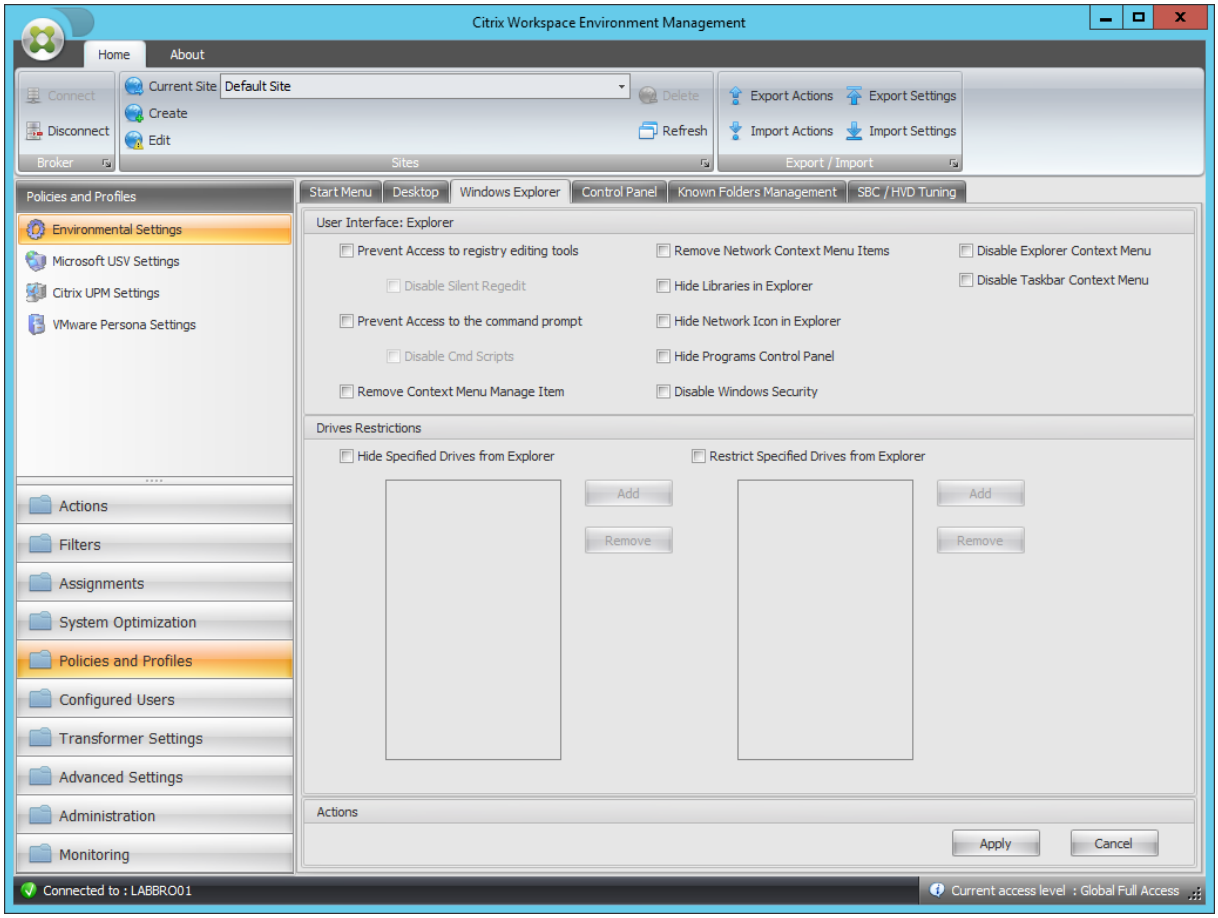
Disable Task Manager	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	DisableTaskMgr
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

Disable Switcher	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Immersiv
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\Immersiv
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\
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
Value Name	DisableCMD
Value Type	DWORD

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

Prevent Access to the Command Prompt	
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\
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\
Value Name	NoNetworkConnections
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Hide Libraries in Explorer	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	{031E4825-7B94-4dc3-B131-E946B44C8DD5}
Value Type	DWORD
Enabled Value	1
Disabled Value	0

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

Hide Libraries in Explorer	
Processing	Service at logon

Hide Network Icon in Explorer	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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\
Value Name	NoProgramsCPL
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Disable Windows Security	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoNtSecurity
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

Disable Explorer Context Menu	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoViewContextMenu
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

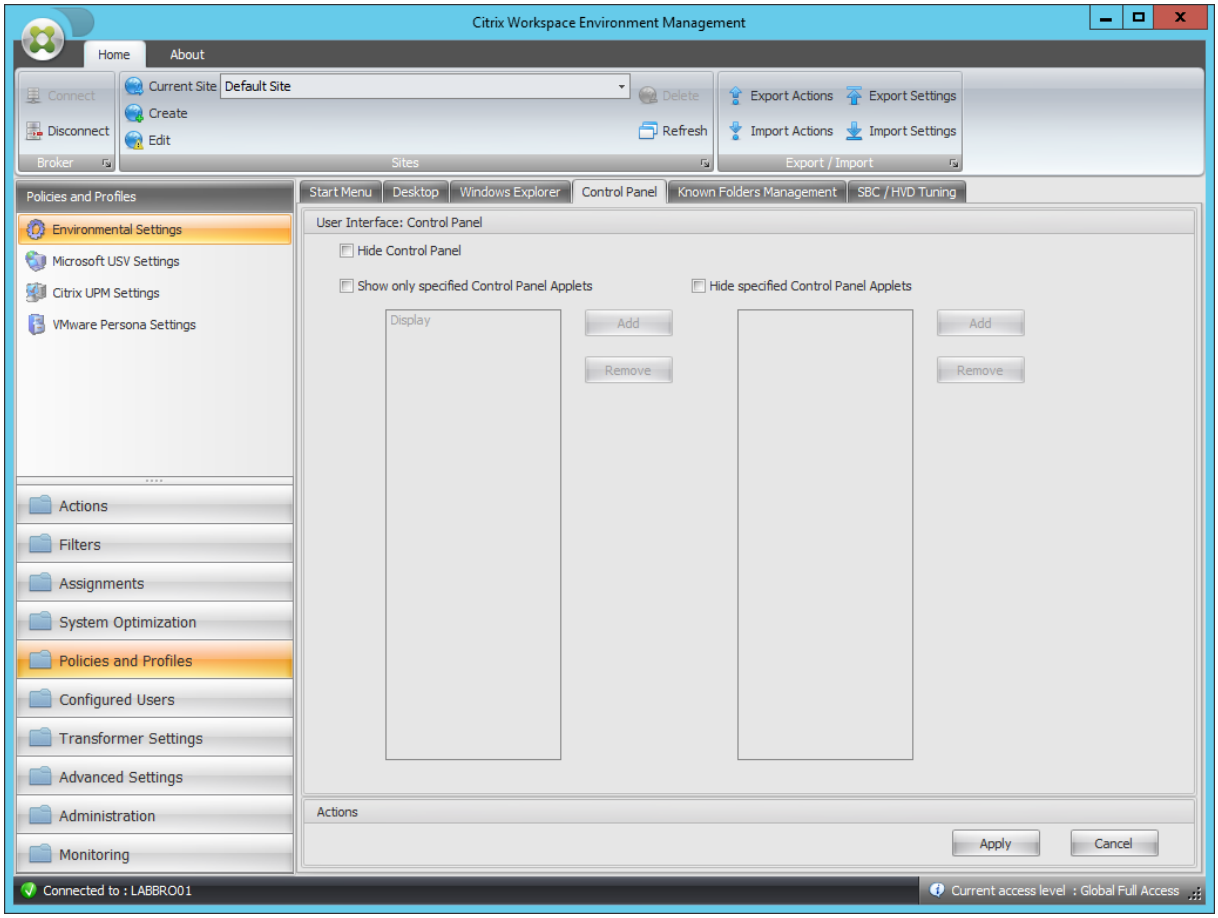
Disable Taskbar Context Menu	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoTrayContextMenu
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Hide specified Drives from Explorer	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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\
Value Name	NoViewOnDrive

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

Restrict Specified Drives from Explorer	
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon



Hide Control Panel	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoControlPanel
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

Hide Control Panel	

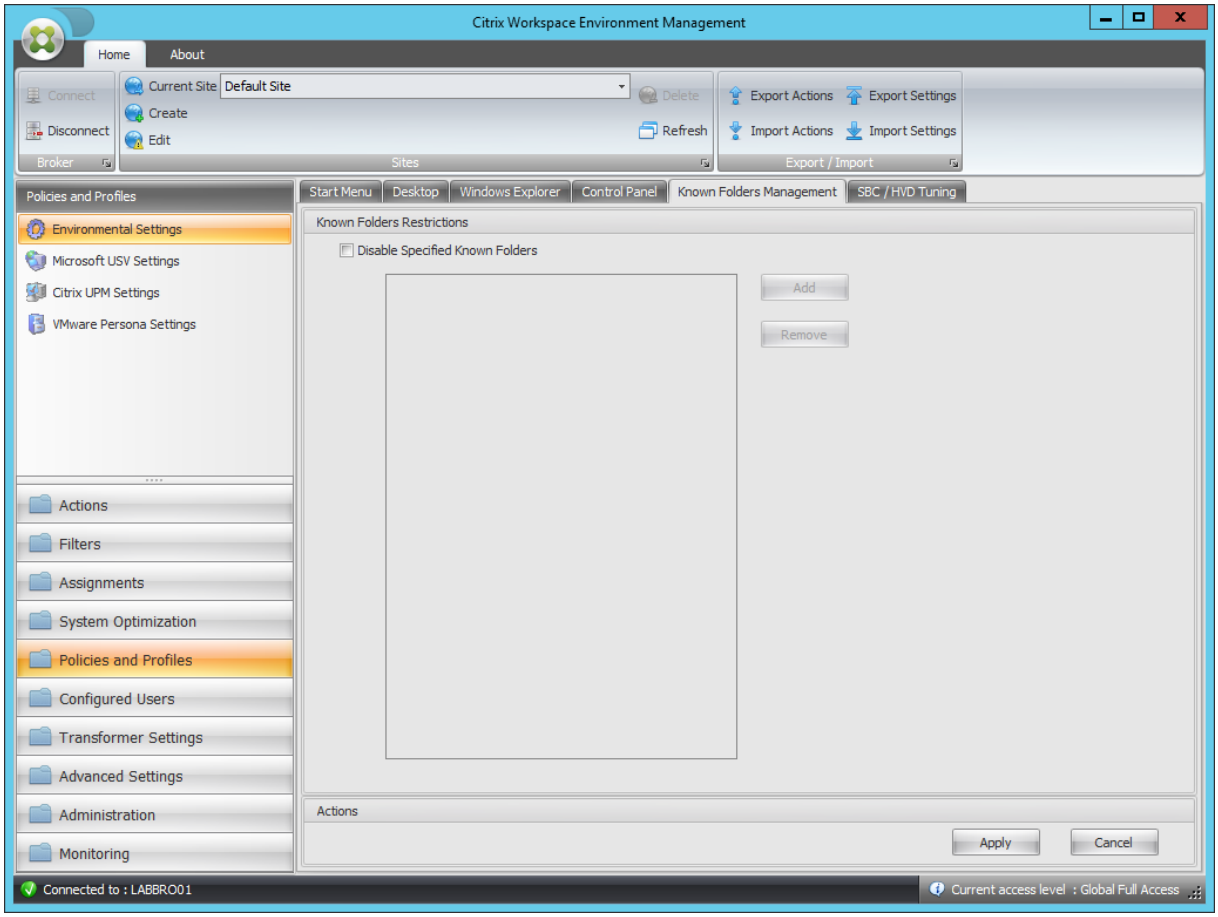
Show only specified Control Panel Applets	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	RestrictCpl
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

For each allowed applet	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ 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\
Value Name	DisallowCpl
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

For each disallowed applet	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\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



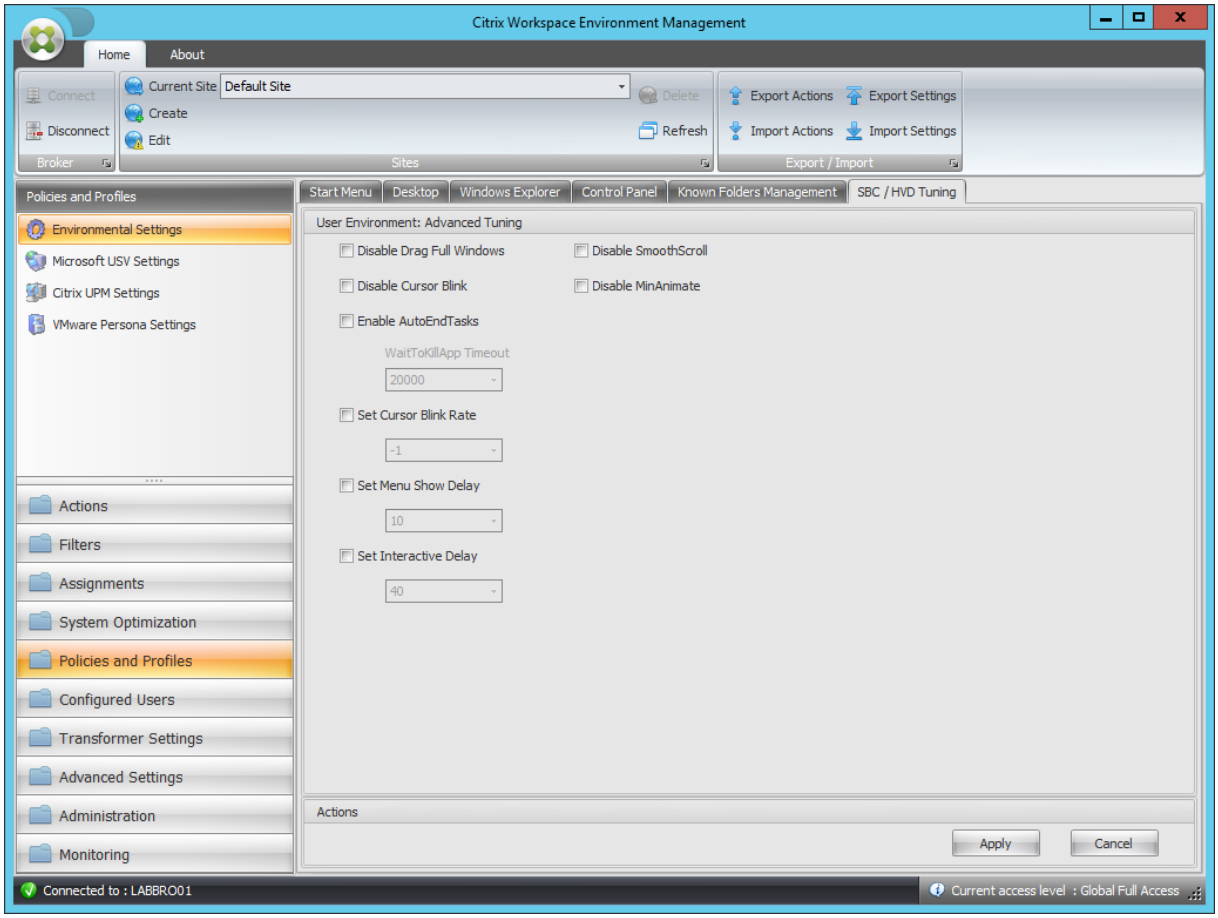
Disable Specified Known Folders	
Parent Key	HKCU\Software\Policies\Microsoft\Windows\Explorer
Value Name	DisableKnownFolders

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

Disable Specified Known Folders	
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
Value Name	Disabled folder name
Value Type	REG_SZ
Enabled Value	Disabled folder name
Disabled Value	Null / Removed
Processing	Service at logon

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



Disable Drag Full Windows

Parent Key	HKCU\Control Panel\Desktop
Value Name	DragFullWindows
Value Type	REG_SZ
Enabled Value	0
Disabled Value	1
Processing	Service at logon

Disable Cursor Blink

Parent Key	HKCU\Control Panel\Desktop
Value Name	DisableCursorBlink
Value Type	DWORD

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

Disable Cursor Blink	
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
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)

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

Set Cursor Blink Rate	
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
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

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

Disable MinAnimate	
Parent Key	HKCU\Control Panel\Desktop
Value Name	MinAnimate
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service at logon

Filter conditions

February 27, 2026

Workspace Environment Management includes the following filter conditions which 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.

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

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.

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

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

Condition Name	**Client IP Address Match**
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.

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.

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

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**
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.
Expected syntax	Two letter ISO language name. Example FR.

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

Condition Name	**User UI Language Match**
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.

Condition Name	**Citrix Provisioning™ Image Mode**
Expected value type	N/A
Expected result type	Select from dropbox.

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

Condition Name	**Citrix Provisioning™ Image Mode**
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
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.

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

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.
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.

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

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). 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.

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

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.

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.

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

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.

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.

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

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.

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.

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

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.

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.

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

Condition Name	**Name is in List**
Expected result type	String. Expected value of the name to look for in the 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. The path must not include any quotes (“).
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.

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

Condition Name	**DateTime Match**
Expected syntax	Single Date: 06/01/2016 Date Range: 06/01/2016-08/01/2016 Multiple entries: 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.

Filter conditions related to Citrix DaaS and Citrix Virtual Apps and Desktops™

WEM supports the following filter conditions for use in your Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) and Citrix Virtual Apps and Desktops deployment. The conditions apply to all currently supported versions. When using the version match condition, be aware of the following considerations:

- You can specify the version numbers in different formats. For example, type `7.30`, `7.30.0`, or `7.30.0.0`. If needed, you can also use the asterisk (*) as a wildcard. For example, `7.30*`. The asterisk matches zero or more characters.
- The specified version is the version number of the Delivery Controller rather than that of the Virtual Delivery Agent. To view the version number, locate the **AutoSelect** application (the AutoSelect.exe file) on the installation media, right-click **AutoSelect**, and click the **Details** tab. The **Product version** field displays the version number that you can specify in WEM.

Condition Name	**Citrix Virtual Apps Version Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Version. Example: 7.30
Expected syntax	N/A
Returns	True if version matches the selected value, false otherwise.

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

Condition Name	**Citrix Virtual Apps Farm Name Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Farm Name. 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. 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
Expected result type	String. Citrix Virtual Desktops Farm Name. 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.

© 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.

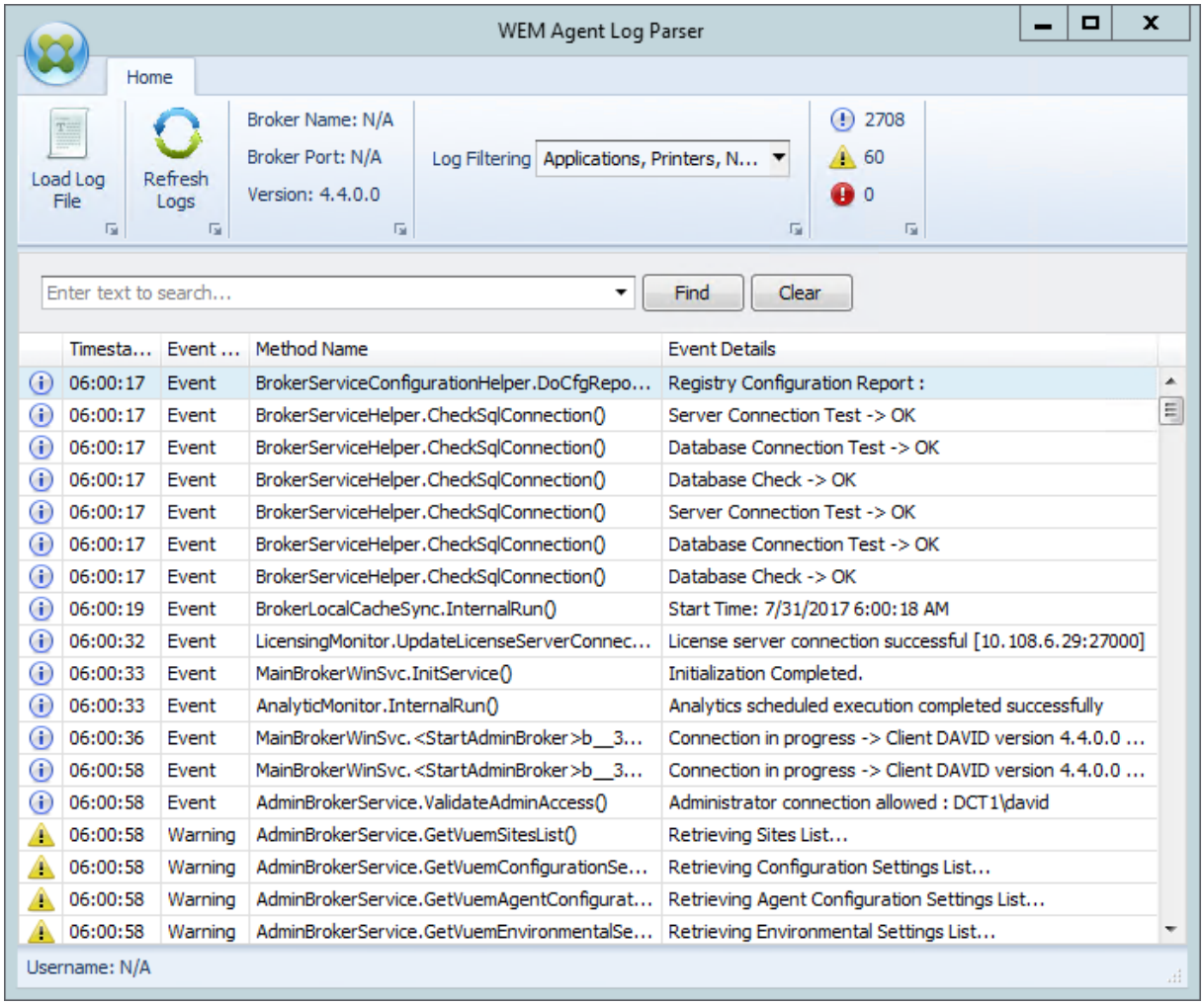
Condition Name	**No Citrix Virtual Desktops Delivery Group Name Match**
Negative condition behavior	Runs Citrix Virtual Desktops Delivery Group Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Desktops DDelivery Group Name Match** for more information.

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

Log parser

September 7, 2025

Workspace Environment Management™ includes a log parser application, which is located in the agent installation directory:



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 log file (the name and port of the infrastructure service it first connected to and the agent version and user name).

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

Port information

September 7, 2025

Workspace Environment Management™ service uses the following ports.

Source	Destination	Type	Port	Details
Agent	WEM service	HTTPS	443	Port on which the on-premises agent connects to the WEM service in Citrix Cloud. This port is available for outbound internet connections.
Agent	Cloud Connector	TCP	8080	Port on which the on-premises agent connects to Cloud Connector. This port is available for outbound LAN (Local Area Network) connections. Messages over the port are secured with Windows Communication Foundation (WCF) message-level security.

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

Source	Destination	Type	Port	Details
Cloud Connector	Agent host	TCP	49752	"Agent port". Listening port on the agent host that receives instructions from Cloud Connector. Ensure that the firewall is configured to permit internal communications between Cloud Connector and WEM service agent. Messages over the port are secured with message-level security.

WEM health check tool

December 4, 2025

The WEM health check tool is a standalone utility installed with the WEM agent. It checks the status of the WEM components and helps you to identify and resolve configuration issues with your WEM deployment.

Launch the tool

The tool requires the **Local administrator** privilege to run. To launch it, on a machine with the WEM agent installed, double-click `Citrix.WEM.Health.Check.Tool.exe` in the following path:

`<Installation folder of WEM agent>\Health Check Tool` (For example, `C:\Program Files (x86)\Citrix\Workspace Environment Management Agent\Health Check Tool`)

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

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 WEM agent and the WEM infrastructure server. Select the **Name**, **Agent Type**, **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.
- 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.

Service agent

To check the configuration of the WEM agent, click the **Start check** button. The following components are considered to generate the health check report.

- Windows Firewall configuration
- Connection method
- Cache location
- Directory service connection time

> **Note:**
>
> - Ensure 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.

The following services are required for the WEM agent to function as expected. Ensure that the services are running and the startup type for each service is set to automatic.

- System event notification service

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

- Citrix WEM agent host service
- Citrix WEM user logon service

XML printer list configuration

September 7, 2025

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<string, List<VUEMUserAssignedPrinter>>>
```

Each device is represented like this:

```
    <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
        <Key>DEVICE1</Key>
        <Value>
            <VUEMUserAssignedPrinter>
                ...
            </VUEMUserAssignedPrinter>
        </Value>
    </SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

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

> **Note:**
>
> When 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.

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>
   </ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

> **Note:**
>
> To ensure that the WEM agent can access the XML printer list file, the XML printer list file must be stored on your local machine or on a shared network resource.

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.

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

<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, the 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 further modified, increment this value by 1 to notify the Agent Host and ensure that the printer action is re-processed.

<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 must be left blank.

<TargetPath>. This path is the UNC path to the printer.

<ExtLogin>. Contains the name of the Windows account used when specifying Windows credentials for connection. [Currently unsupported. Leave this field blank].

<ExtPassword>. Contains the password for the Windows account used when specifying Windows credentials for connection. [Currently unsupported. Leave this field blank].

<Reserved01>. This contains advanced settings. **Do not** alter it in any way.

```
1 &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**

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

```
<?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>
                <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;
                   SelfHealingEnabled&lt;/Name&gt;&lt;Value&gt;0&lt
                   ;/Value&gt;&lt;/VUEMActionAdvancedOption&gt;&lt
                   ;/ArrayOfVUEMActionAdvancedOption&gt;</
                   Reserved01>
            </VUEMUserAssignedPrinter>
      </Value>
     <Value>
            <VUEMUserAssignedPrinter>
                <IdPrinter>2</IdPrinter>
                <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"
```

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

```
                            ?&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;
                            SelfHealingEnabled&lt;/Name&gt;&lt;Value&gt;0&lt
                            ;/Value&gt;&lt;/VUEMActionAdvancedOption&gt;&lt
                            ;/ArrayOfVUEMActionAdvancedOption&gt;</
                            Reserved01>
41                      </VUEMUserAssignedPrinter>
42                  </Value></
                        SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
                        >
43                  <
                         SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
                         >
44                  <Key>DEVICE2</Key>
45                  <Value>
46                      <VUEMUserAssignedPrinter>
47                          <IdPrinter>1</IdPrinter>
48                          <IdSite>1</IdSite>
49                          <State>1</State>
50                          <ActionType>0</ActionType>
51                          <UseExtCredentials>0</UseExtCredentials>
52                          <isDefault>0</isDefault>
53                          <IdFilterRule>1</IdFilterRule>
54                          <RevisionId>1</RevisionId>
55                          <Name>HP LaserJet 2200 Series</Name>
56                          <Description />
57                          <DisplayName />
58                          <TargetPath>\\server.example.net\HP LaserJet 2200
                                Series</TargetPath>
59                          <ExtLogin />
60                          <ExtPassword />
61                          <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;
                                SelfHealingEnabled&lt;/Name&gt;&lt;Value&gt;0&lt
                                ;/Value&gt;&lt;/VUEMActionAdvancedOption&gt;&lt
                                ;/ArrayOfVUEMActionAdvancedOption&gt;</
                                Reserved01>
62                      </VUEMUserAssignedPrinter>
63                  </Value></
                        SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
                        >
64              </
                    ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
                    >
```

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

Glossary

September 7, 2025

This article contains terms and definitions used in the Workspace Environment Management™ (WEM) software and documentation.

[1] on-premises term only

[2] 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 [1]. 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.

agent port [1]. 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.

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

agent service port [1]. 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 [1]. 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 [1]. 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™ [2]. 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 [1]. The account used by the database creation wizard to connect to the SQL instance to create the Workspace Environment Management database.

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 [1]. 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).

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

infrastructure service account [1]. 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 [1]. 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 [1]. 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".

mixed-mode authentication [1]. 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 [2]. 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 [2]. *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).

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

Site. Legacy term for "Configuration set".

SQL user account [1]. 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.

vuemUser [1]. 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 [1]. 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 [2]. A Citrix Cloud service which delivers WEM management components as a SaaS service.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.