Workspace Environment Management 1903

Contents

Workspace Environment Management 1903

April 3, 2019

Workspace Environment Management 1903 is the current release. For documentation of earlier releases and the Citrix Cloud Workspace Environment Management service, see the following sections:

- Workspace Environment Management 1811
- Workspace Environment Management 1808
- Workspace Environment Management 4.7
- Workspace Environment Management 4.6
- Workspace Environment Management 4.5
- Workspace Environment Management 4.4
- Earlier versions of Workspace Environment Management
- Workspace Environment Management service

For information about upgrading, see Upgrade a deployment.

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

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

Introducing Workspace Environment Management

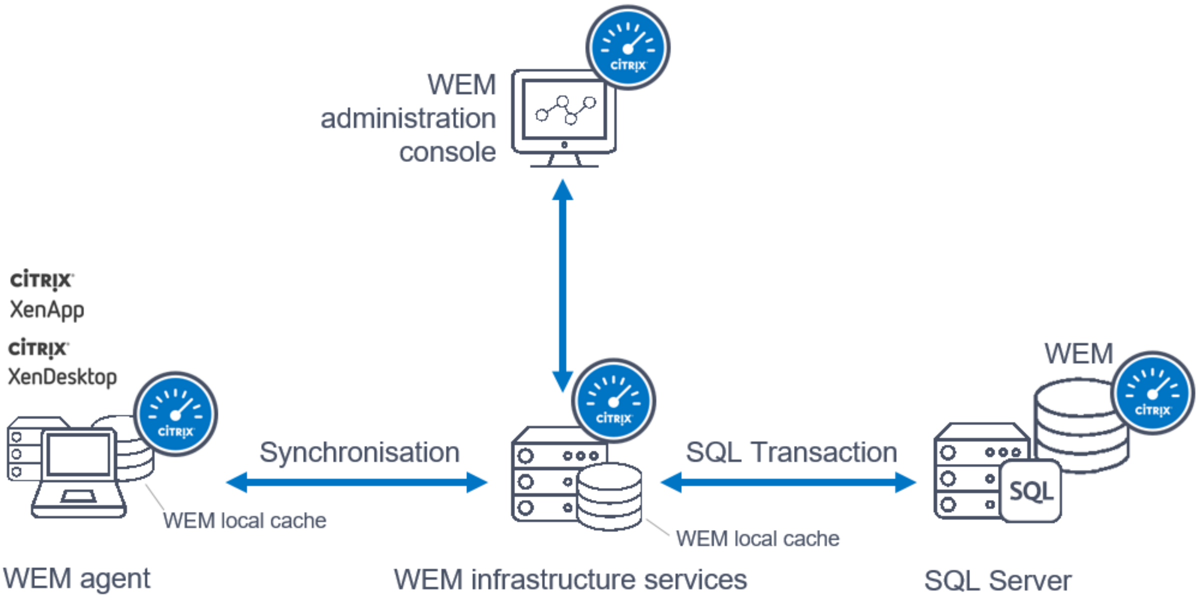
Workspace Environment Management uses intelligent resource management and profile management technologies to deliver the best possible performance, desktop logon, and application response times for Citrix Virtual Apps and Desktops deployments. It is a software-only, driver-free solution.

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

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

Technical overview

Workspace Environment Management (WEM) has the following architecture:



Infrastructure services. The infrastructure services are installed on a Windows server. They synchronize the various back-end components (SQL Server, Active Directory) with the front-end components (administration console, agent).

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

Administration console. The Workspace Environment Management administration console is installed on a Windows client or on a server operating system (OS). It connects to the infrastructure services. You use the administration console to manage your Workspace Environment Management installation (to create and assign resources, manage policies, authorize users, and so on).

Agent. The Workspace Environment Management agent connects to the Workspace Environment Management infrastructure services and is responsible for enforcing the settings you configure by using the administration console. The agent can either be deployed on VDAs or on physical Windows devices (for Transformer use cases). It can be installed on a Windows client (to manage client environments) or on a Windows Server (to manage server environments, or to manage published desktops and applications).

> **Note:**
>
> - The agent cannot be installed on the infrastructure server. The agent installer fails in this scenario.

> - The Transformer feature is not supported on server operating systems.

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

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

What's new

April 28, 2019

For information about upgrading, see Upgrade a deployment.

What's new in Workspace Environment Management 1903

Workspace Environment Management 1903 addresses several issues to improve the user experience. For information about bug fixes, see Fixed issues.

> **Note:**
>
> New product names and version numbers were introduced in Workspace Environment Management 1808. That information is retained in this article for reference. For more information, see New product names and New product and component version numbers in this article.

What's new in previous releases

What's new in Workspace Environment Management 1811

Workspace Environment Management 1811 includes the following new features. For information about bug fixes, see Fixed issues.

Administration console

A Profile Management health status column is provided on the **Administration** > **Agents** > **Statistics** tab. As of this release, Workspace Environment Management supports performing automated status checks on your agent hosts to determine whether Profile Management is configured optimally. You can view the status in the column.

Documentation

Workspace Environment Management documentation is updated to reflect current product behavior.

What's new in Workspace Environment Management 1808

New product names

If you've been a Citrix customer or partner for a while, you'll notice new names in our products and in this product documentation. If you're new to this Citrix product, you might see different names for a product or component.

The new product and component names stem from the expanding Citrix portfolio and cloud strategy. Articles in this product documentation use the following names:

- **Citrix Virtual Apps and Desktops:** Citrix Virtual Apps and Desktops offers a virtual app and desktop solution, provided as a cloud service and as an on-premises product, giving employees the freedom to work from anywhere on any device while cutting IT costs. Deliver Windows, Linux, web, and SaaS applications or full virtual desktops from any cloud: public, on premises or hybrid. Virtual Apps and Desktops was formerly XenApp and XenDesktop.
- **Citrix Workspace app:** The Citrix Workspace app incorporates existing Citrix Receiver technology as well as the other Citrix Workspace client technologies. It has been enhanced to deliver additional capabilities to provide end users with a unified, contextual experience where they can interact with all the work apps, files, and devices they need to do their best work. For more information, see this blog post.
- **Citrix Provisioning:** The Citrix Provisioning is a solution for managing virtual machine images, combining previous technologies known as Machine Creation Services (MCS) and Citrix Provisioning Services (PVS). Citrix Provisioning was formerly Provisioning Services.

Here's a quick recap:

Is	Was
Citrix Virtual Apps and Desktops	XenApp and XenDesktop
Citrix Workspace app	Citrix Receiver
Citrix Provisioning	Provisioning Services

Implementing this transition in our products and their documentation is an ongoing process.

- In-product content might still contain former names. For example, you might see instances of earlier names in console text, messages, and directory/file names.

- It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.
- Related product documentation and other resources (such as videos and blog posts) that are linked from this product's documentation might still contain former names.

Your patience during this transition is appreciated. For more detail about our new names, see https://www.citrix.com/about/citrix-product-guide/.

New product and component version numbers

In this release, product and component version numbers are displayed in the format: ***YYMM.c.m.b***.

- *YYMM* = Year and month when the features are finalized. For example, if the features are finalized in August, a release in September 2018 appears as 1808.
- *c* = Maintenance version (if applicable).
- *m* = Citrix Cloud release number for the month.
- *b* = Build number. This field is shown only on the About page of the product, and in the OS's feature for removing or changing programs.

For example, **Workspace Environment Management 1808.0.1** indicates that the released product with features finalized in August 2018 is associated with Citrix Cloud release 1 in that month, and is not a maintenance version. Some UI elements display only the version's year and month, for example, **Workspace Environment Management 1808**.

In earlier releases of this product (Workspace Environment Management 4.7 and earlier), version numbers were displayed in the format: 4.version, where the version value incremented by one for each release. For example, the release following 4.6 was 4.7. Those earlier releases will not be updated with the new numbering format.

Administration console

In this release, an "Everyone" default group is provided on the **Assignments > Action Assignment** tab. To simplify assigning actions for all users in Active Directory, you can use the 'Everyone' default group to assign the actions.

Profile management

As of this release, Workspace Environment Management supports configuring all settings for Citrix Profile Management 1808. The following new options are now available in the administration console:

- **Enable application profiler** (option for defining application-based profile handling)
- **Enable search index roaming for Microsoft Outlook users** (option for improving the user experience when searching mail in Microsoft Outlook)

- **Enable Large File Handling** (option for eliminating the need to synchronize large files over the network)

Documentation

Workspace Environment Management documentation is updated to reflect current product behavior.

What's new in Workspace Environment Management 4.7

New-wemDatabase PowerShell cmdlet updated

PowerShell modules in the Workspace Environment Management SDK are updated at this release. A new parameter CommandTimeout is provided for the **New-wemDatabase** cmdlet which allows you to configure timeout period for connection attempts to the WEM database. After the timeout period an error message is displayed. The default timeout is 300 seconds.

Documentation

Workspace Environment Management documentation is updated to reflect current product behavior.

The Workspace Environment Management SDK documentation is updated to version 4.7.

What's new in Workspace Environment Management 4.6

Assigned applications can include StoreFront store apps

You can now assign resources published in Citrix StoreFront stores as application shortcuts in Workspace Environment Management. This allows you to configure Start menu shortcuts which Workspace Environment Management end users can use to easily access remote store resources. Agent host machines configured to use the Transformer feature show shortcuts to Citrix StoreFront store resources inside the Applications tab. Configure the StoreFront stores that Citrix Receiver connects to using a new Advanced Settings tab. Then add store resources as applications in the Add Application dialog, which contains a redesigned General settings tab. For more information see Applications.

Transformer integrated with Receiver for Windows SDK

Transformer is now integrated with the Citrix Receiver for Windows SDK. This allows you to make StoreFront-based assigned application actions available to Transformer kiosk users, and for Citrix Receiver pass-through authentication to be used. Only published applications which users have permission to access are displayed in the Transformer kiosk Applications tab.

> **Note:**
>
> If you have previously configured Transformer for **Enable Autologon Mode** and now wish to configure users for Transformer integrated with Receiver for Windows SDK, you must clear the option **Enable Autologon Mode** (in the "Transformer Settings > Advanced > Logon/Logoff & Power settings" tab). This allows users to log in to the Transformer client endpoint machine using their own credentials. These credentials are passed through to provide access to their assigned StoreFront-based applications.

Active Directory performance

The Active Directory Subsystem has been redesigned to improve performance and stability. Performance improvements are particularly noticeable when you add AD or OU objects, and dead forests or domains are detected in your environment.

User interface

The administration console user interface has changed:

- In **Advanced Settings** > **Configuration** pane, there is a new **StoreFront** tab for configuring the StoreFront stores that Citrix Receiver connects to.
- In **Actions** > **Applications**, the **Add Application** dialog **General Settings** tab is redesigned for adding StoreFront store resources as applications. The **Advanced Settings** tab **Application Type** option is removed.
- In **Active Directory Objects,** there is a new **Advanced** pane. The **AD Settings** tab contains a new option **Active Directory search timeout** for configuring how long Active Directory searches are performed before they time out. The default value is 1000 msec. We recommend that you use a timeout value of at least 500 msec to avoid timeouts before searches complete.

Agent administrative templates

The administrative templates provided to configure the agent have been renamed to make the filenames versionless. For more information see Configure the agent.

Documentation

Workspace Environment Management documentation is updated to reflect current product behavior.

What's new in Workspace Environment Management 4.5

Application security

Application Security functionality has been added to the administration console **Security pane**. This allows you to control the applications users are permitted to run by defining rules in Workspace Environment Management. This functionality is similar to Windows AppLocker but gives you the additional ability to:

- define rules without immediately assigning them
- bulk-assign rules to users
- import rules from Windows AppLocker

For more information, see Security.

Workspace Environment Management SDK PowerShell Modules

PowerShell modules are released as the first part of a Workspace Environment Management SDK. The modules are installed by the infrastructure services installation process. You can perform the following administrative tasks by running the cmdlets in the modules directly from the PowerShell console, or from PowerShell scripts:

- create a Workspace Environment Management database
- update a Workspace Environment Management database
- get the configuration from a local or remote infrastructure server
- set the configuration of a local or remote infrastructure server

For more information, see the Citrix Developer Documentation.

Support for SQL Server Always On availability groups

Workspace Environment Management has been tested with SQL Server Always On availability groups, and is now certified for use on that technology. For more information and advice, see System requirements.

Process optimization

History now user-centric. Workspace Environment Management (WEM) intelligent optimization relies on WEM "remembering" how many times a process infringes rules configured in the administration console. Based on this "memory," WEM optimizes (or not) the process when it is next started.

In previous releases, this "memory" was based only on process name. In other words, if a process infringed a rule when it was running as User A, it was also considered to be infringing for all users connecting to the agent, and the process was optimized globally for all users.

Starting in this release, the intelligent optimization "memory" is based on both process name and user details. This means that intelligent optimization is now user-centric. In other words, if a process infringes a rule when it was running as User A, but does not infringe a rule when it was running as User B, the process is optimized only when running as User A.

History now in local database. Workspace Environment Management (WEM) has two local databases: one contains the agent local cache, and another stores local data. Historically, WEM's intelligent optimization memory was stored either in the agent registry or in an XML file. An XML file was used if the custom argument **UseNonPersistentCompliantHistory** was set during agent installation.

From this release, WEM's intelligent optimization memory is stored in the agent local database (LocalAgentDatabase) located in the agent installation folder.

AgentServiceUseNonPersistentCompliantHistory custom argument for agent installation

The **Citrix Workspace Environment Management Agent Setup** executable no longer acknowledges the **AgentServiceUseNonPersistentCompliantHistory** custom argument. This custom argument previously allowed you to save agent service process optimization history to an XML file. The optimization history is now stored in the agent local database (LocalAgentDatabase) located in the agent installation folder.

User interface

The following changes are made to the administration console user interface:

- A new **Application Security** pane is added to the **Security** tab.

Documentation

Workspace Environment Management documentation is updated to reflect current product behavior.

Workspace Environment Management SDK documentation is added to the Citrix Developer Documentation.

What's new in Workspace Environment Management 4.4

Data analytics

From this release, the Workspace Environment Management infrastructure service sends anonymous usage data to Google Analytics. For more information, and for opt-out instructions, see Infrastructure services.

Profile Management

From this release, Workspace Environment Management supports Citrix Profile Management 7.15. The following new options are now available in the administration console:

- **Enable Logon Exclusion Check** (option for controlling file system exclusions)
- **Enable Profile Streaming Exclusion List - Directories** (option for controlling user profile streaming)

Database maintenance

In the Infrastructure Services Configuration utility, the **Database Maintenance** tab has a new option **Agent registrations retention period**. This allows agent registration logs to be deleted after a set time, which reduces the size of the database. It also reduces lag in populating the Registrations tab in the administration console.

User interface

The following changes are made to the administration console user interface:

- A new **Security** tab is introduced to contain settings controlling end-user activity.
- The **Process Management** controls have been moved to the new Security tab.

Documentation

At this release, Workspace Environment Management documentation is updated to reflect current product behavior. The documentation has also been remodeled as a single "versionless" documentation set describing the "current release." This approach reduces duplication in the online documentation set, gives more focused search results, and is better suited to agile release processes. Associated changes include:

- A top level "current release" article contains links to previous documentation sets in PDF format only. (HTML documentation for previous releases is no longer provided.)
- "What's new" summarizes the new functionality at the current release, and in previous releases.
- A new "Reference" section gathers reference information in one location. Port information previously in the introductory article is relocated to "Reference."

What's new in Workspace Environment Management 4.3

Site management

In previous releases, site settings were stored on the agent side and it was possible to change them from the agent GPO. Workspace Environment Management 4.3 introduces a different approach to site management which improves product security. Sites are now assigned to machines (or Security Groups or OUs) by the infrastructure service (broker) using a new Machines page in the administration console. A new Registrations tab under Administration>Agents in the administration console indicates machines which are bound incorrectly to multiple sites, so that you can take the appropriate action to remove the duplicate binding.

From this release, Workspace Environment Management "sites" are referred to as "configuration sets" in the user interface and documentation.

Agent localization improvements

The session agent user interface is now localized for the following languages: German, Spanish, French, Italian, Japanese, Korean, Dutch, Russian, Traditional and Simplified Chinese.

User interface improvements

Various text labels and messages in the installation wizards, administration console, and GPO templates have been rationalized and made mutually consistent to improve the user experience. For example, fields used to enter the same parameters in different installation wizards now use the same labels. Current and changed terminology is described in a new glossary.

Documentation

Workspace Environment Management 4.3 documentation is updated to reflect current product behavior. Various minor improvements have also been made, including the following improvements designed to assist users:

- A number of installation field descriptions have been revised to better explain their purpose.
- The documentation uses new standardized terminology visible in the installation wizards, GPO templates, and in the administration console. For example, the term "broker" is replaced by "infrastructure service".
- A glossary has been added to explain the new terminology seen in the installation wizards, the administration console, and the documentation. Changed terms are also indicated.
- The technical overview diagram is updated.
- A new port information table has been added to summarize port usage.

What's new in Workspace Environment Management 4.2

Profile Management

Workspace Environment Management 4.2 now supports all versions of Profile Management up to v5.6. New options are now provided in the Citrix Profile Management Settings pages in the Administration Console.

Documentation

Workspace Environment Management 4.2 documentation is now provided in HTML format in docs.citrix.com. Articles can be downloaded as PDF as required. Advice on load balancing has been added to the section Install infrastructure services.

What's new in Workspace Environment Management 4.1

Transformer module re-enabled

The Transformer module is available in the Administration Console. Transformer allows you to configure your physical machines to operate a locked-down thin client version of Windows.

Agent Host enhancements

Improvements to the Agent Host remove the communication between the WEM Broker Service and Agent Host executable. All communication now occurs between the WEM Broker Service and Agent Host Service, which then passes its instructions down to the Agent Host executable. This includes local cache access.

Documentation on docs.citrix.com

Workspace Environment Management 4.1 documentation is now available from docs.citrix.com. These PDFs are no longer included in the download. Filter conditions are now documented in the Administration Guide.

Fixed issues

April 3, 2019

Fixed in Workspace Environment Management 1903

The following issues have been fixed in the current release:

- With language packs installed, options in the Start menu > User Account menu might not appear in the language you selected. [WEM-1176, LC8811]
- You might find that the Norskale Broker Service.exe consumes more than 2GB of RAM several days after you perform frequent Active Directory (AD) operations (for example, specify users, computers, groups, and organizational units). The issue occurs when you have a very large AD

because the garbage collection mechanism cannot automatically release the RAM consumed by the System.Threading.Tasks namespace objects that the Norskale Broker Service.exe uses. [WEM-3251, LD1195]

Fixed in previous releases

Fixed in Workspace Environment Management 1811

The following issues have been fixed in the current release:

- 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]
- Attempts to upgrade the WEM database using the command line might fail. [WEM-1410]
- After you apply a percentage of the CPU’s processing power for a process on the **System Optimization** > **CPU Management** > **CPU Clamping** tab of the administration console for the first time and configure a different percentage for the same process later, the change does not take effect. [WEM-1993, LD0110]
- When the Citrix WEM agent starts, a Citrix WEM Agent Init file (.log) and a Citrix WEM Agent file (.log) are created separately in the root of the current user’s Users folder. However, while WEM agent switches from the Citrix WEM Agent Init file to the Citrix WEM Agent file, some logs might be missing. [WEM-2233]
- When a forest (current or trusted) contains a large number of OUs (for example, 10,000), if you click **Add OU** from the administration console, you might find some OUs to be missing from the **Organizational Units** window. This issue occurs because the search task times out before the search completes. [WEM-2378, LD0428]
- The **Workspace Environment Management** node has been moved from **Computer Configuration** > **Policies** > **Administrative Templates** > **Citrix** to **Computer Configuration** > **Policies** > **Administrative Templates** > **Citrix Components**. [WEM-2582]

Fixed in Workspace Environment Management 1808

- The Workspace Environment Management Agent Host screen capture feature allows end users to take screenshots of error messages in their environment. They can then send the screenshots to the administrator via Microsoft Outlook for support. However, when end users click the **Send to Support** button, the following error message appears: “Error encountered while sending email.” [WEM-1123]

- Application Security features are not available if the Workspace Environment Management administration console is installed on Windows 7 SP1 or Windows Server 2008 R2 SP1 (or earlier versions). In the Security tab, none of the Application Security options can be selected. [WEM-1216, LC9023]
- When the number of connected agents exceeds a certain threshold (for example, 5,000), if you frequently specify users, computers, groups, and organizational units, you might find that the Norskale Broker Service.exe consumes more than 2GB of RAM several days later. The issue occurs because some Microsoft LDAP APIs used by Norskale Broker Service.exe are unable to release the consumed RAM automatically. [WEM-1494, LC9623]
- When a forest (current or trusted) contains more than 1,000 OUs, if you click **Add OU** from the administration console, you might find some OUs to be missing from the **Organizational Units** window. The issues occurs because `LDAP API FindAll()` returns no more than 1,000 results by default. [WEM-1986, LD0121]
- After you upgrade the WEM agent to Version 4.7, if you select **Enable Intelligent CPU Optimization** and/or **Enable Intelligent I/O Optimization** on the **System Optimization > CPU Management > CPU Management Settings** tab of the administration console, error messages about Error 87 frequently appear in Windows Event logs. This issue does not affect the user experience, thus you can dismiss these error messages. [WEM-2051]

Fixed in Workspace Environment Management 4.7

- You can use the Citrix Workspace Environment Management Infrastructure Services Setup.exe to install the Citrix Workspace Environment Management SDK without installing the infrastructure service (by selecting “Custom” installation type and deselecting “Default feature”). However, if you leave the option “Start the Database Management Utility” selected then click “Finish,” an error message about Error 2753 is displayed. You can click OK to dismiss this error dialog, which is benign. [WEM-541]
- When you are configuring the Workspace Environment Management database, if you use incorrect settings the system may become unresponsive for up to six minutes. The system then displays an error message reporting “A network-related or instance-specific error occurred while establishing a connection to SQL Server. Examples of incorrect settings include incorrect SQL user name and password or invalid database instance. This happens because Workspace Environment Management makes multiple database connection retries with the incorrect settings. [WEM-790]
- In the administration console Active Directory Objects section Machines tab, when you click **Add OU**, the Organization Units dialog does not list all the items it should. There are two scenarios to be aware of:

  - When the infrastructure server and administration console are not installed on the parent domain (for example, they are installed on the tree-domain or on a sub-domain), none of the Active Directory structure or OUs (forests, domains, sub-domains, and so on) outside the current forest are shown.
  - When the infrastructure server and administration console are installed on the parent domain, only the parent domain OU is shown. The OUs of sub-domains and tree-domains in different forests are not shown.

  To add machines which are in a different forest, in the Machines tab, click **Add Object** and select the other forest. [WEM-1069]

- When end-users access applications via Workspace Environment Management, the CPU usage of NorSkale Agent Host service.exe increases to 20% and remains there for 5 to 60 seconds, thus affecting the user experience. [WEM-1094, LC9230]

- WEM agents are randomly reported with the following different status under **Administration > Agents > Registrations**: "Agent <AgentHostName> is bound to multiple configuration sets." "Agent <AgentHostName> is not be bound to any Configuration Set." This issue occurs only when using OUs as AD objects in Configuration Sets. It prevents agents registering successfully with infrastructure servers. [WEM-1302, LC9524]

- The Workspace Environment Management administration console **Administration > Agents** tab reports the Netscaler Subnet IP address instead of the agent IP address. This prevents the agent cache being refreshed because the Agents tab times out. [WEM-1406, LC9645]

- When users log on, the Workspace Environment Management session agent reports "processing applications…", but this never completes. This occurs only when customer assigns multiple applications to the agent and enables multi-functions. [WEM-1740, LC8601]

- Attempting to add an application of type URL in the Workspace Environment Management administration console fails. The event and broker logs show "AdminBrokerService.CreateVuemApp():Cannot insert the value NULL into column 'WorkingDirectory', table 'CitrixWEM.dbo.VUEMApps'; column does not allow nulls. INSERT fails." [WEM-1741, LC9551]

Fixed in Workspace Environment Management 4.6

- When you uninstall the Workspace Environment Management agent, the uninstall process does not delete the Windows Firewall inbound rule "Norskale agent in". Manually delete this rule in the Windows Firewall with Advanced Security dialog. [WEM-312]
- When the option "Launch Agent at Reconnect" is selected, the Workspace Environment Management agent executable does not run when reconnecting with published desktops on agent hosts which are running Windows desktop operating systems, via ICA. (RDP sessions are unaffected.) [WEM-322, LC8816]

- If you attempt to add an agent host machine to a configuration set when the agent host machine is in a different forest to the infrastructure service, it can take several minutes before the agent host is added, depending on the actual AD topology involved. During this time, the administration console displays the message "Please Wait loading…" and further activities are not possible. [WEM-358]
- Attempts to create or update a WEM database, on an SQL Server instance which uses case-sensitive collation, fails. Ensure that the SQL Server instance uses *case-insensitive *collation before attempting to create or update a WEM database. [WEM-540]
- The Workspace Environment Management agent randomly crashes after VDAs are upgraded to XenApp and XenDesktop 7.16. [WEM-937, LC8926]
- In the Workspace Environment Management administration console Citrix Profile Management Settings, the Synchronization tab option "Enable File Mirroring" does not match the Citrix Studio Profile Management policy setting it is derived from. The option should read "Enable File Synchronization" and allow files to be added. [WEM-971, LC9090]
- When you are adding an Application Security executable rule of type "Publisher", dragging the Publisher info slider to "File name" or above causes an exception in the Workspace Environment Management administration console. [WEM-1199, LC9255]
- On laptop machines in transformer mode, the Transformer battery icon does not stay synchronized with the battery percent reported by the OS. When the power cable is connected or disconnected, the transformer battery icon is refreshed with the correct percentage value, but it then continues to show the same fixed value until the next power cable change is detected. [LC9261]
- The WEM agent installs VUEMRSAV.exe (Workspace Environment Management Resultant Actions Viewer), a utility which allows users to view the WEM configuration defined for them by the administrator. If an administrator assigns an action directly to a specific user, when that user runs VUEMRSAV.exe, the assigned action is missing in the Applied Actions tab. If an administrator assigns an action to a User Group to which the user belongs (for example, 'Domain Users'), when that user runs VUEMRSAV.exe, the assigned action is visible in the Applied Actions tab, which is the correct behavior. [WEM-1200]

Fixed in Workspace Environment Management 4.5

- When you examine the properties of rules in the Microsoft Security Policy Editor (secpol.msc), script rules set to "Audit" mode in the Workspace Environment Management Security tab are incorrectly shown as not configured. (PowerShell can be used to confirm that these rules are actually in audit mode.) [WEM-352]
- In the WEM Infrastructure Server Configuration wizard Advanced tab, if you select the option **Use cache even if online**, it is not saved when you close the wizard. A workaround is to set the registry key BrokerUseCacheEvenIfOnline = 1 in HKLM\System\CurrentControlSet\Control\Norskale\Infrastru Services. [WEM-396]

- While in the Security Tab and switching between Configuration Sets, the side panel may incorrectly display its state, either enabled/disabled. Switching to another tab and back resolves this issue. [WEM-405]
- When you select multiple rules and click Edit, any changes to rule assignments you make are applied to all users and user groups you select. In other words, both new and existing rule assignments are merged across those rules. If you do not change rule assignments, existing rule assignments are unchanged. To fine-tune rule assignments, select one rule at a time and click Edit. [WEM-420]
- When you select multiple rules and then use Edit, the Permissions option defaults to "Allow," even if some or all the selected rules are set to deny. In the rule list, permissions are correctly reported in the Action column. [WEM-421]

Fixed in Workspace Environment Management 4.4

- If you run the Workspace Environment Management administration console as a standard Windows user, and you attempt to start the **Modeling Wizard**, the wizard does not start. [WEM-187]
- When you attempt to add a user group, which is in a different AD domain to the infrastructure server, as a processed group in the Citrix User Profile Management tab in the administration console, the exception *IndexOutOfRangeException is raised, and the group is not processed. [WEM-210]
- Links in "This PC" in Windows 10 do not reflect folder redirection, and still point to local folders. [WEM-234]
- The Agent Host waits about 5 minutes before starting if Workspace Environment Management is installed on Windows version 8, or Server 2012, and a language pack is installed. [WEM-244]
- If you launch or refresh a UI session agent when it is not bound to a configuration set, keyboard and mouse locks which are active during the agent refresh are not released. [WEM-321]
- If you attempt to add an agent host machine to a configuration set when the agent host machine is in a different domain to the infrastructure service, the machine is not added in the administration console Active Directory Objects tab. This happens regardless of the actual AD topology involved (parent/child domains, multi-forest setups, one- or two-way trust relationships, and so on). [WEM-326, WEM-299]

Fixed in Workspace Environment Management 4.3

- When the Workspace Environment Management session agent is running in command line mode, User Statistics data is not reported to the WEM infrastructure services. [WEM-41]

- The Workspace Environment Management session agent interface does not render correctly when a computer display is extended to external displays connected via a dock. This problem, which occurs when extending to multiple displays with different screen resolution settings, results in a portion of the right-hand side of the display not rendering completely. This prevents users seeing the home button or being able to change other native Workspace Environment Management settings. [WEM-90]
- The Workspace Environment Management session agent causes the mouse to stop working on virtual machines which have the System Center Configuration Manager (SCCM) client installed with Power Management enabled. [WEM-115]
- When you are using the Transformer feature, the session agent generates an unhandled exception if Wi-Fi is turned off using "ms-settings:network-wifi." [WEM-133]
- The Workspace Environment Management session agent causes the mouse to stop working on virtual machines after an interruption to network access is restored. [WEM-159]

Fixed in Workspace Environment Management 4.2

- File Association actions cannot be processed by the Agent Host on Windows 8, 8.1, Server 2012, Server 2012 R2, and Server 2016 due to registry access issues. [WEM-15]
- The Agent Host waits about 5 minutes before starting if Workspace Environment Management is installed on Windows version 8, 8.1, 10, Server 2012, Server 2012 R2, or Server 2016 (all branches and builds) and a language pack is installed. [WEM-17]

Known issues

April 3, 2019

Workspace Environment Management 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]
- When you use a configuration object with Workspace Environment Management PowerShell modules SDK cmdlets, all parameters must be specified. If they are not, the command fails with an InvalidOperation error. [WEM-691, WEM-693]
- In PowerShell, when you use the **help** command with the **-ShowWindow** switch to display help in a floating window for a Workspace Environment Management PowerShell cmdlet, the Exam-

ples section of the help is unpopulated. To see the examples, use the **get-help** command with the **-examples**, **-detailed**, or **-full** switch instead. [WEM-694]

- 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]
- When you enable the process launcher on the **Administration Console** > **Transformer Settings** > **Advanced** > **Process Launcher** tab to launch a Windows built-in application (for example, calc.exe) as entered in the process command line field, the agent host might keep opening the application after you refresh Citrix WEM Agent. [WEM-3262]
- After WEM upgrades to the latest version, if you still use 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 with an .exe extension using a file path condition, the rule does not work. This issue occurs because WEM converts the path for that file incorrectly. For example, suppose you browse to the .exe file in C:\ProgramData folder. Instead of converting the file path to %OSDRIVE%\ProgramData<filename>, WEM converts it to %SYSTEMDRIVE%\ProgramData<filename>. [WEM-3581]
- 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]
- On the Security tab of the administration console, if you attempt to create an AppLocker rule for a file with a .bat extension, WEM fails to display the .bat file in the **Open** window after you browse to the folder where the .bat file is located. [WEM-3585]
- 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]
- Workspace Environment Management fails to convert a UNC path to a local path. The issue occurs when you use the **Administration Console > Actions > Applications > Application List**

tab to associate an icon located on the network with an application. [WEM-3977]

Third party notices

January 3, 2019

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

Workspace Environment Management Third Party Notices

Deprecation

February 28, 2019

The announcements in this article are intended to give you advanced notice of platforms and Workspace Environment Management features which are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. Announcements may change in subsequent releases and might not include every deprecated feature or functionality.

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

Deprecations and removals

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

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

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

Item	Announced in	Removed in	Alternative
Support for WEM infrastructure services on the following OS platforms: Windows Server 2008 R2 SP1, and Windows Server 2012.	4.7	**1808**	
Support for the WEM administration console on the following OS platforms: Windows Vista SP2 32-bit and 64-bit, Windows 7 SP1 32-bit and 64-bit, Windows 8.x 32-bit and 64-bit, Windows Server 2008 SP2, Windows Server 2008 R2 SP1, and Windows Server 2012.	4.7	**1808**	
Support for the WEM agent on the following OS platforms: Windows Vista SP2 32-bit and 64-bit, and Windows Server 2008 SP2.	4.7	**1808**	
In-place upgrade from WEM 3.0, 3.1, 3.5, 3.5.1 to WEM 4.x.*	4.5	Upgrade to WEM 3.5.2, then upgrade to WEM 4.x.	
Support for all WEM components on Windows XP SP3 32-bit and 64-bit.	4.5	4.5	Use a supported OS platform.

Item	Announced in	Removed in	Alternative
Support for WEM agent on the following OS platforms: Windows XP SP3 32-bit and 64-bit, Windows Server 2003 32-bit and 64-bit, Windows Server 2003 R2 32-bit and 64-bit	4.5	4.5	Use a supported OS platform.
Support for assigning and binding existing (pre-version 4.3) agents to sites via GPO.	4.3		Upgrade agents to Workspace Environment Management 4.3 or later.
Support for WEM administration console on the following OS platforms: Windows XP SP3 32-bit and 64-bit, Windows Server 2003 32-bit and 64-bit, Windows Server 2003 R2 32-bit and 64-bit	4.2	4.5	Use a supported OS platform.
Support for WEM administration console on the following OS platforms: Windows Vista SP1 32-bit and 64-bit, Windows Server 2008, Windows Server 2008 R2	4.2	4.5	

Item	Announced in	Removed in	Alternative
Support for all WEM components on Microsoft .NET Framework 4.0, 4.5.0, or 4.5.1.	4.2	4.5	Upgrade to Microsoft .NET Framework 4.5.2.

Quick start guide

February 26, 2019

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

Overview

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

Prerequisites

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

Installation and configuration

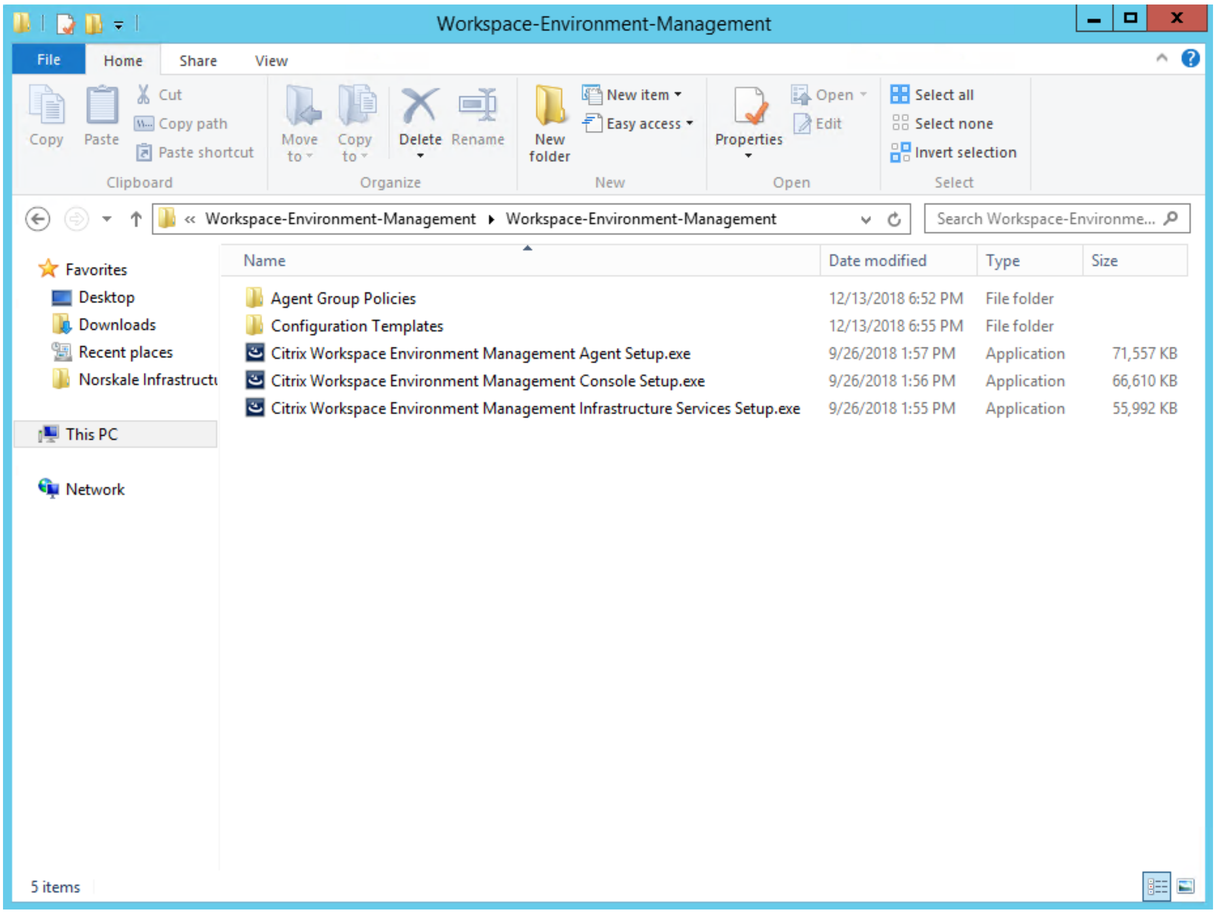
Citrix recommends that you install the latest version of WEM. Deploying WEM consists of installing and configuring three core components: Infrastructure services, Administration console, and Agent. The following procedures detail how to install and configure these components:

- Infrastructure services
- Administration console
- Agent

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

Step 1: Install the infrastructure services

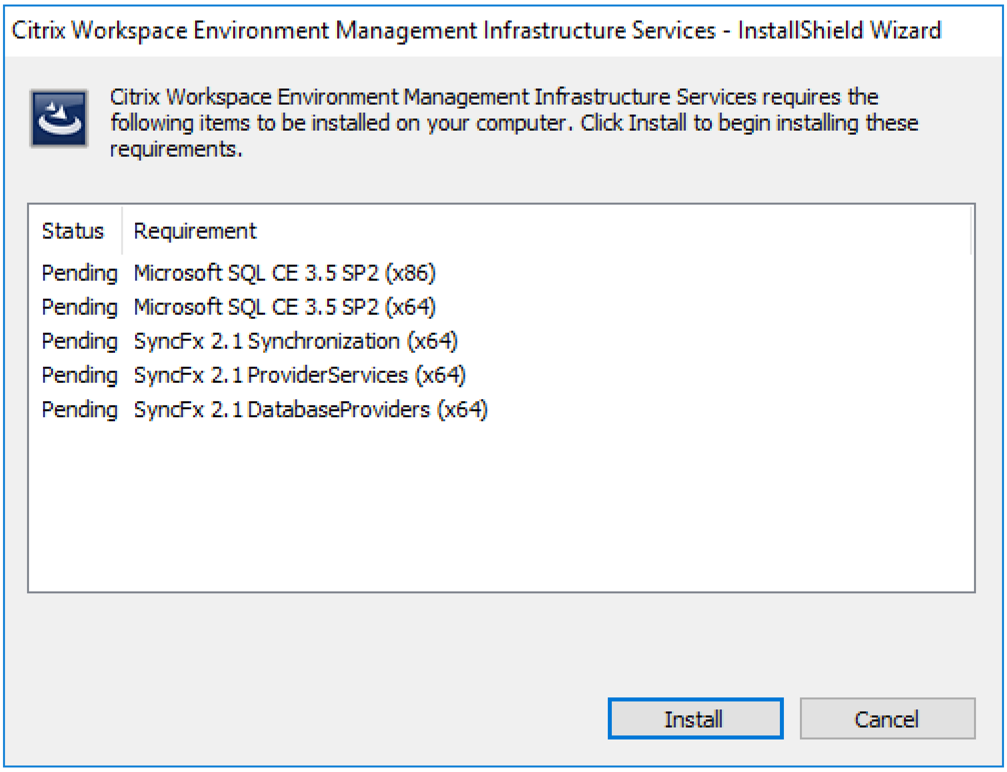
1. Download the latest WEM installer here. Extract the zip file to a convenient folder.



Name	Date modified	Type	Size
Agent Group Policies	12/13/2018 6:52 PM	File folder	
Configuration Templates	12/13/2018 6:55 PM	File folder	
Citrix Workspace Environment Management Agent Setup.exe	9/26/2018 1:57 PM	Application	71,557 KB
Citrix Workspace Environment Management Console Setup.exe	9/26/2018 1:56 PM	Application	66,610 KB
Citrix Workspace Environment Management Infrastructure Services Setup.exe	9/26/2018 1:55 PM	Application	55,992 KB

2. Run **Citrix Workspace Environment Management Infrastructure Services Setup.exe** on your infrastructure server.

3. Click **Install**.

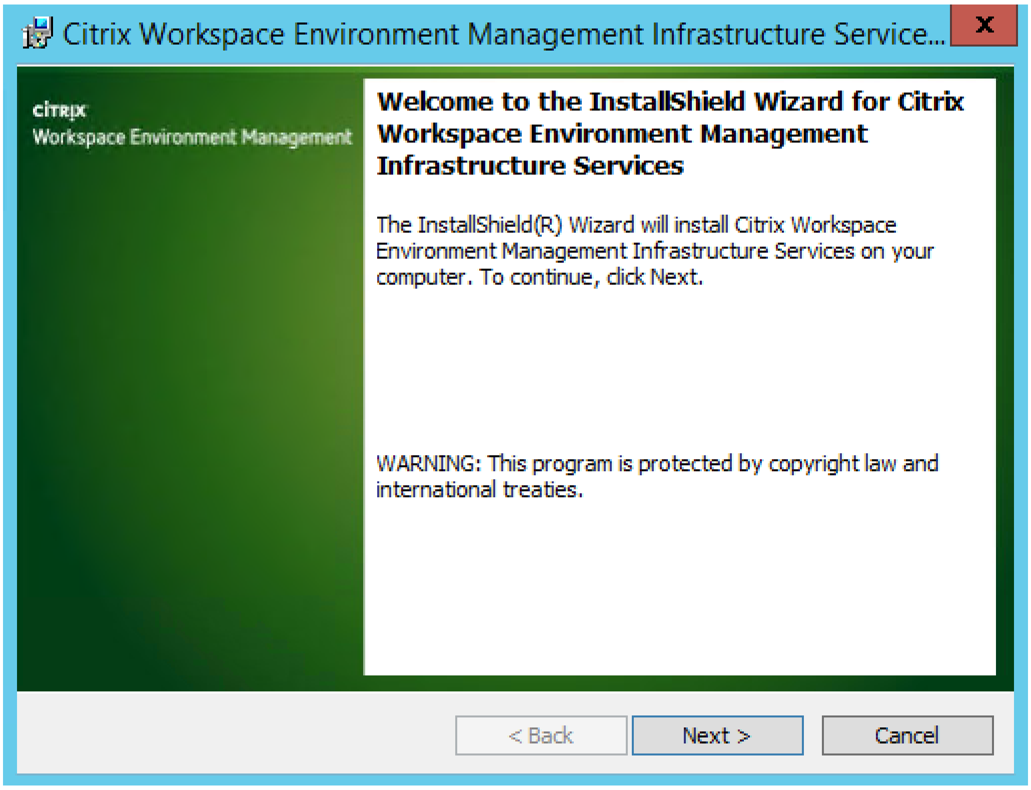


Citrix Workspace Environment Management Infrastructure Services - InstallShield Wizard

Citrix Workspace Environment Management Infrastructure Services requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	Microsoft SQL CE 3.5 SP2 (x86)
Pending	Microsoft SQL CE 3.5 SP2 (x64)
Pending	SyncFx 2.1 Synchronization (x64)
Pending	SyncFx 2.1 ProviderServices (x64)
Pending	SyncFx 2.1 DatabaseProviders (x64)

4. Click **Next**.



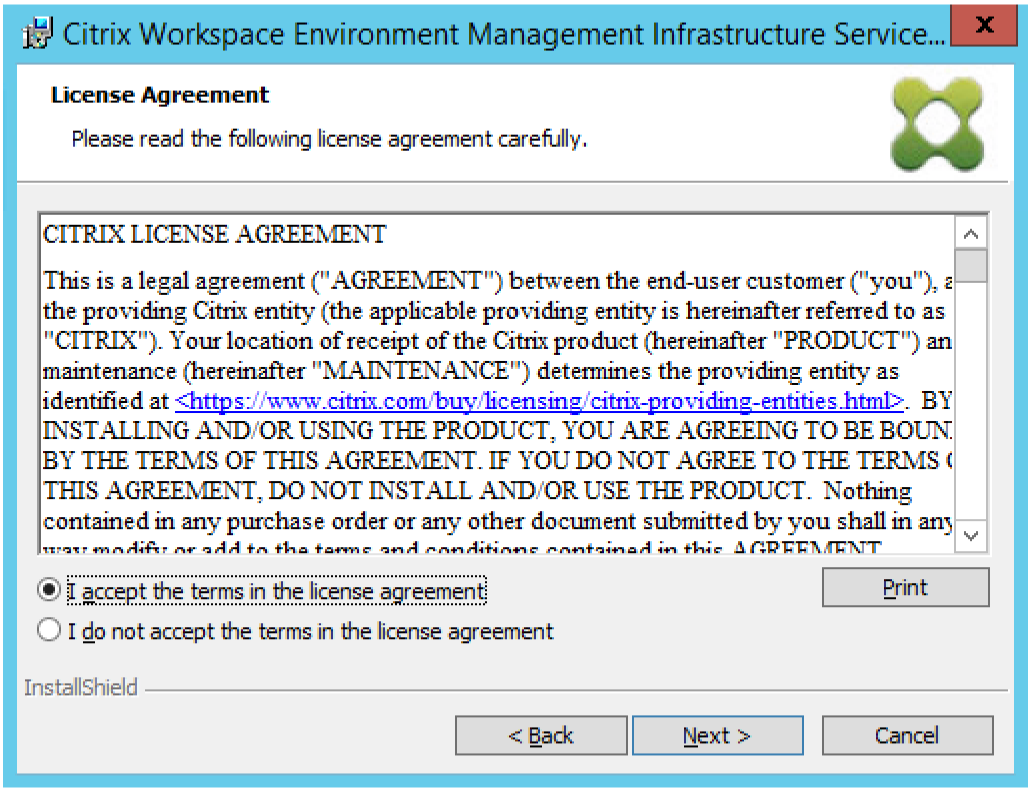
Citrix Workspace Environment Management Infrastructure Service...

Welcome to the InstallShield Wizard for Citrix Workspace Environment Management Infrastructure Services

The InstallShield(R) Wizard will install Citrix Workspace Environment Management Infrastructure Services on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

5. Select "I accept the terms in the license agreement" and then click **Next**.


Citrix Workspace Environment Management Infrastructure Service...

License Agreement

Please read the following license agreement carefully.

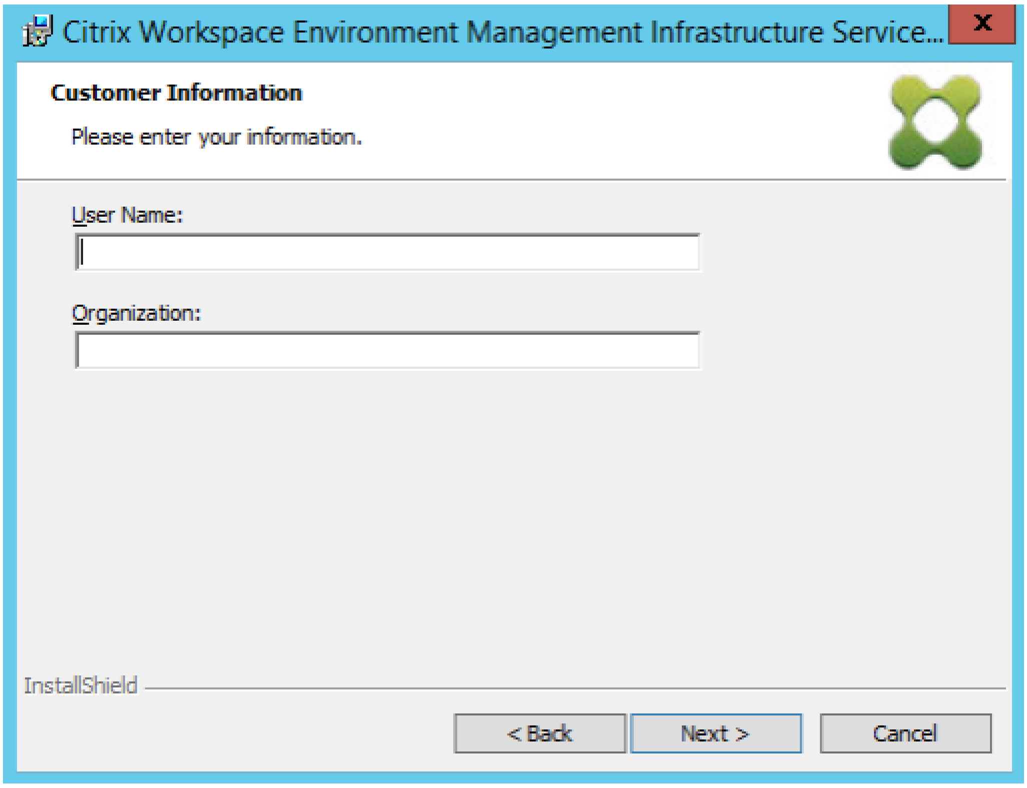
CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), a
the providing Citrix entity (the applicable providing entity is hereinafter referred to as
"CITRIX"). Your location of receipt of the Citrix product (hereinafter "PRODUCT") an
maintenance (hereinafter "MAINTENANCE") determines the providing entity as
identified at <https://www.citrix.com/buy/licensing/citrix-providing-entities.html>. BY
INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUN
BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS (
THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing
contained in any purchase order or any other document submitted by you shall in any
way modify or add to the terms and conditions contained in this AGREEMENT

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

6. Type your user name and organization and then click **Next**.


Citrix Workspace Environment Management Infrastructure Service...

Customer Information

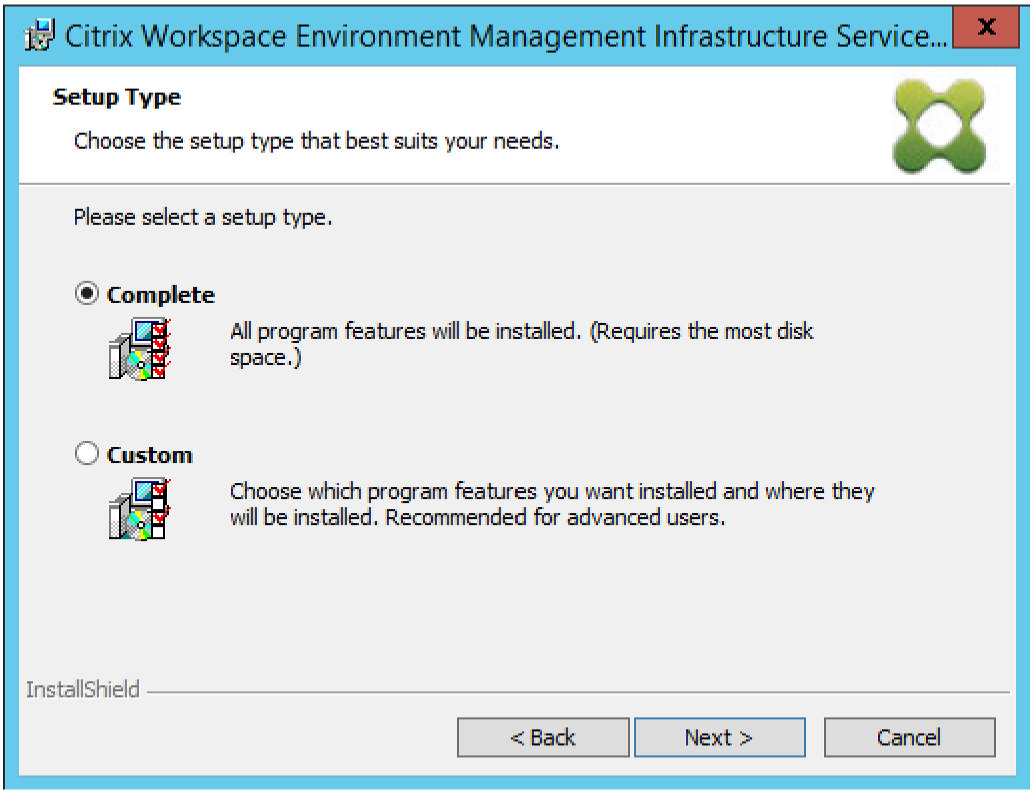
Please enter your information.

User Name:

Organization:

7. Select **Complete** and then click **Next**.

> **Note:**
>
> To change the installation folder, or to prevent SDK installation, select **Custom**.



Citrix Workspace Environment Management Infrastructure Service...

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

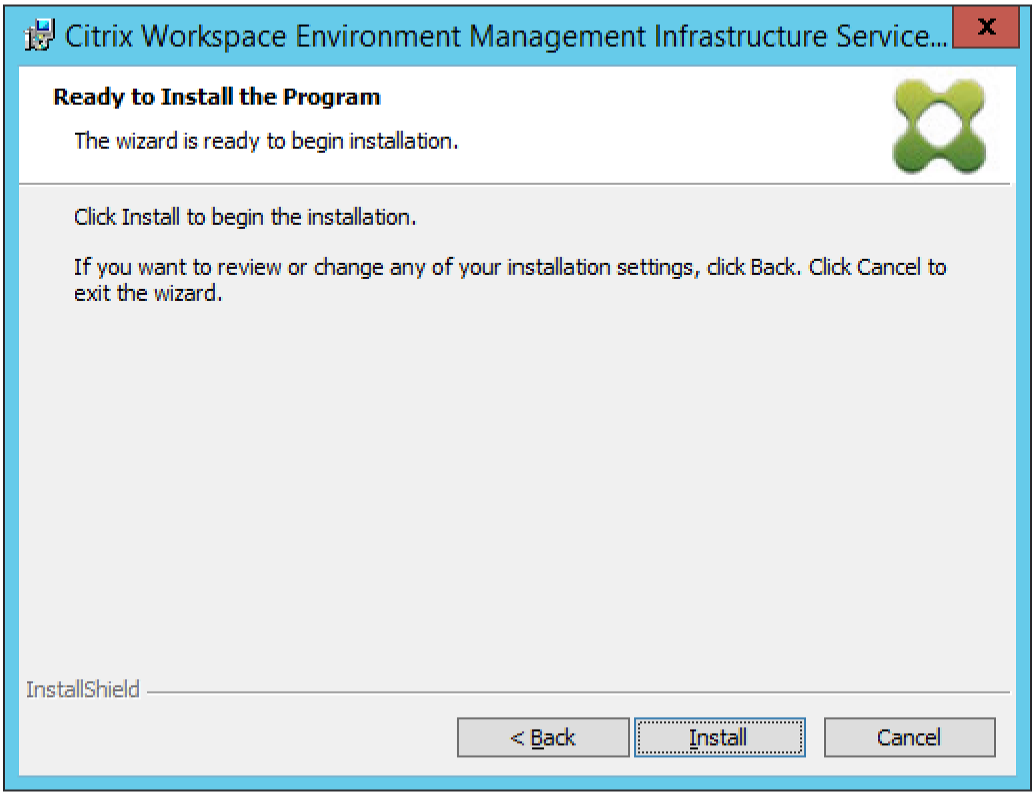
● **Complete**

All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

8. On the Ready to Install the Program page, click **Install**.



Citrix Workspace Environment Management Infrastructure Service...

Ready to Install the Program

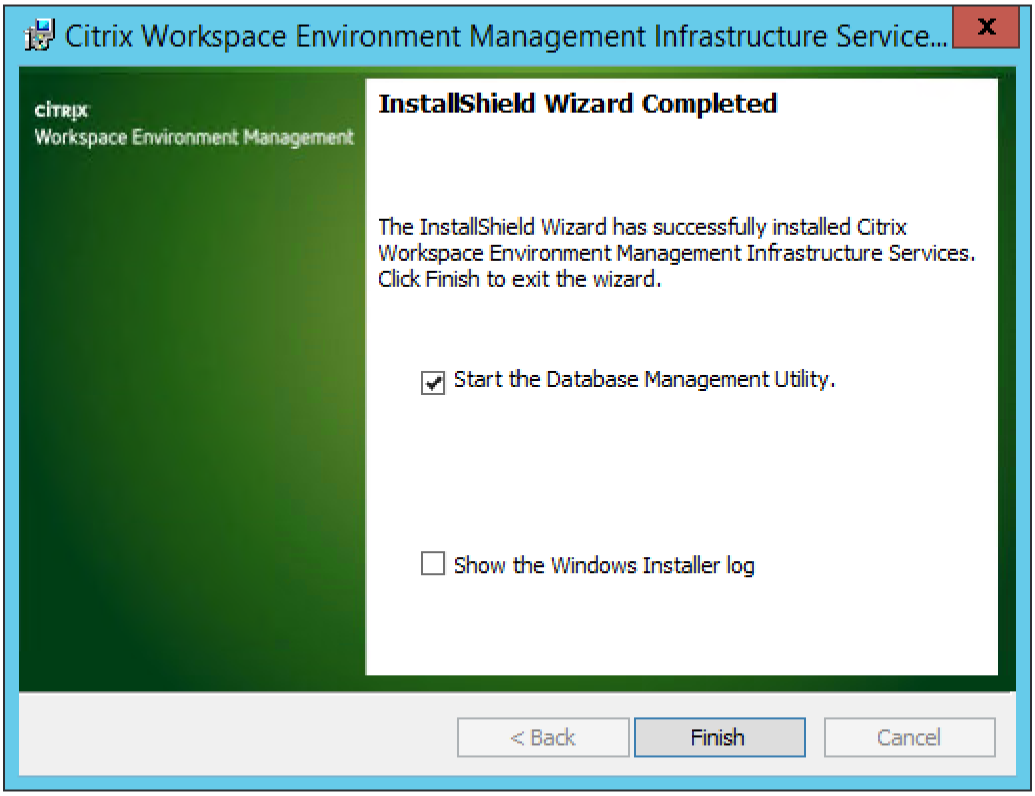
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

9. Click **Finish** and then go to Step 2.

> **Note:**
>
> By default, the **Start the Database Management Utility** option is selected, and the utility starts automatically. You can also start the utility from the **Start** menu at **Citrix** > **Workspace Environment Management** > **WEM Database Management Utility**.



Citrix Workspace Environment Management Infrastructure Service...

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Citrix Workspace Environment Management Infrastructure Services. Click Finish to exit the wizard.

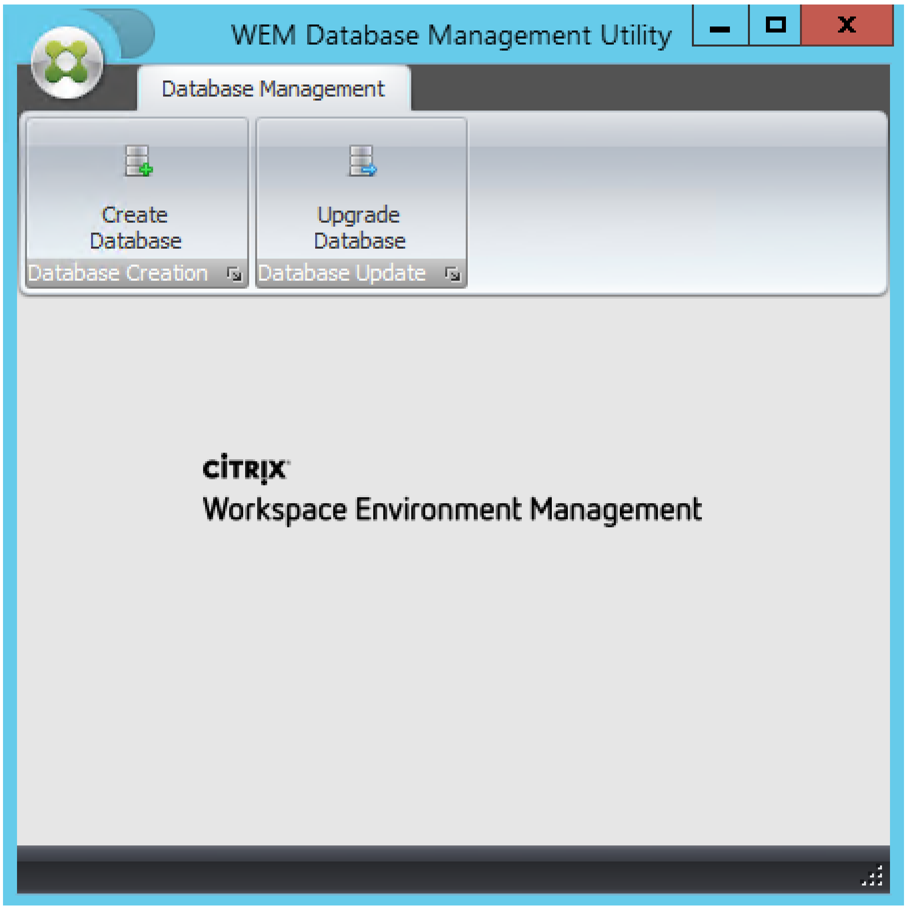
☑ Start the Database Management Utility.

□ Show the Windows Installer log

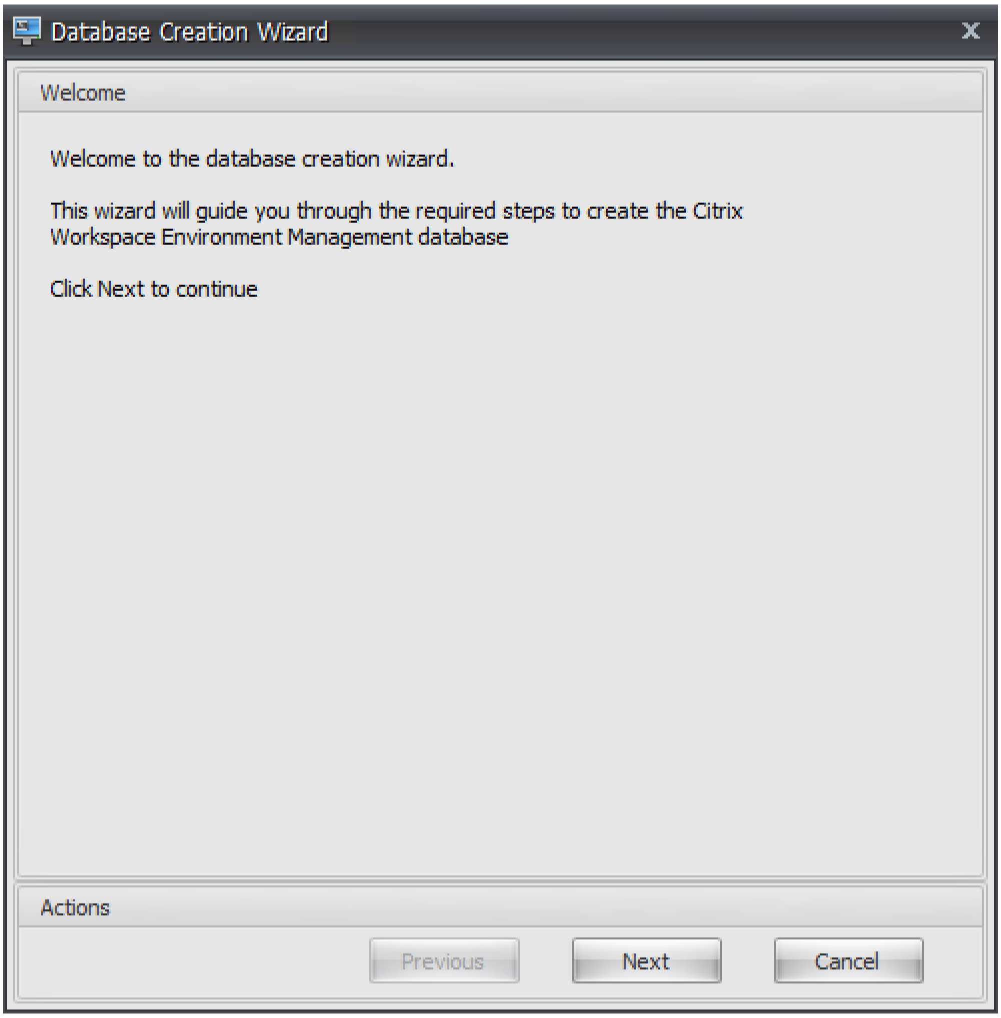
Step 2: Create a WEM database

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

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



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



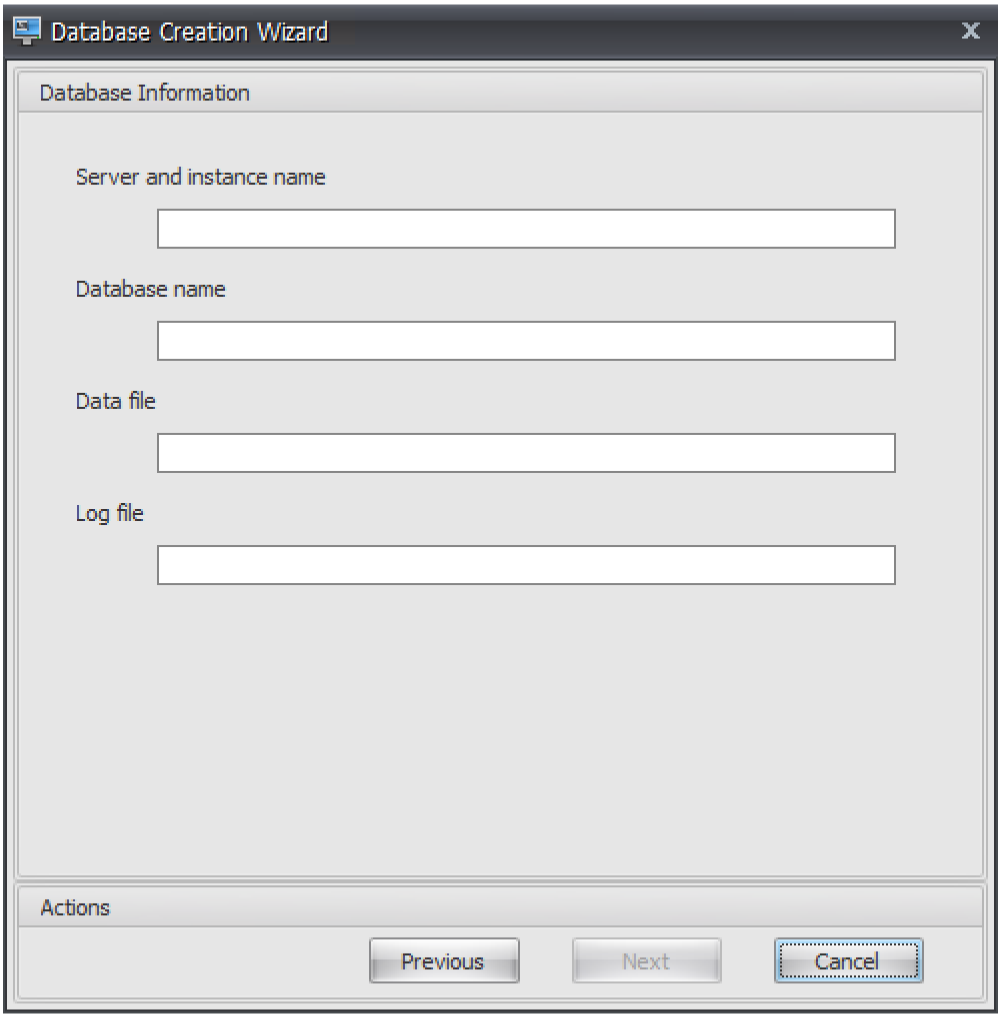
Welcome to the database creation wizard.

This wizard will guide you through the required steps to create the Citrix Workspace Environment Management database

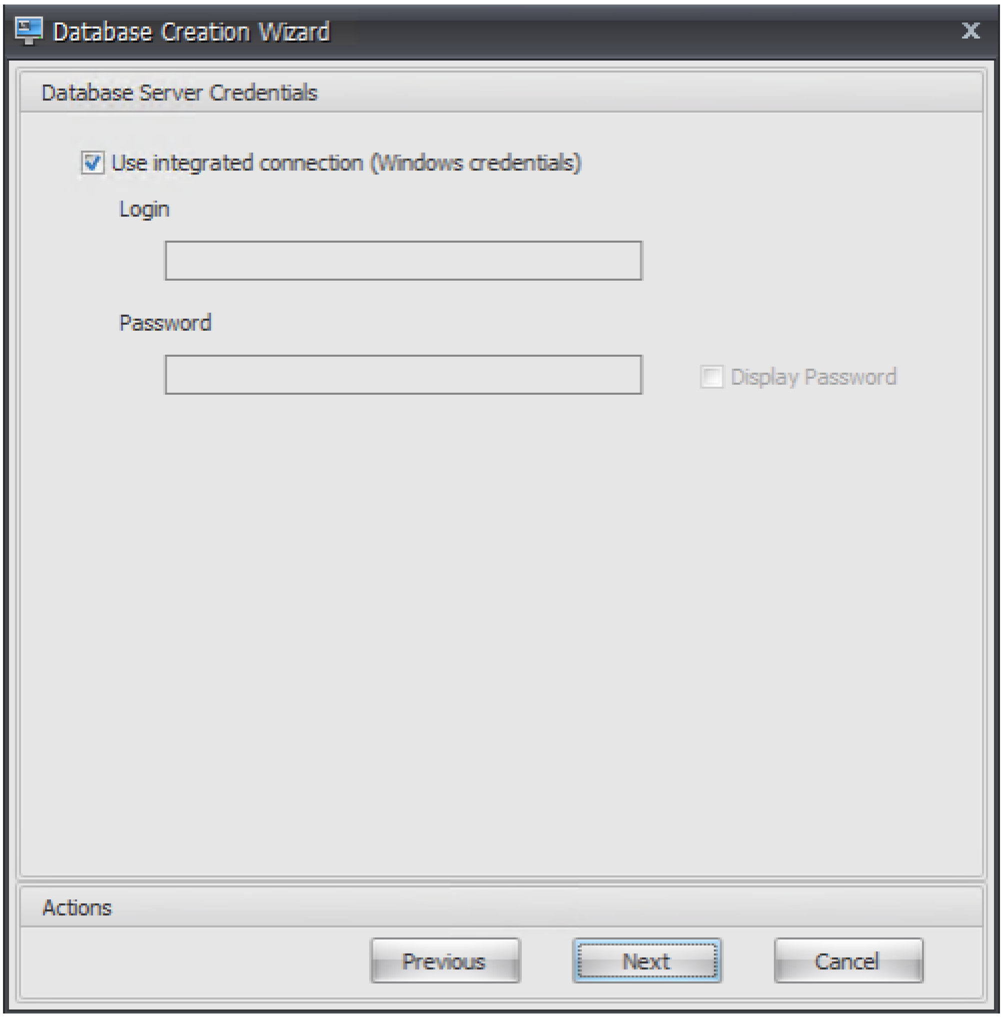
Click Next to continue

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

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



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



Database Creation Wizard

Database Server Credentials

☑ Use integrated connection (Windows credentials)

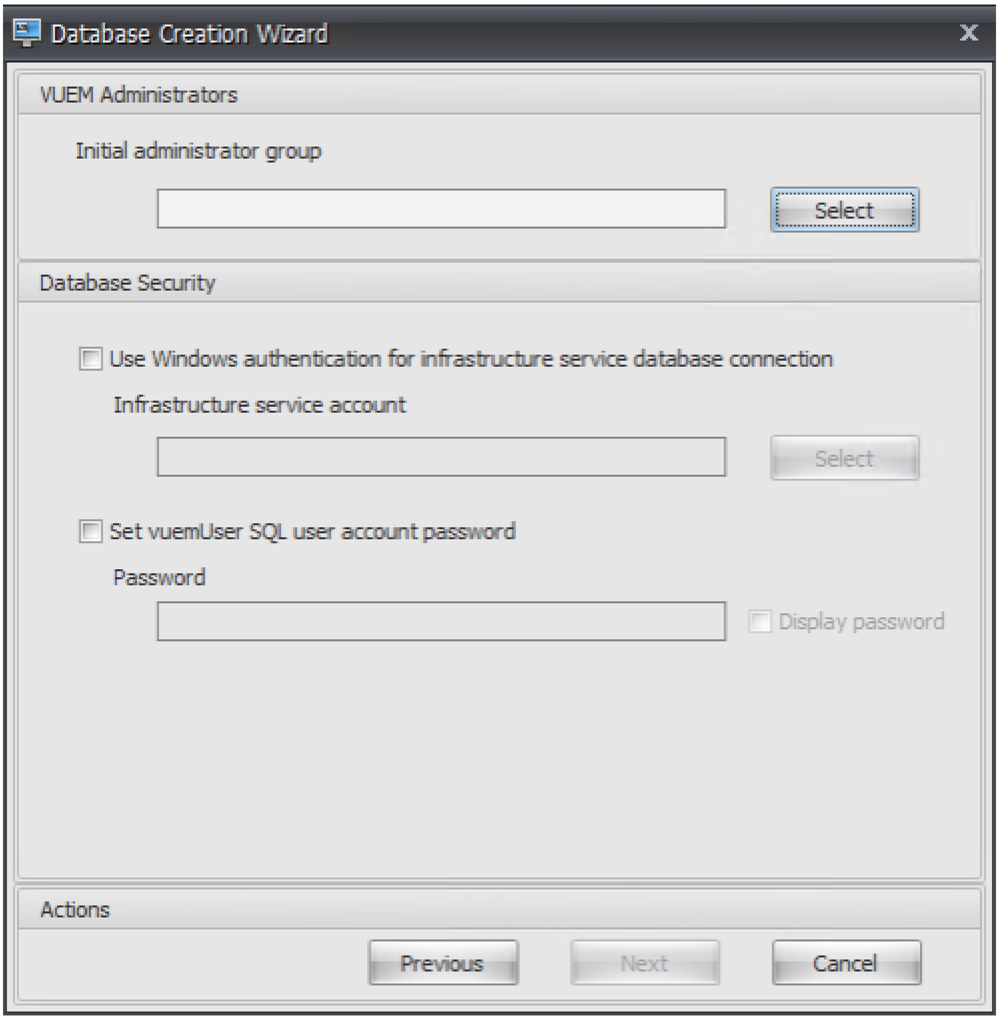
Login

Password

□ Display Password

Actions

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



Database Creation Wizard

VUEM Administrators

Initial administrator group

Database Security

□ Use Windows authentication for infrastructure service database connection

Infrastructure service account

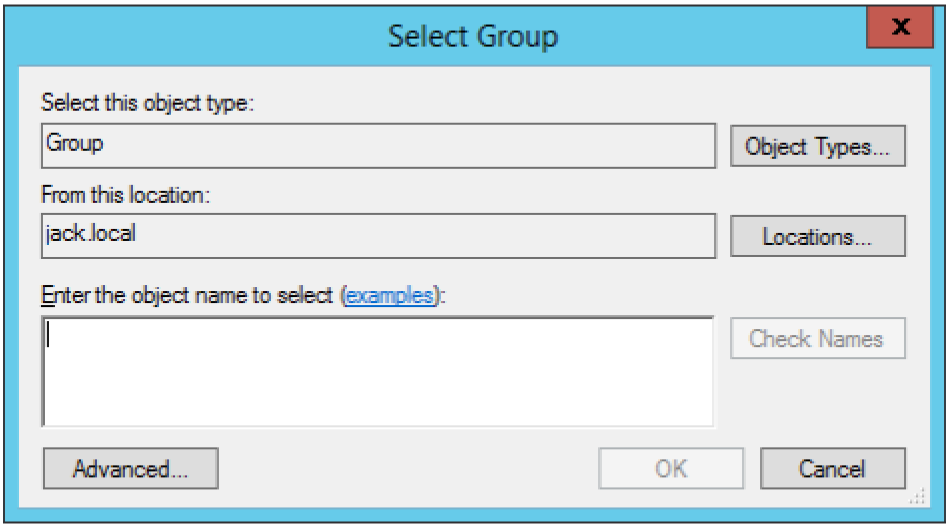
□ Set vuemUser SQL user account password

Password

□ Display password

Actions

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



Select Group

Select this object type:
Group

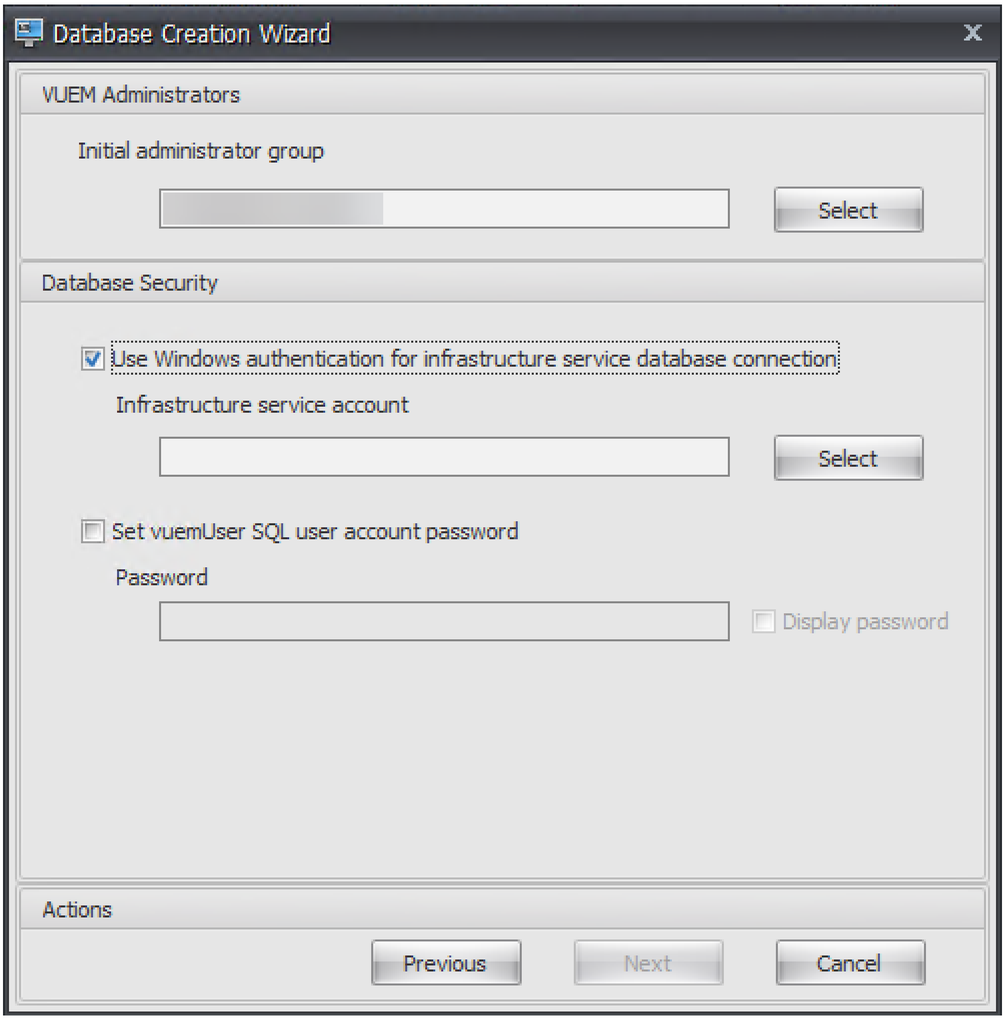
From this location:
jack.local

Enter the object name to select (examples):

7. Under Database Security, select **Use Windows authentication for infrastructure service**

database connection and then click **Select**.

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



Database Creation Wizard

VUEM Administrators

Initial administrator group

Database Security

☑ Use Windows authentication for infrastructure service database connection

Infrastructure service account

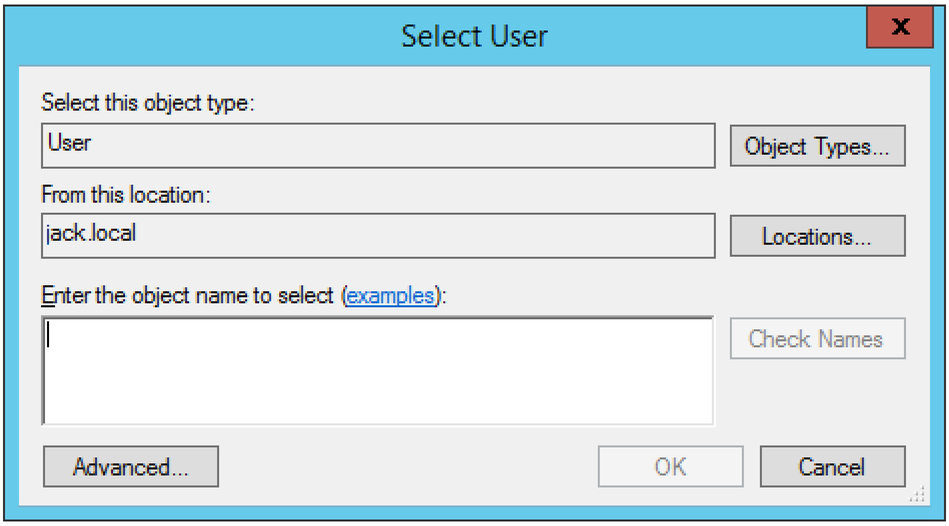
□ Set vuemUser SQL user account password

Password

□ Display password

Actions

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



Select User

Select this object type:

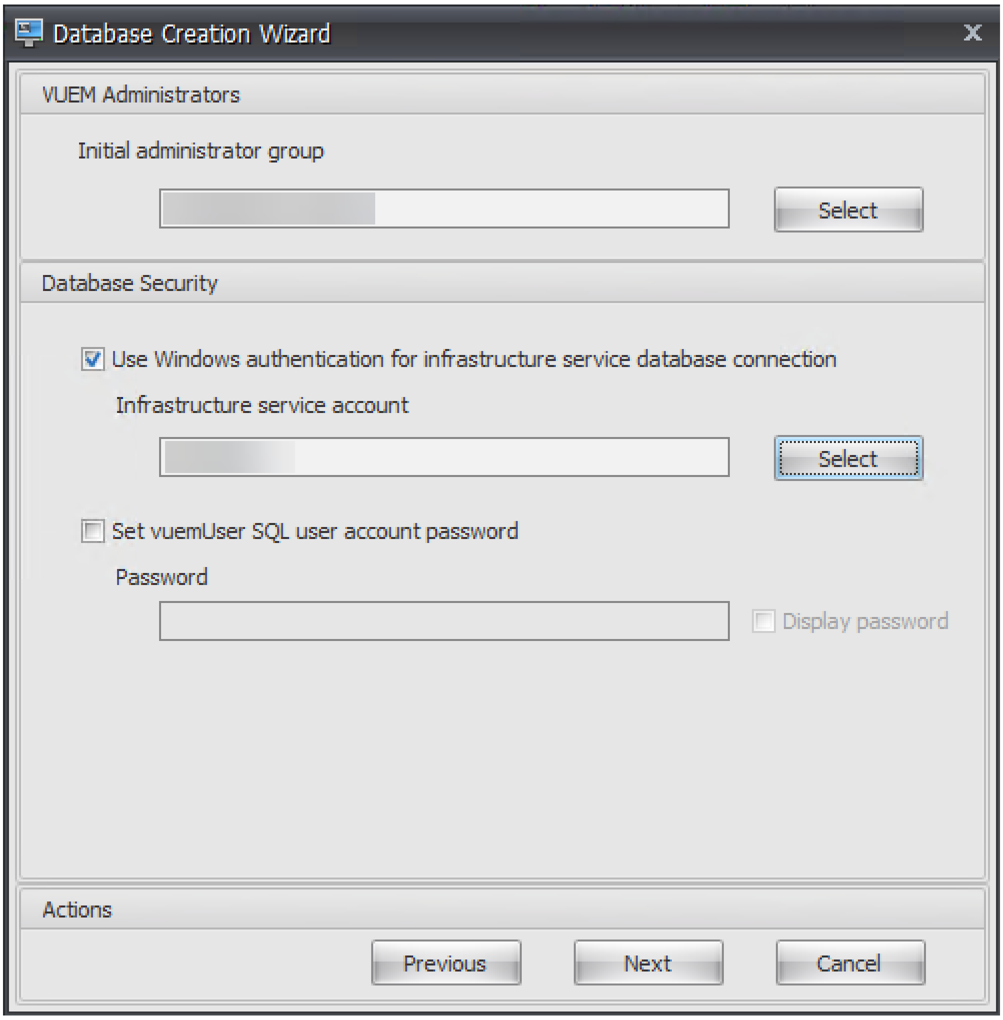
User

From this location:

jack.local

Enter the object name to select (examples):

9. Click **Next**.



Database Creation Wizard

VUEM Administrators

Initial administrator group

[redacted]

Database Security

☑ Use Windows authentication for infrastructure service database connection

Infrastructure service account

[redacted]

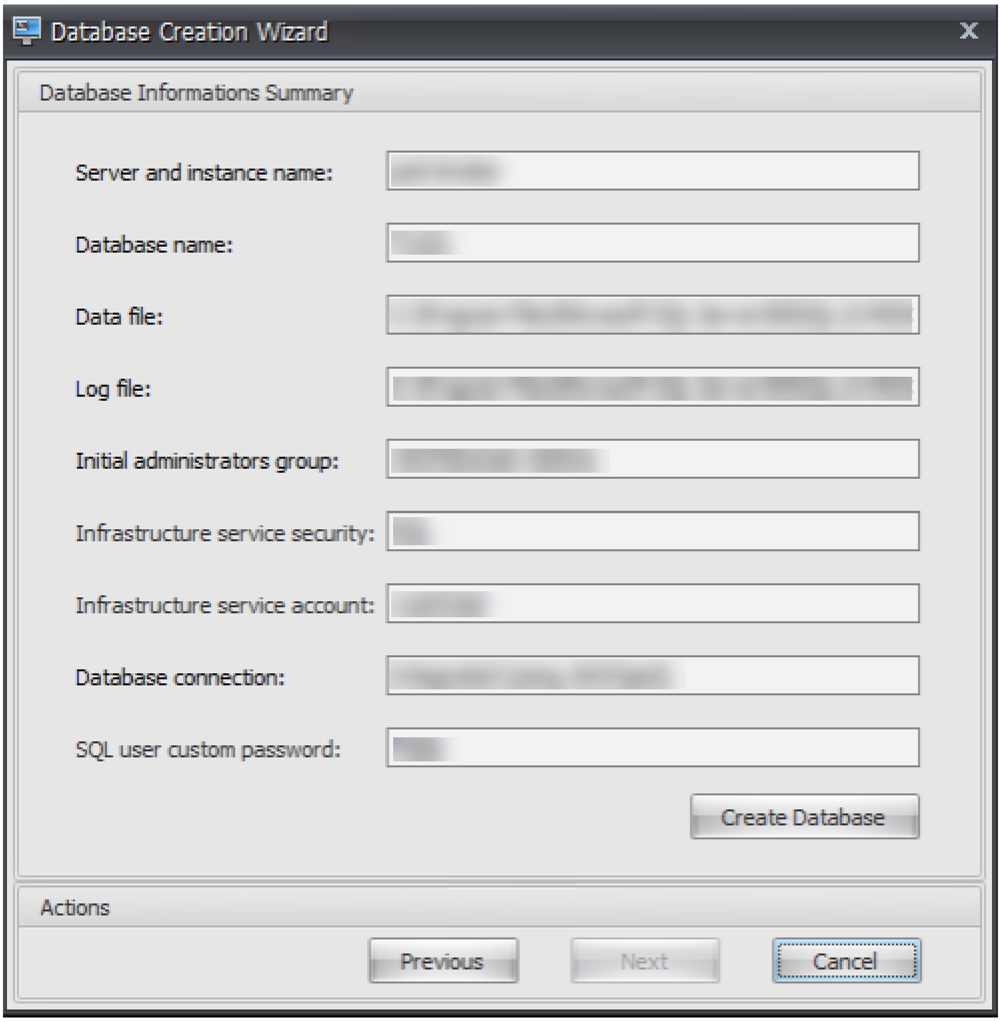
□ Set vuemUser SQL user account password

Password

□ Display password

Actions

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



Server and instance name: [redacted]

Database name: [redacted]

Data file: [redacted]

Log file: [redacted]

Initial administrators group: [redacted]

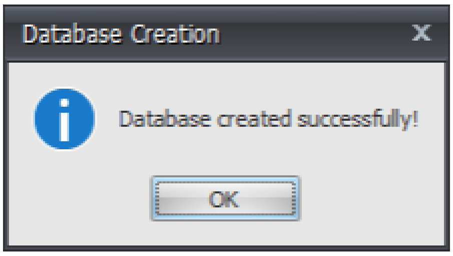
Infrastructure service security: [redacted]

Infrastructure service account: [redacted]

Database connection: [redacted]

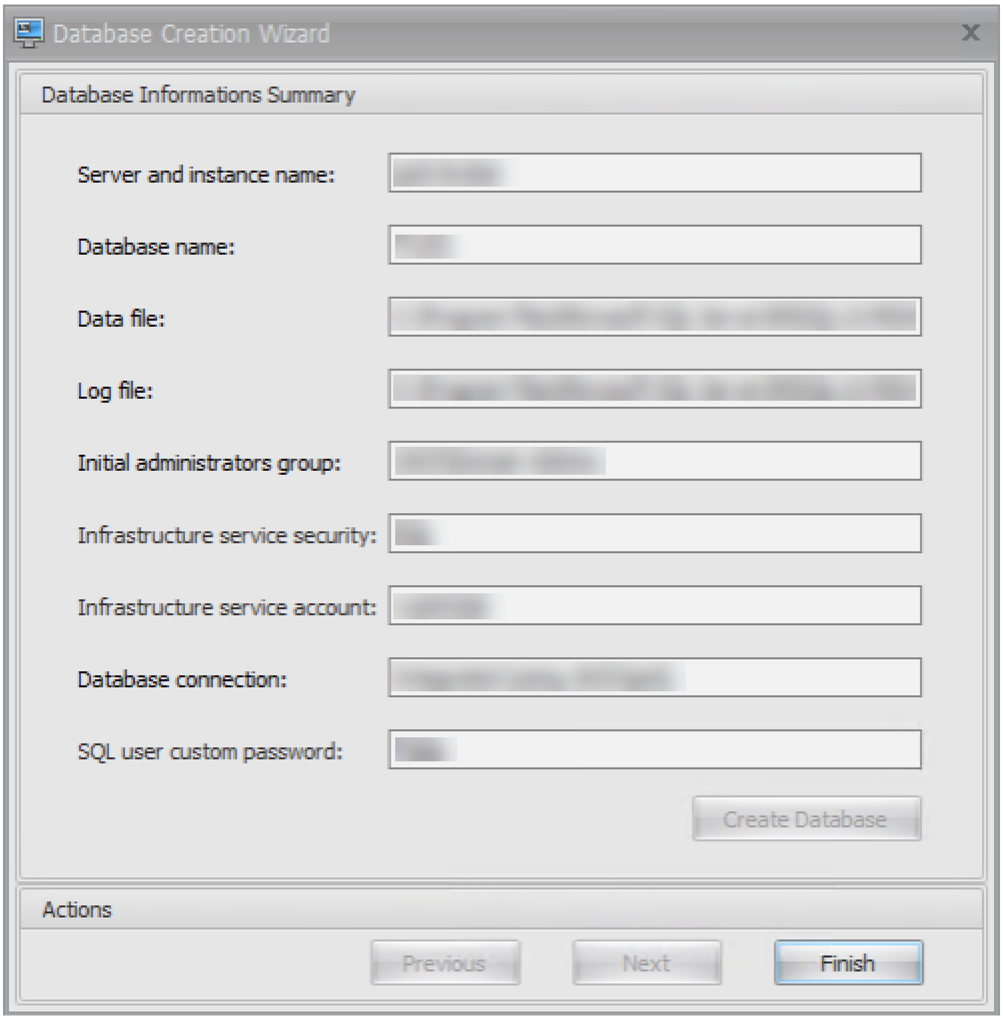
SQL user custom password: [redacted]

11. Click **OK**.



Database created successfully!

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



Database Informations Summary

Server and instance name: [redacted]

Database name: [redacted]

Data file: [redacted]

Log file: [redacted]

Initial administrators group: [redacted]

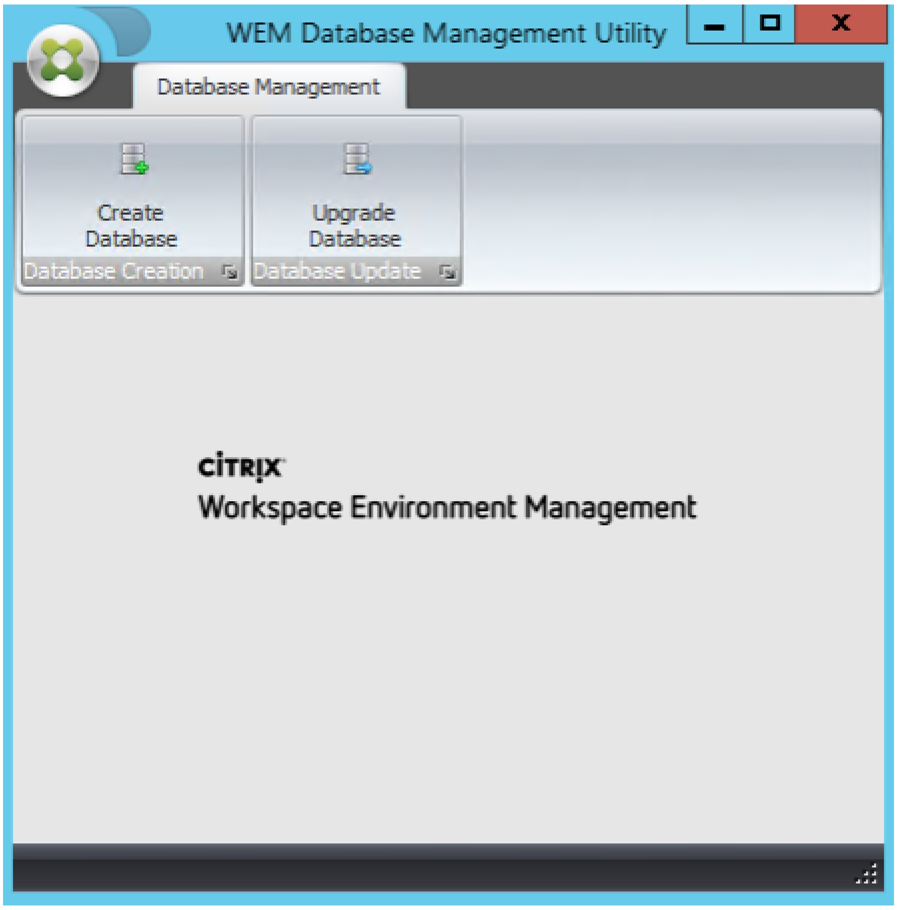
Infrastructure service security: [redacted]

Infrastructure service account: [redacted]

Database connection: [redacted]

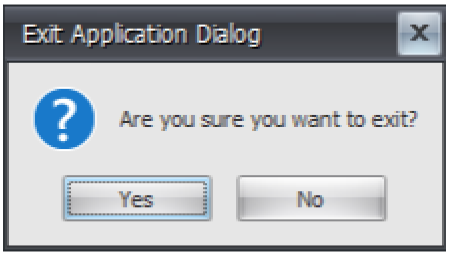
SQL user custom password: [redacted]

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



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

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

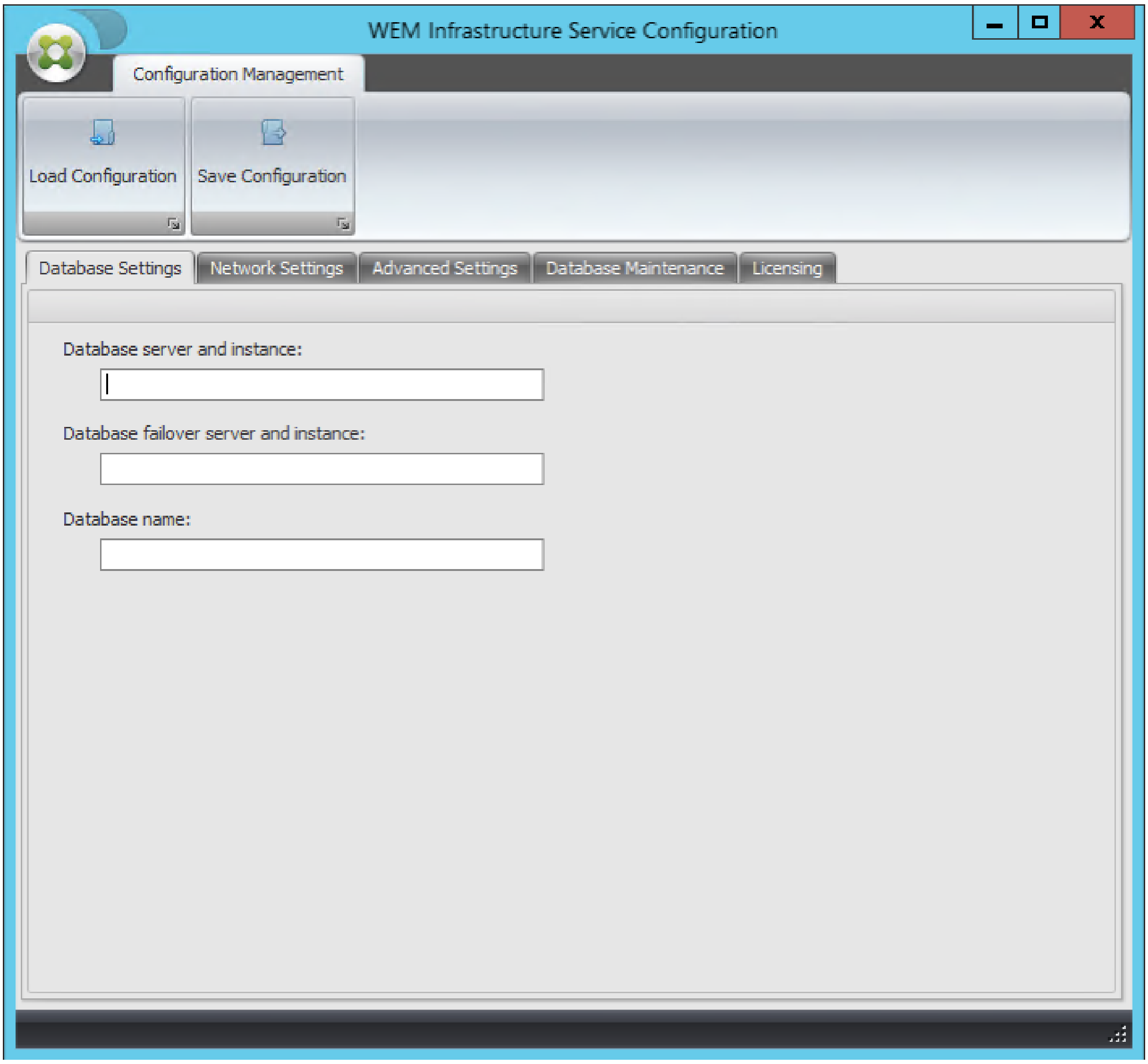


Are you sure you want to exit?

Step 3: Configure infrastructure services

1. Open the **WEM Infrastructure Service Configuration Utility** from the **Start** menu.

2. On the **Database Settings** tab, type the required information.



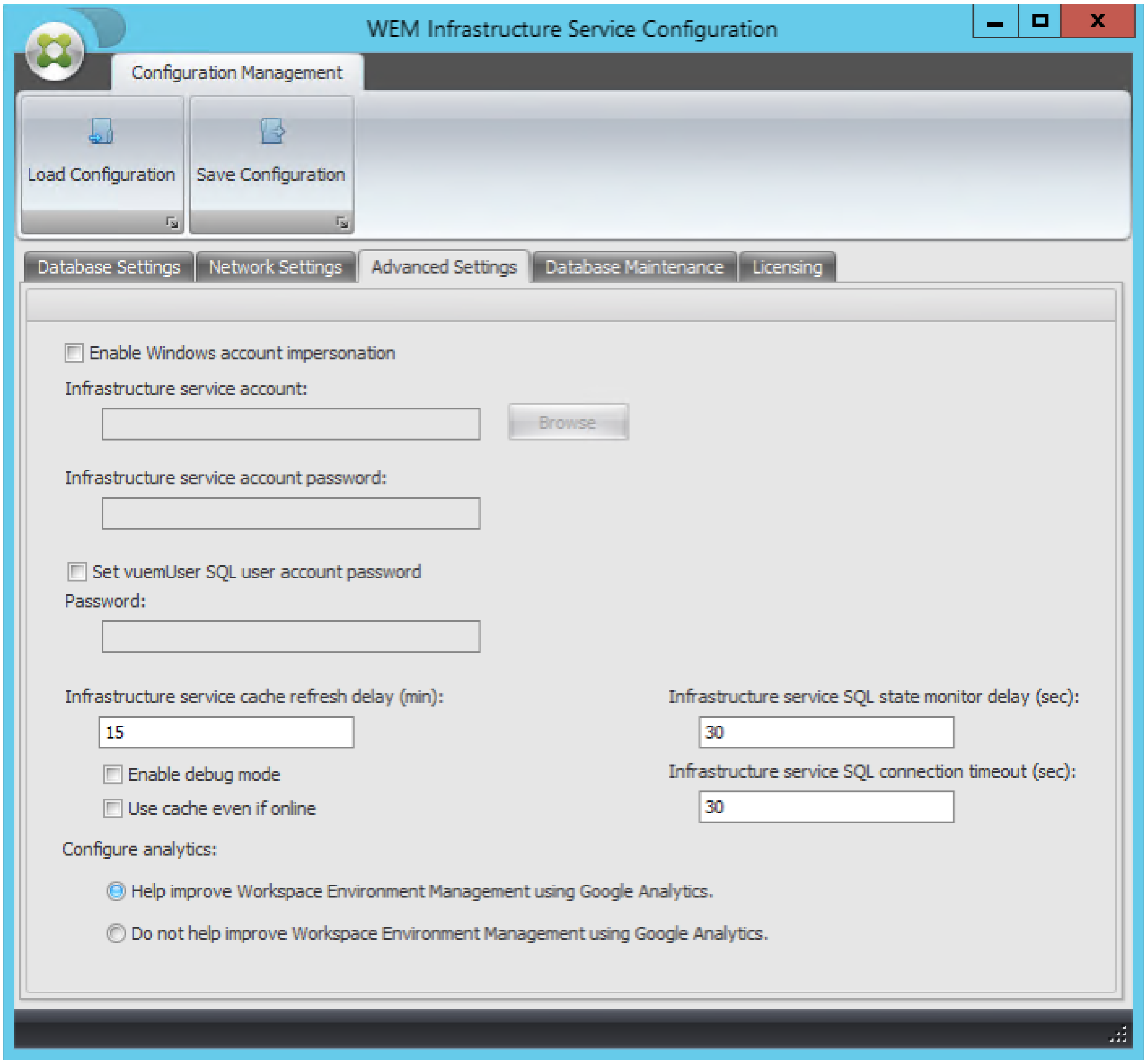
Database server and instance:

Database failover server and instance:

Database name:

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

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



□ Enable Windows account impersonation

Infrastructure service account:

Infrastructure service account password:

□ Set vuemUser SQL user account password

Password:

Infrastructure service cache refresh delay (min): 15

□ Enable debug mode

□ Use cache even if online

Infrastructure service SQL state monitor delay (sec): 30

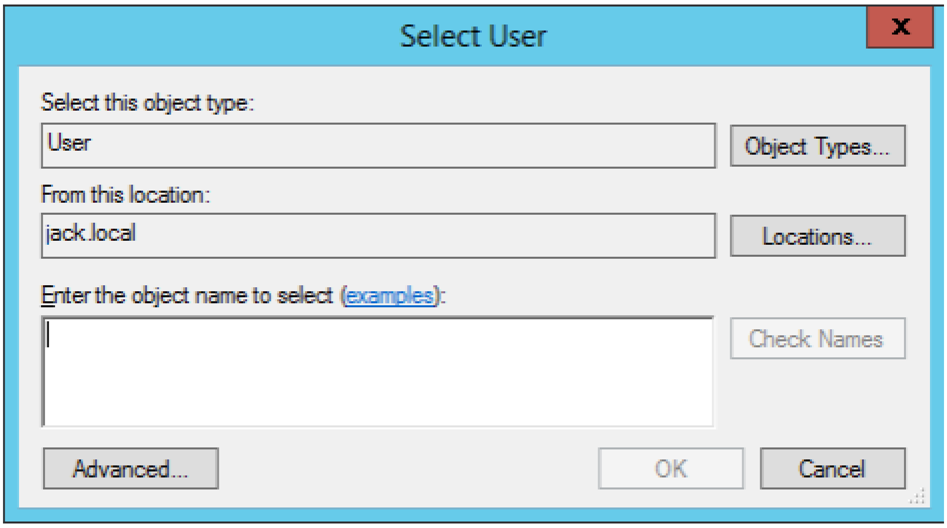
Infrastructure service SQL connection timeout (sec): 30

Configure analytics:

● Help improve Workspace Environment Management using Google Analytics.

○ Do not help improve Workspace Environment Management using Google Analytics.

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

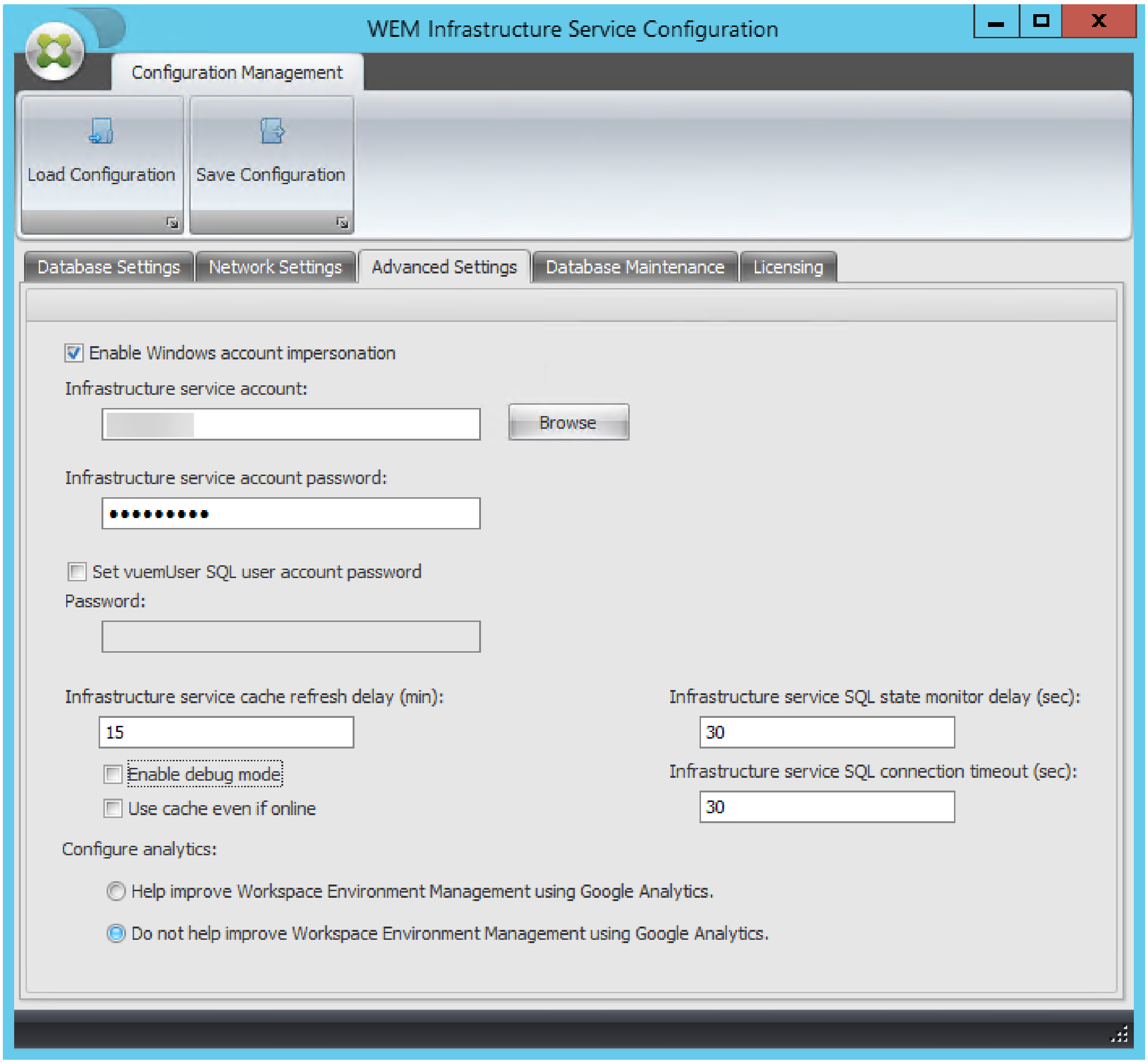


Select this object type: User

From this location: jack.local

Enter the object name to select (examples):

5. Type the infrastructure service account password.



☑ Enable Windows account impersonation

Infrastructure service account:

Infrastructure service account password: ●●●●●●●●●

□ Set vuemUser SQL user account password

Password:

Infrastructure service cache refresh delay (min): 15

□ Enable debug mode

□ Use cache even if online

Infrastructure service SQL state monitor delay (sec): 30

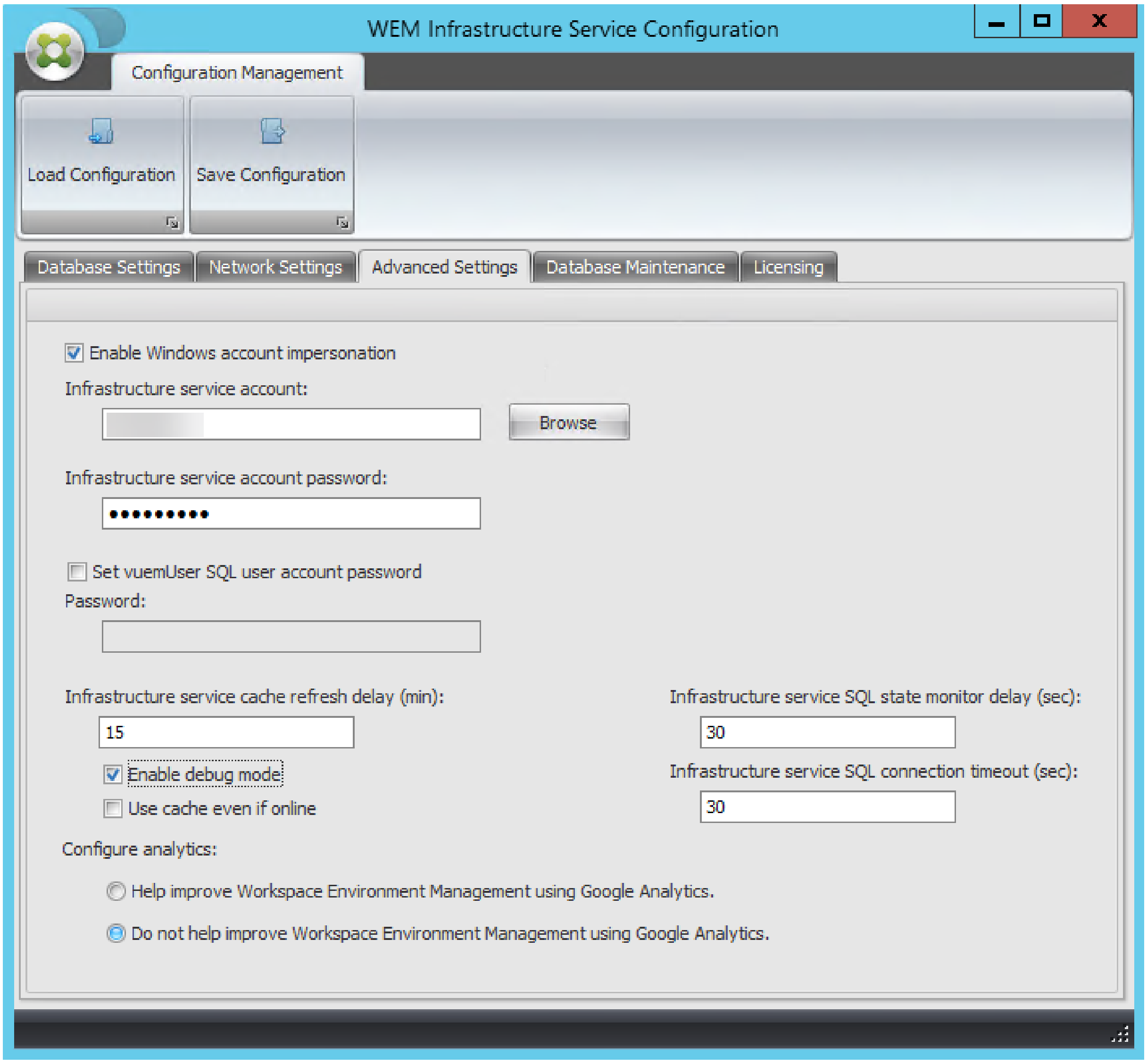
Infrastructure service SQL connection timeout (sec): 30

Configure analytics:

○ Help improve Workspace Environment Management using Google Analytics.

● Do not help improve Workspace Environment Management using Google Analytics.

6. Select **Enable debug mode**.



☑ Enable Windows account impersonation

Infrastructure service account:

Infrastructure service account password: ••••••••••

□ Set vuemUser SQL user account password

Password:

Infrastructure service cache refresh delay (min): 15

☑ Enable debug mode

□ Use cache even if online

Infrastructure service SQL state monitor delay (sec): 30

Infrastructure service SQL connection timeout (sec): 30

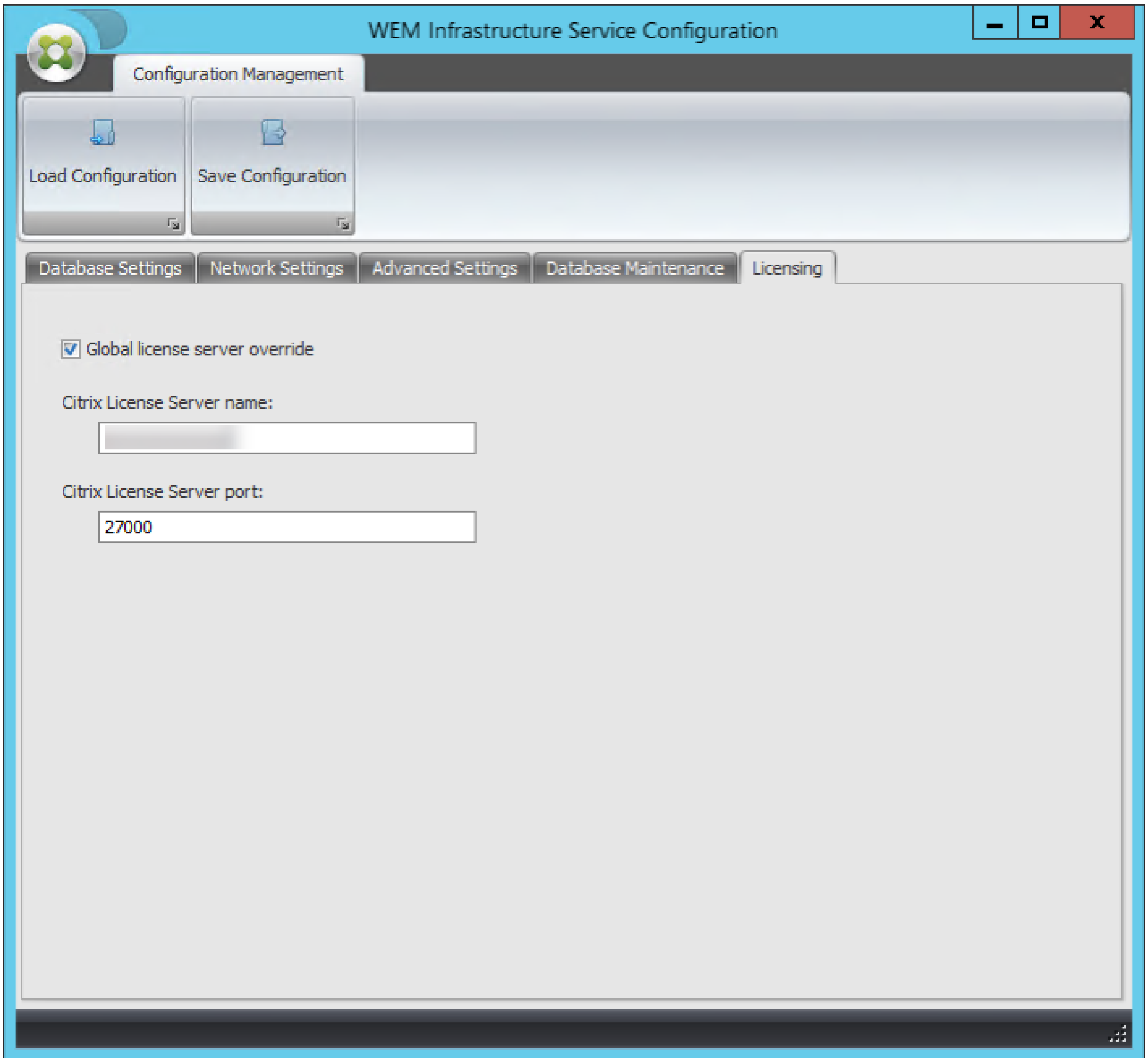
Configure analytics:

○ Help improve Workspace Environment Management using Google Analytics.

● Do not help improve Workspace Environment Management using Google Analytics.

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

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



☑ Global license server override

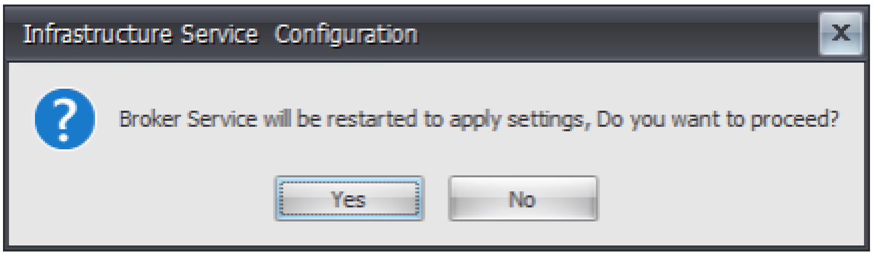
Citrix License Server name:

[redacted]

Citrix License Server port:

27000

8. Click **Yes**.

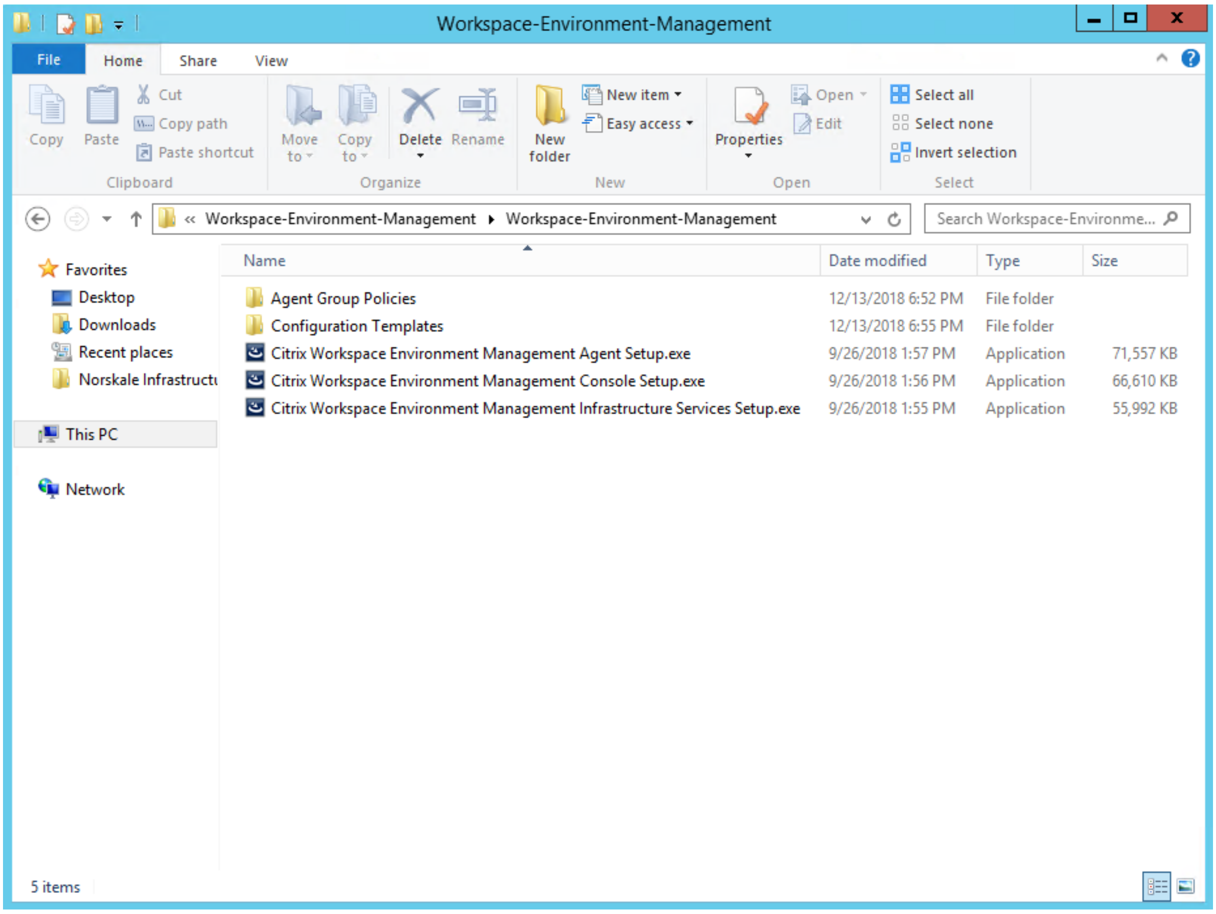


Broker Service will be restarted to apply settings, Do you want to proceed?

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

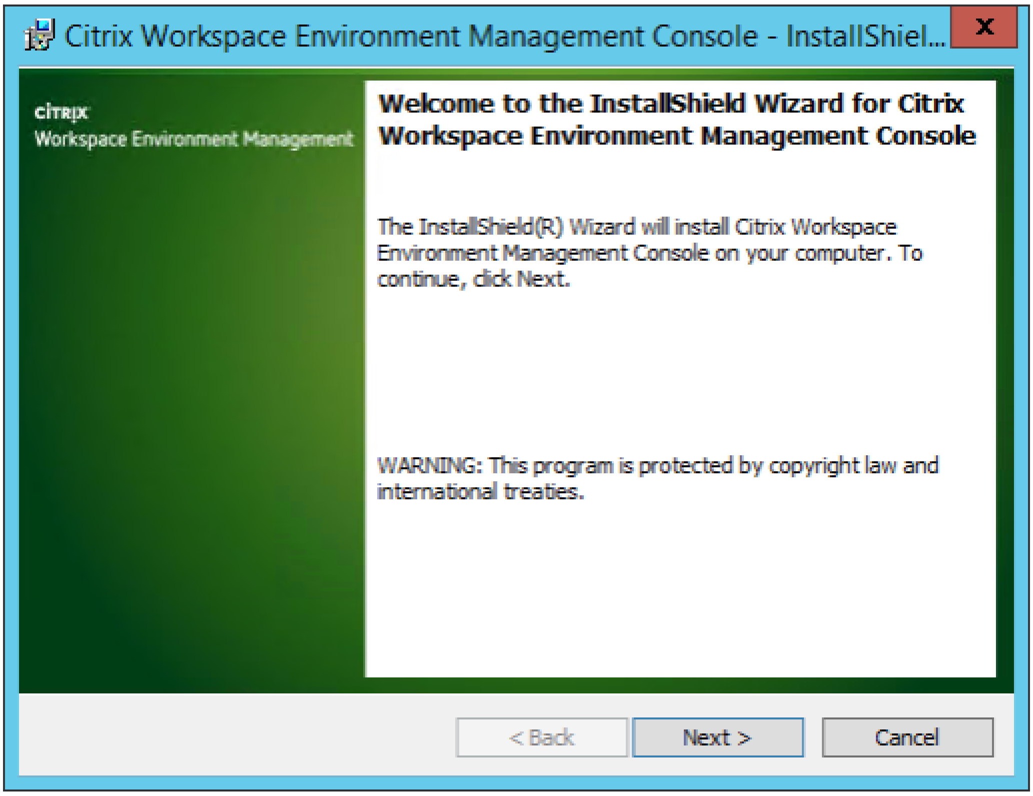
Step 4: Install the administration console

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



Name	Date modified	Type	Size
Agent Group Policies	12/13/2018 6:52 PM	File folder	
Configuration Templates	12/13/2018 6:55 PM	File folder	
Citrix Workspace Environment Management Agent Setup.exe	9/26/2018 1:57 PM	Application	71,557 KB
Citrix Workspace Environment Management Console Setup.exe	9/26/2018 1:56 PM	Application	66,610 KB
Citrix Workspace Environment Management Infrastructure Services Setup.exe	9/26/2018 1:55 PM	Application	55,992 KB

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



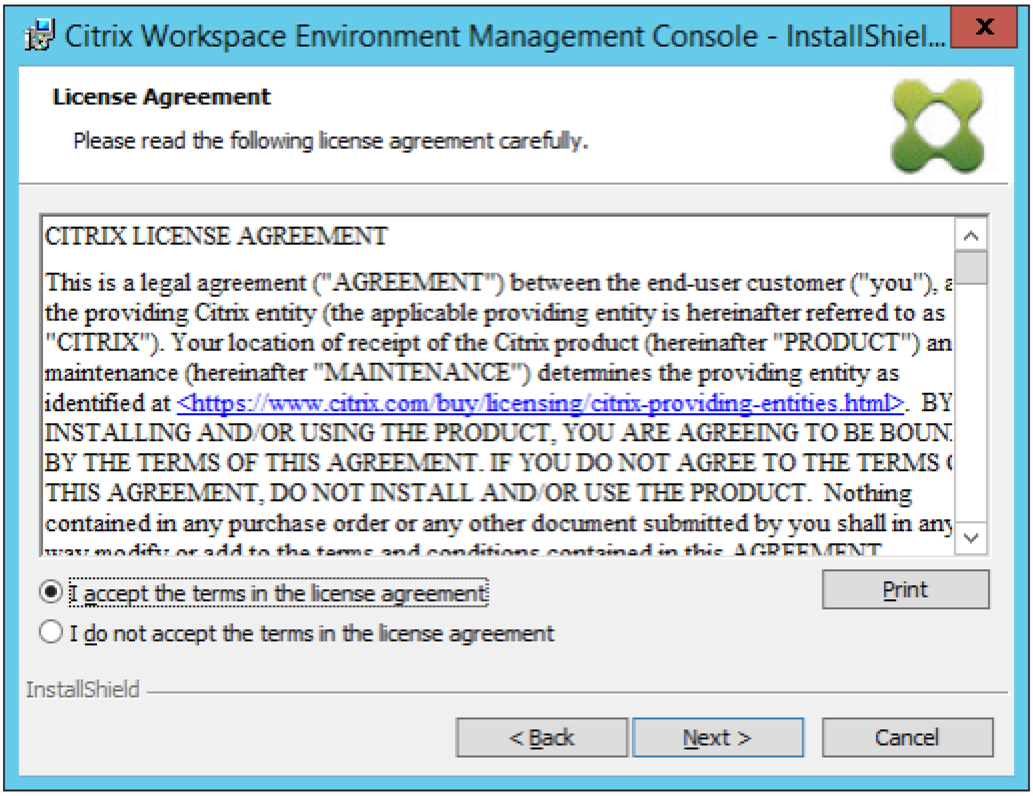
Citrix Workspace Environment Management Console - InstallShiel...

Welcome to the InstallShield Wizard for Citrix Workspace Environment Management Console

The InstallShield(R) Wizard will install Citrix Workspace Environment Management Console on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3. On the License Agreement page, select "I accept the terms in the license agreement" and then click **Next**.



Citrix Workspace Environment Management Console - InstallShiel...

License Agreement

Please read the following license agreement carefully.

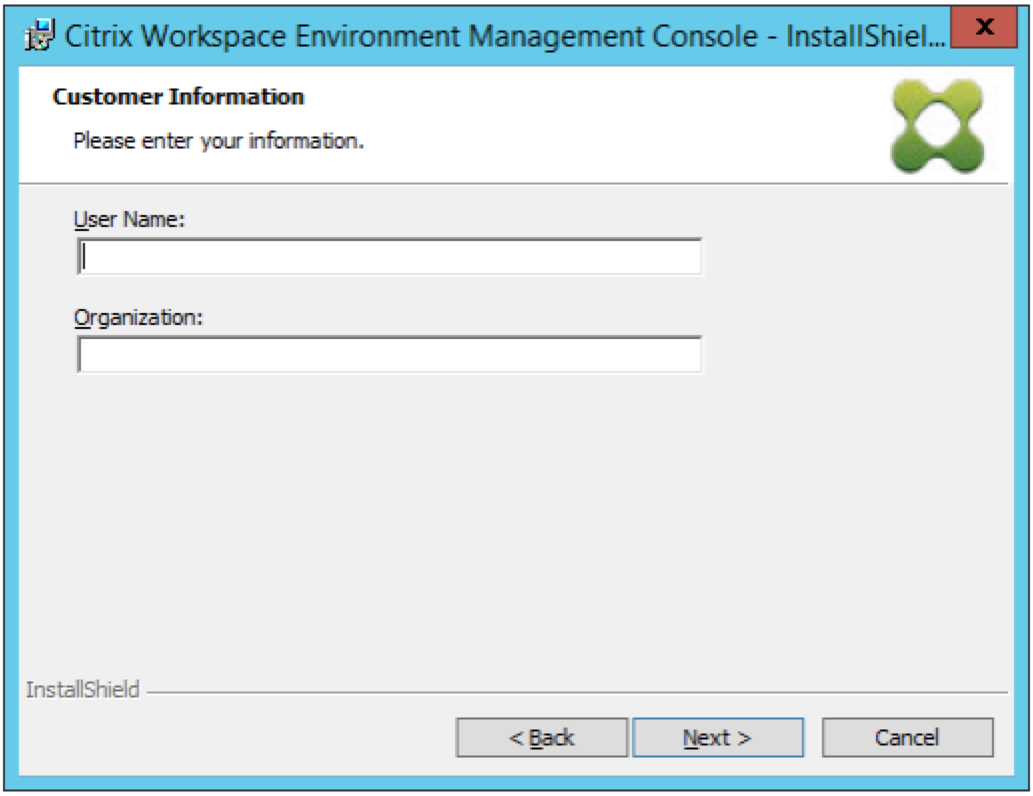
CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), a the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). Your location of receipt of the Citrix product (hereinafter "PRODUCT") an maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at <https://www.citrix.com/buy/licensing/citrix-providing-entities.html>. BY INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUN BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS (THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4. On the Customer Information page, type the required information and then click **Next**.



Citrix Workspace Environment Management Console - InstallShiel...

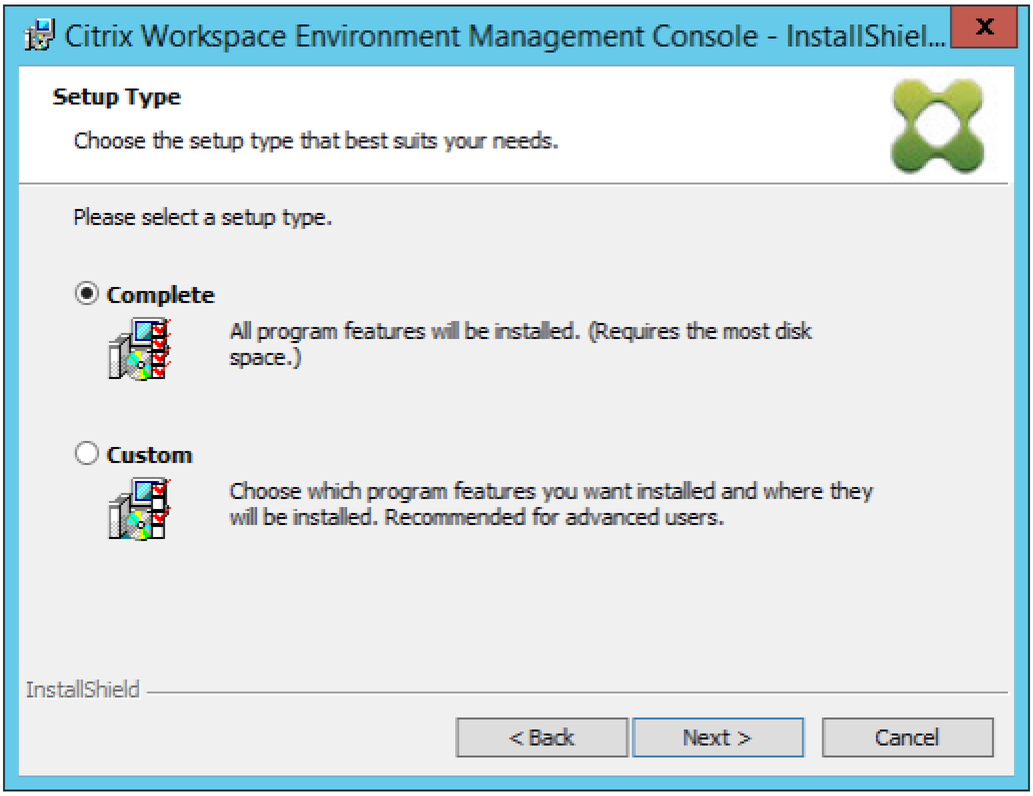
Customer Information

Please enter your information.

User Name:

Organization:

5. On the Setup Type page, select **Complete** and then click **Next**.



Citrix Workspace Environment Management Console - InstallShiel...

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

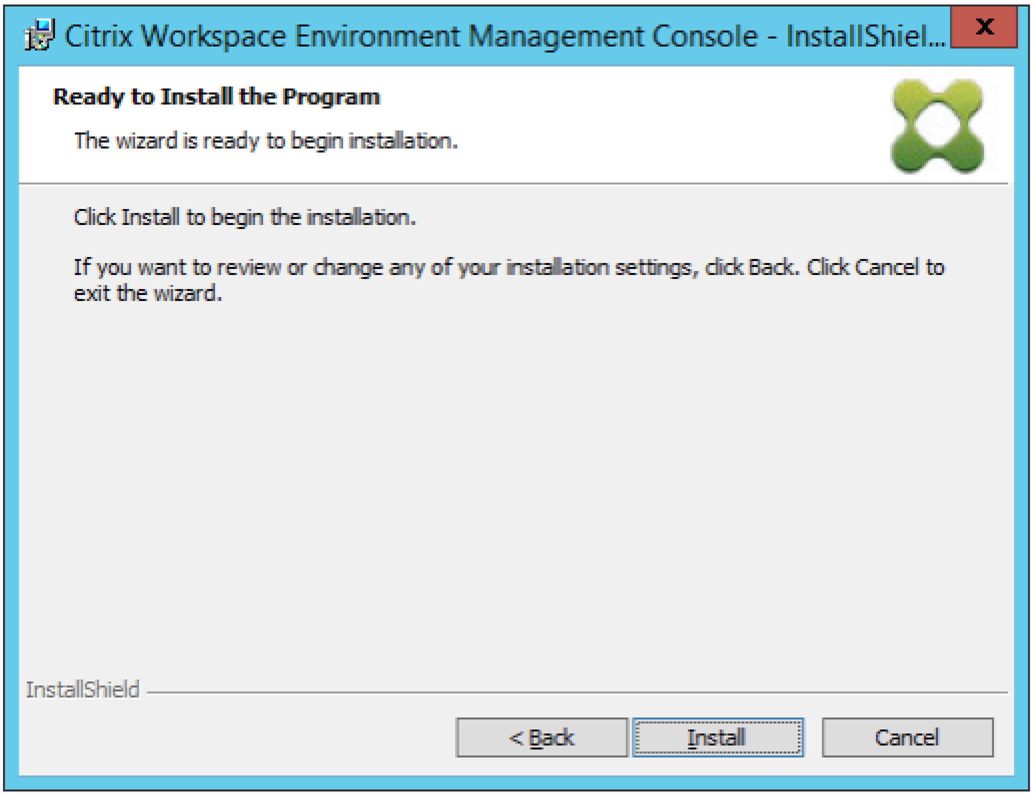
● **Complete**

All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

6. On the Ready to Install the Program page, click **Install**.



Citrix Workspace Environment Management Console - InstallShiel...

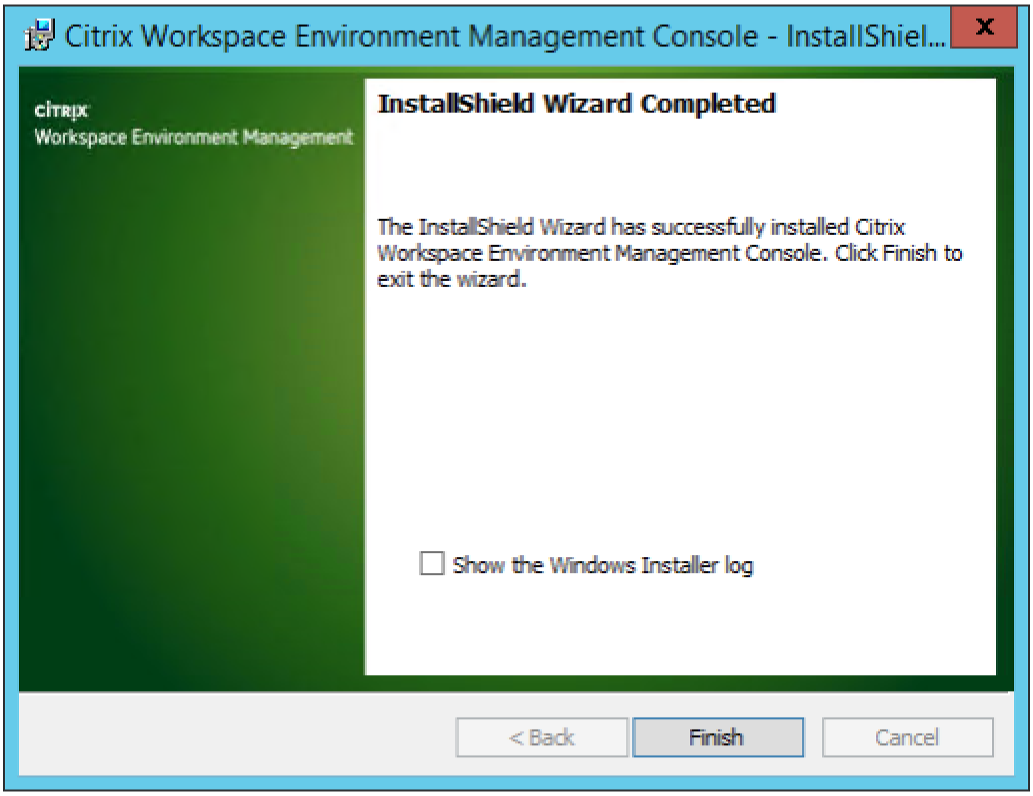
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

7. Click **Finish** to exit the wizard.



Citrix Workspace Environment Management Console - InstallShiel...

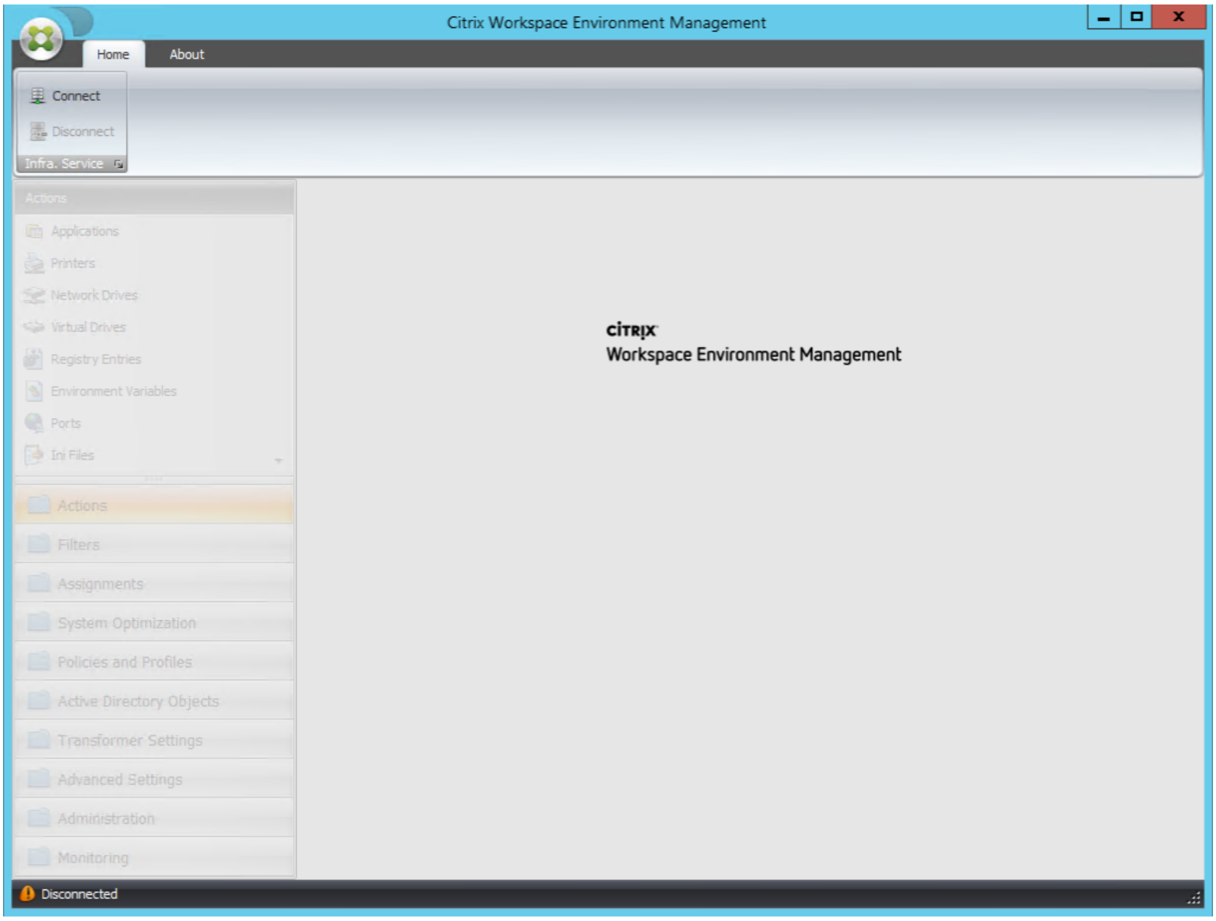
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Citrix Workspace Environment Management Console. Click Finish to exit the wizard.

☐ Show the Windows Installer log

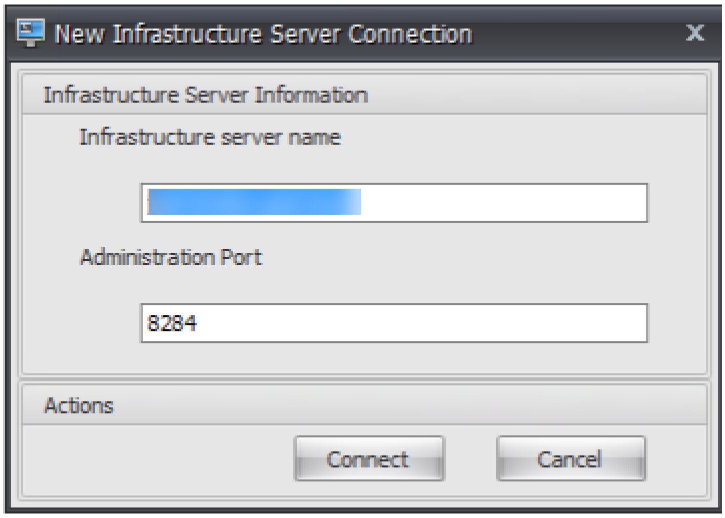
Step 5: Configure configuration sets

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



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

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



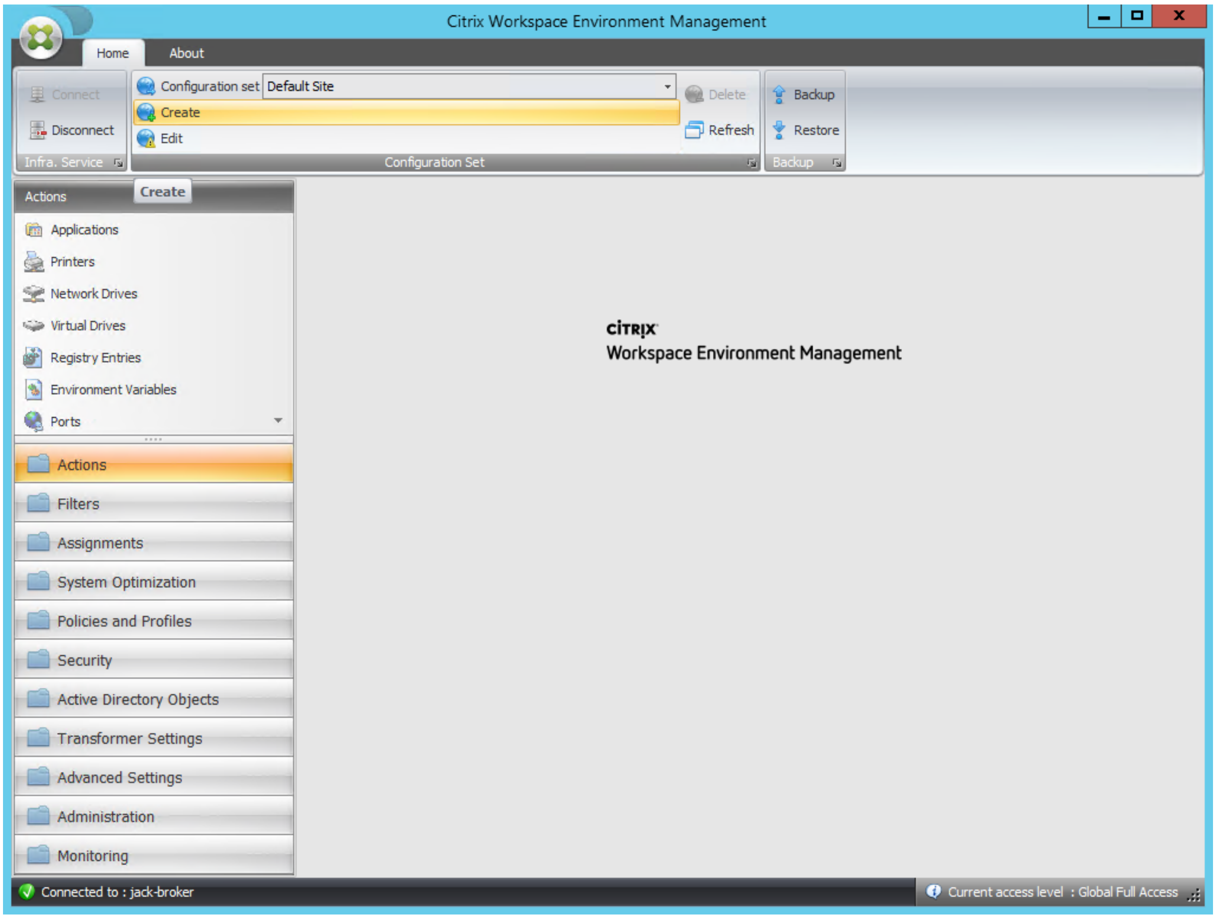
New Infrastructure Server Connection

Infrastructure Server Information

Infrastructure server name: [redacted]

Administration Port: 8284

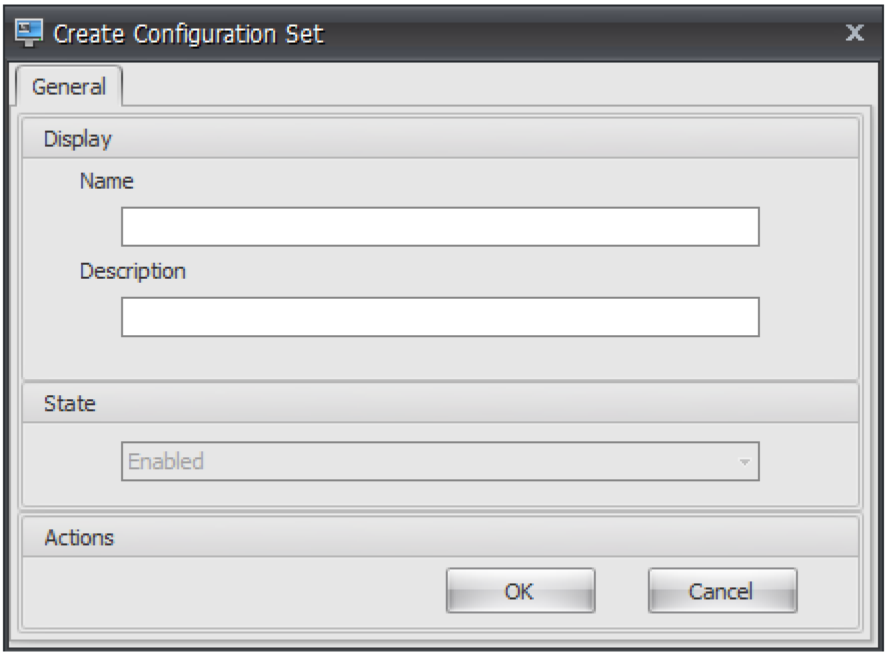
3. On the **Home** tab, on the ribbon, click **Create** to create your configuration set.



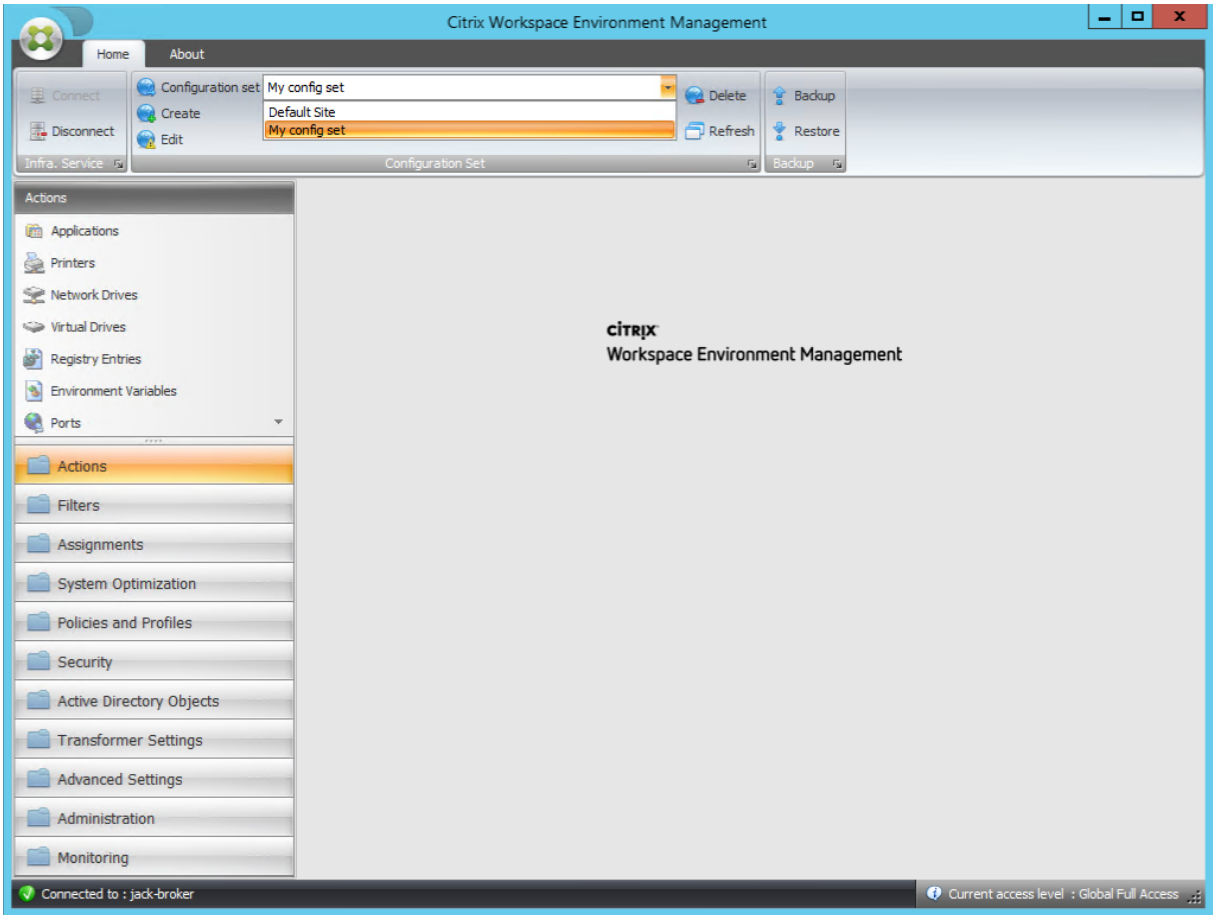
Connected to : jack-broker

Current access level : Global Full Access

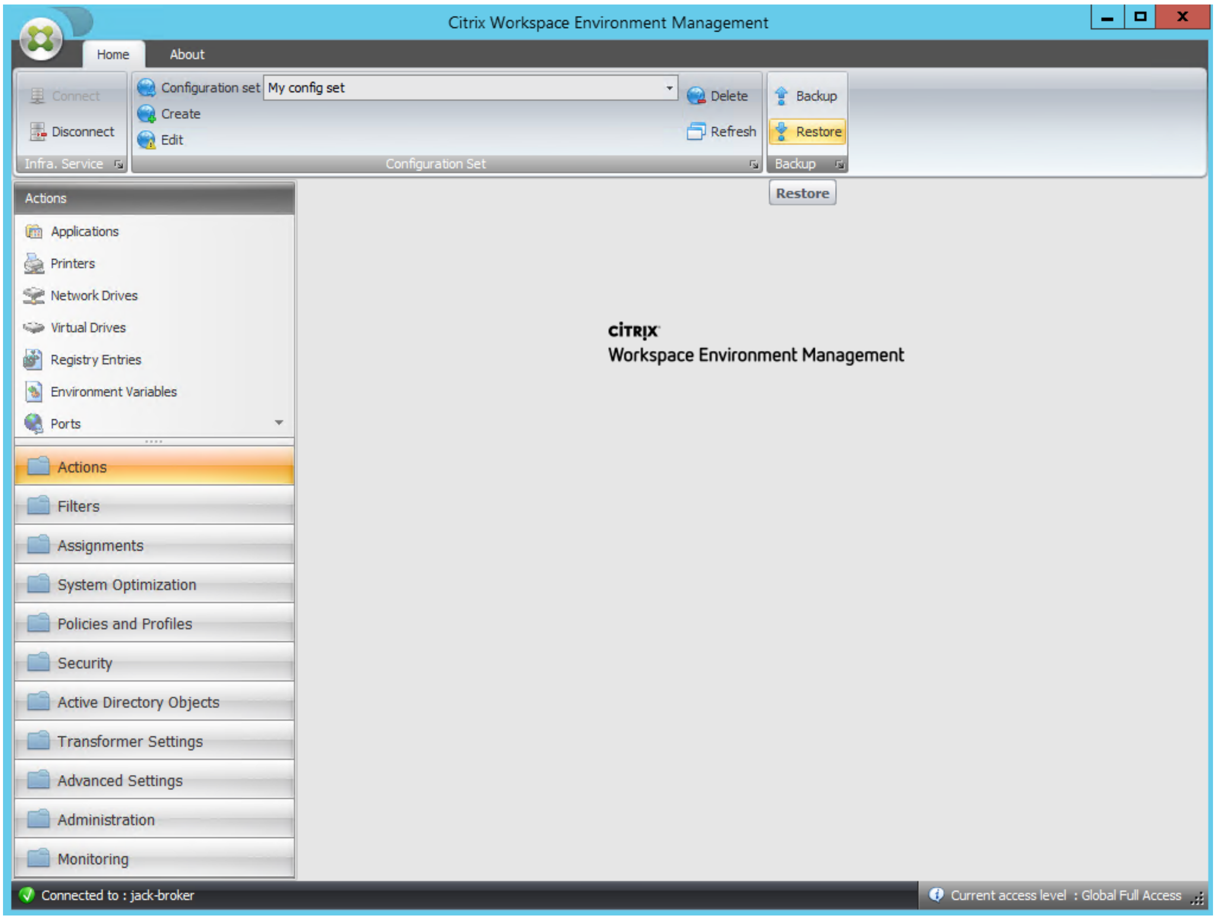
4. In the Create Configuration Set window, type a name and description for your configuration set and then click **OK**.



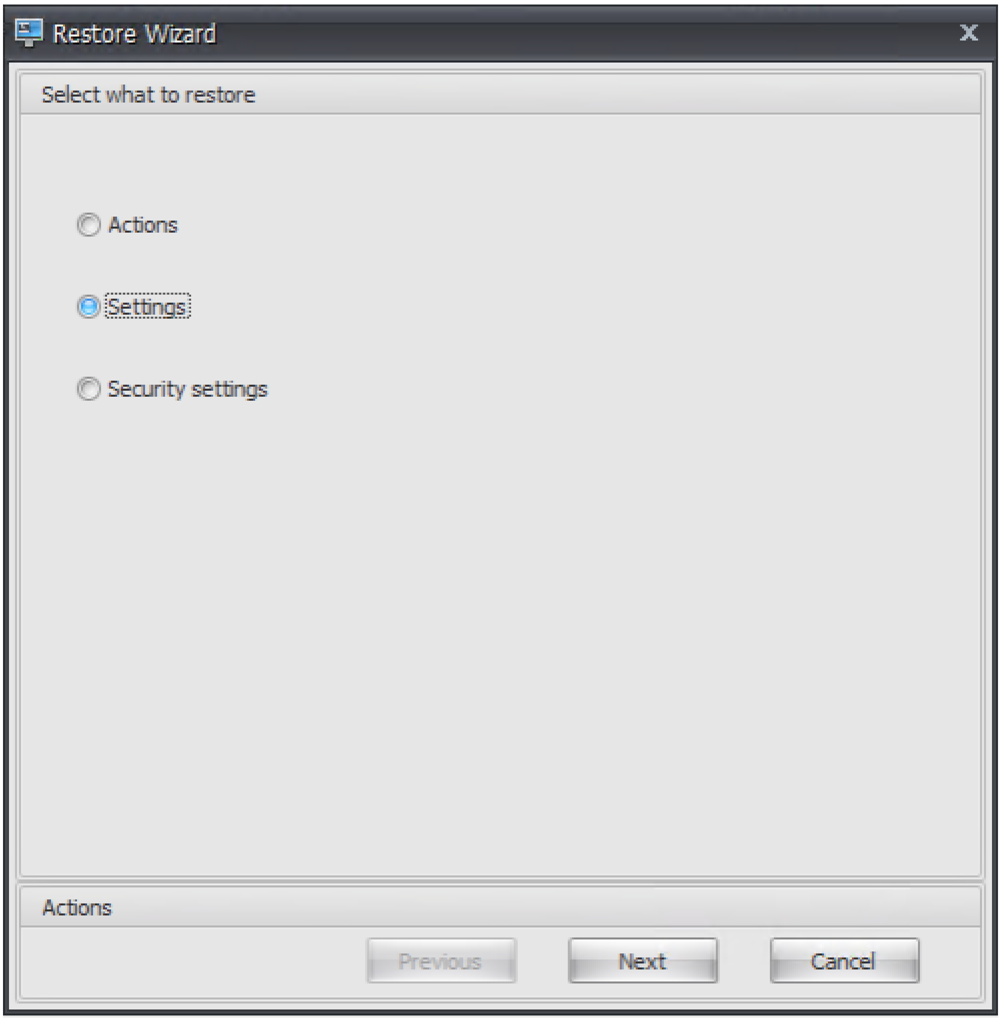
5. On the ribbon, under **Configuration Set**, select the newly created configuration set.



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



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



Restore Wizard

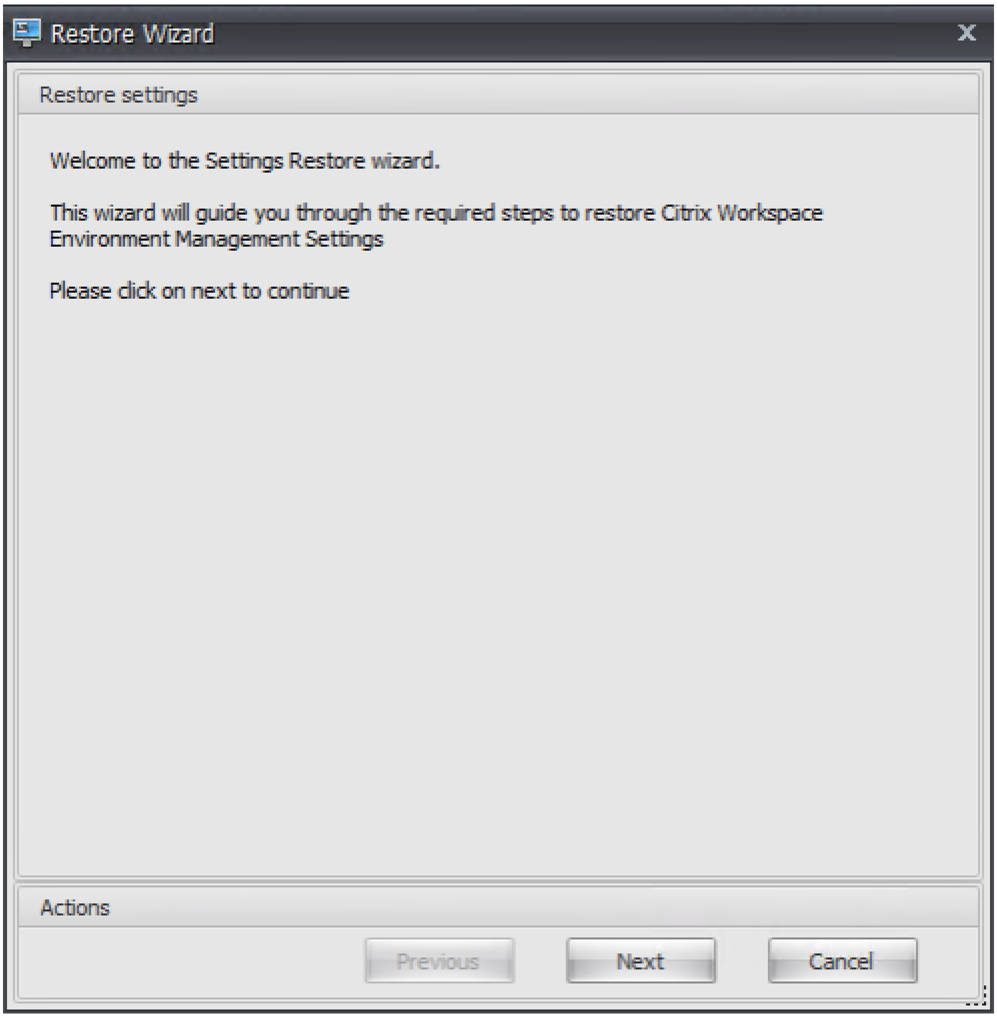
Select what to restore

○ Actions

● Settings

○ Security settings

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

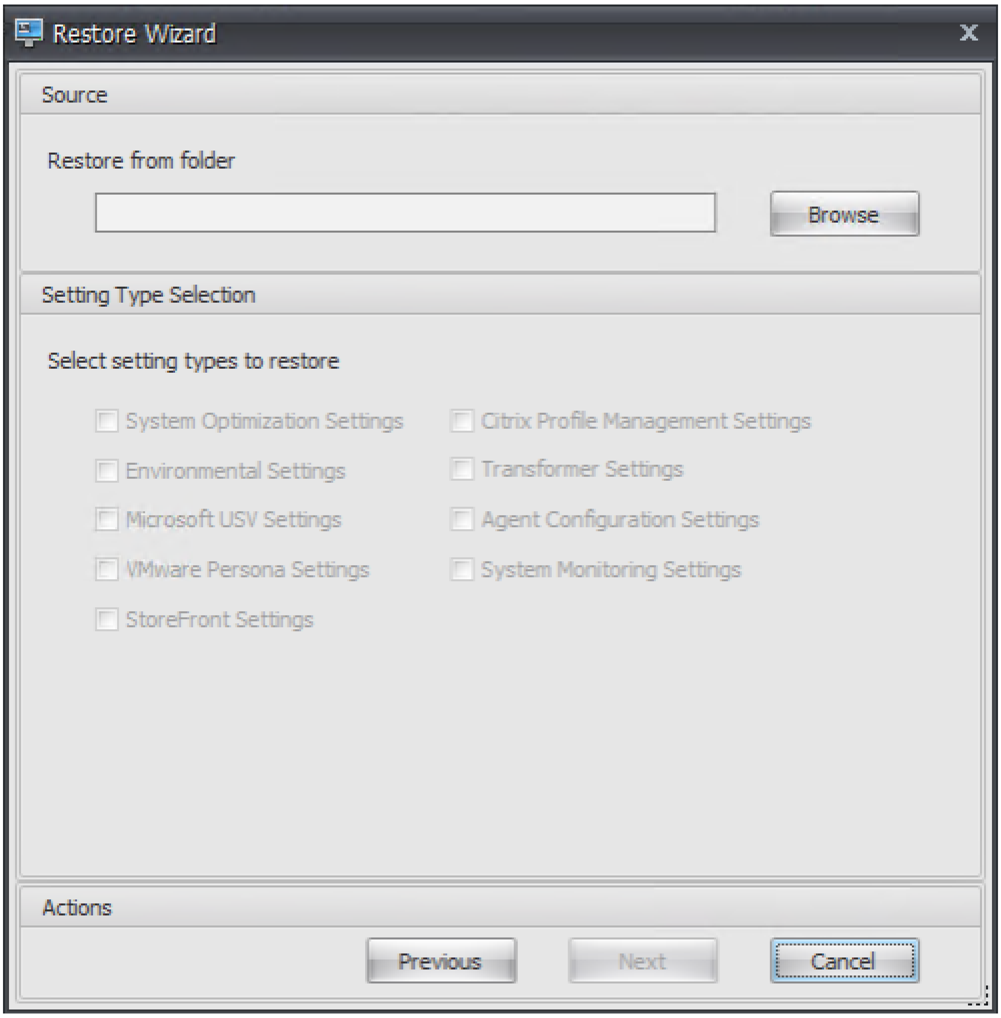


Welcome to the Settings Restore wizard.

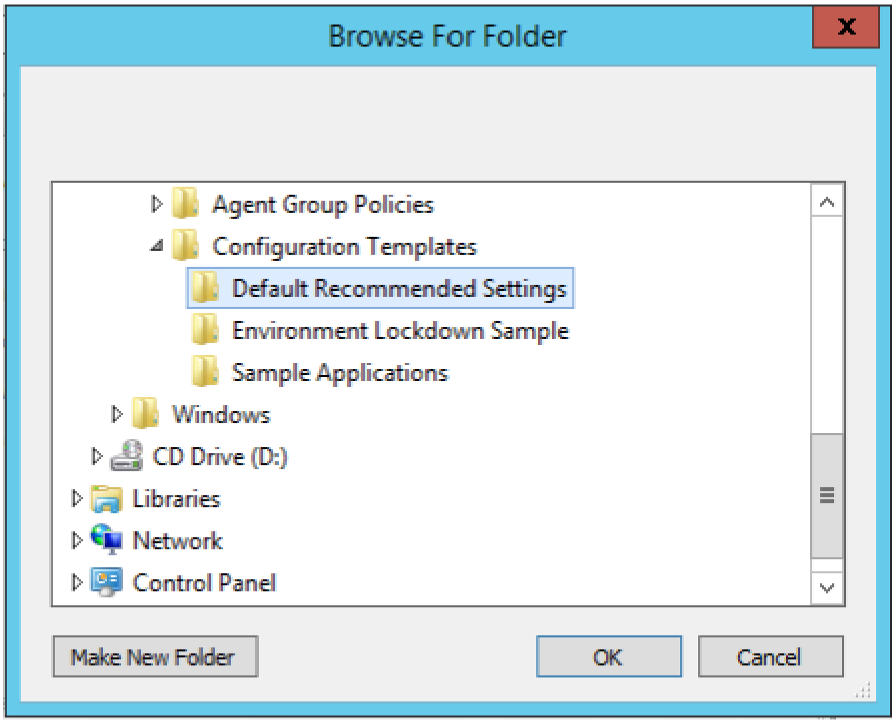
This wizard will guide you through the required steps to restore Citrix Workspace Environment Management Settings

Please click on next to continue

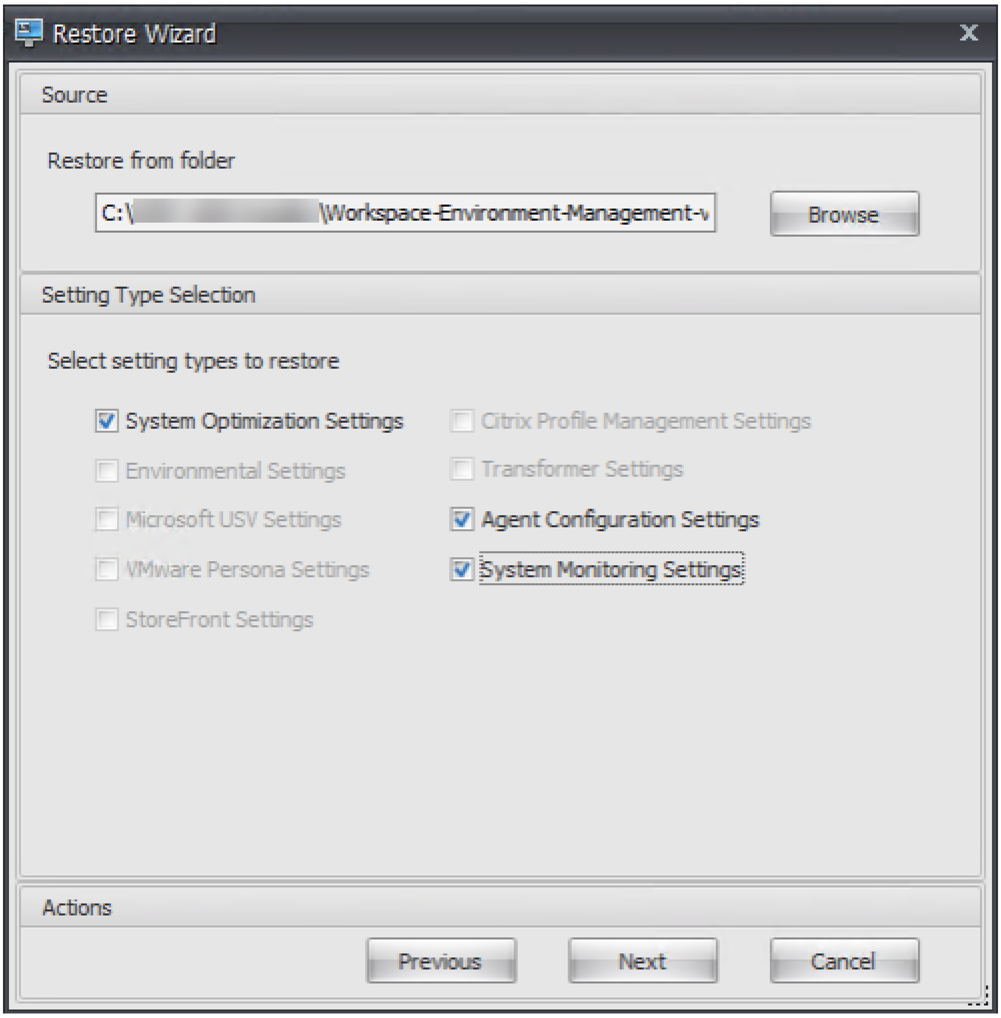
9. On the Source page, click **Browse**.



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



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



Restore Wizard

Source

Restore from folder

C:\[redacted]\Workspace-Environment-Management-v

Setting Type Selection

Select setting types to restore

☑ System Optimization Settings

□ Environmental Settings

□ Microsoft USV Settings

□ VMware Persona Settings

□ StoreFront Settings

□ Citrix Profile Management Settings

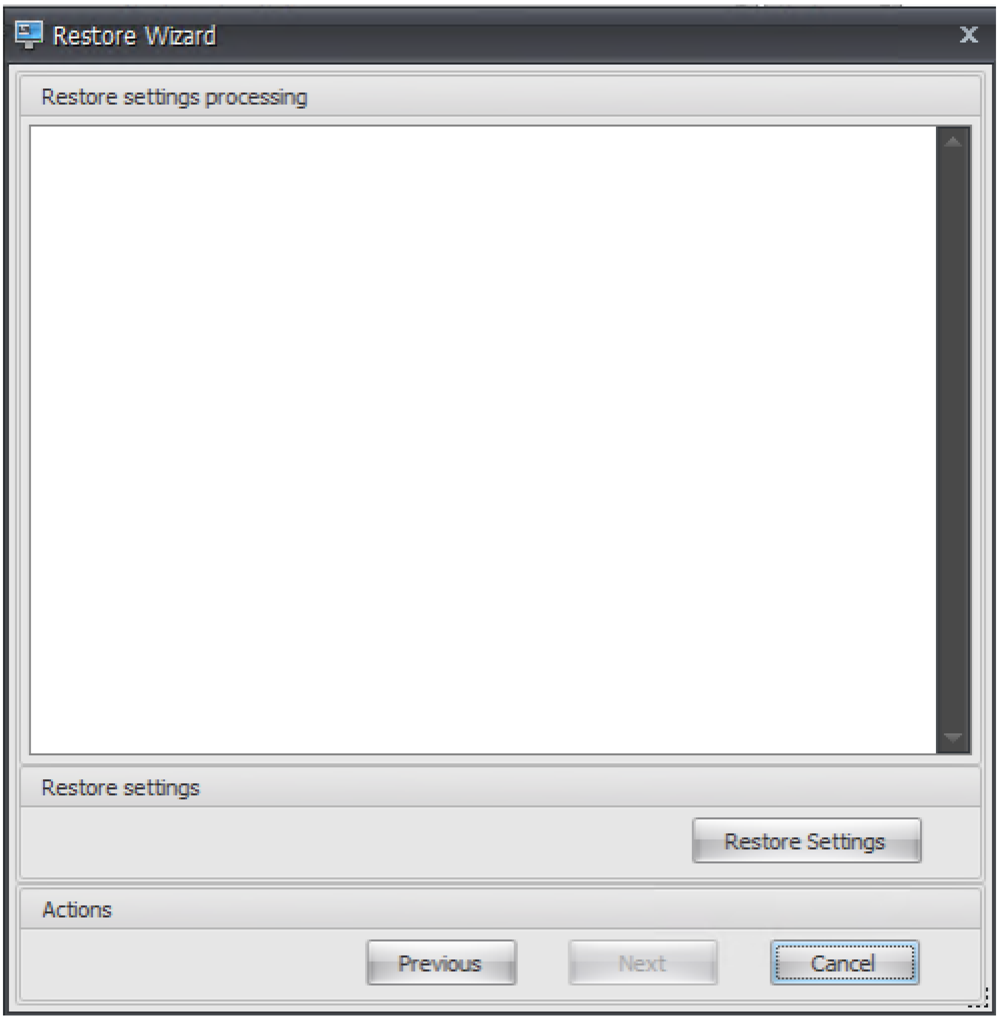
□ Transformer Settings

☑ Agent Configuration Settings

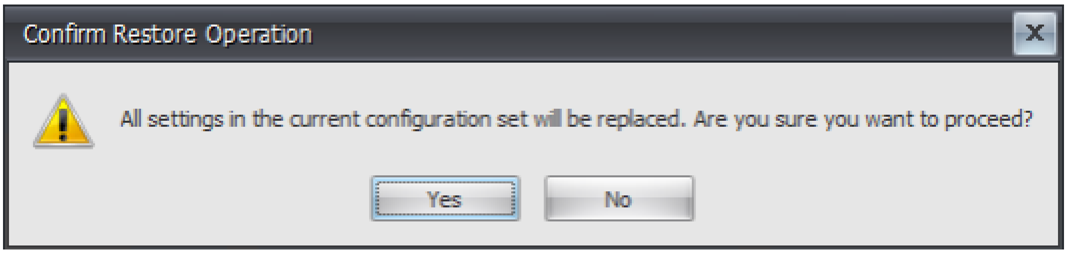
☑ System Monitoring Settings

Actions

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

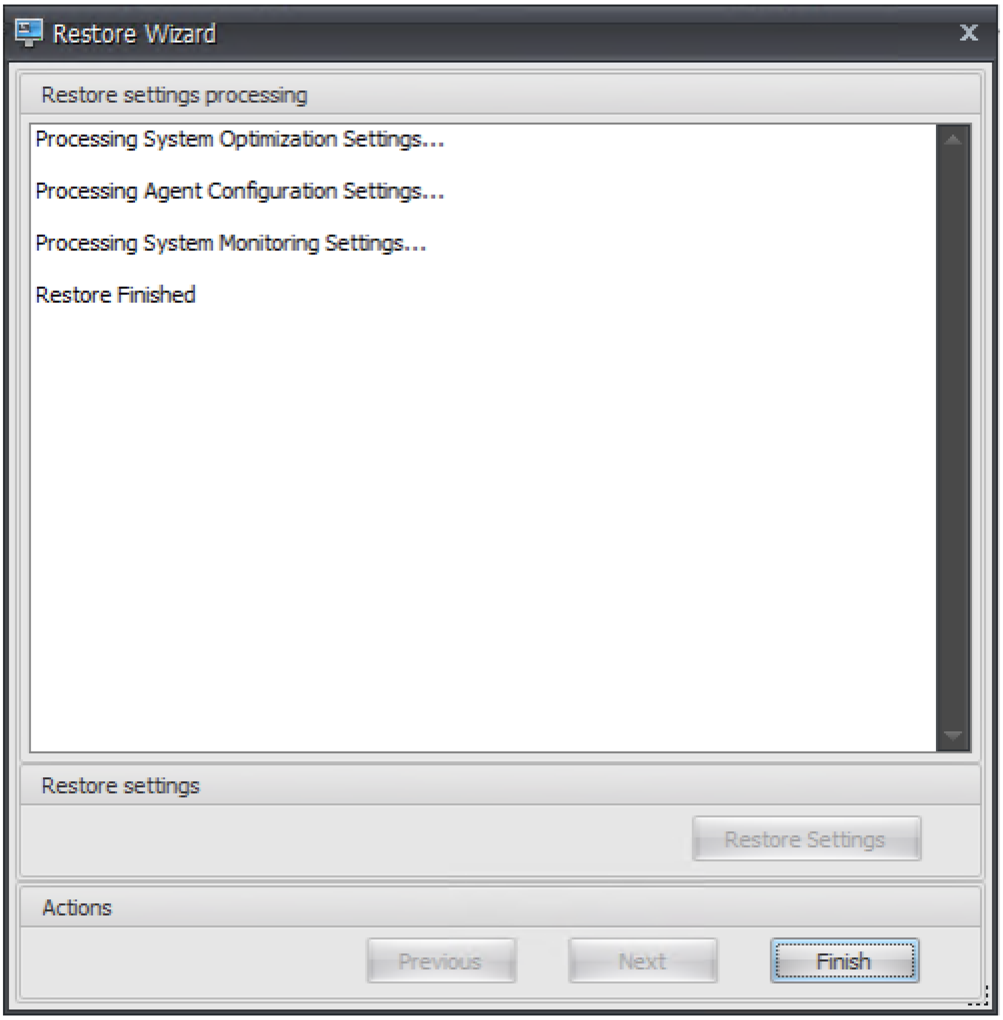


13. Click **Yes**.



All settings in the current configuration set will be replaced. Are you sure you want to proceed?

14. Click **Finish**.



Processing System Optimization Settings...

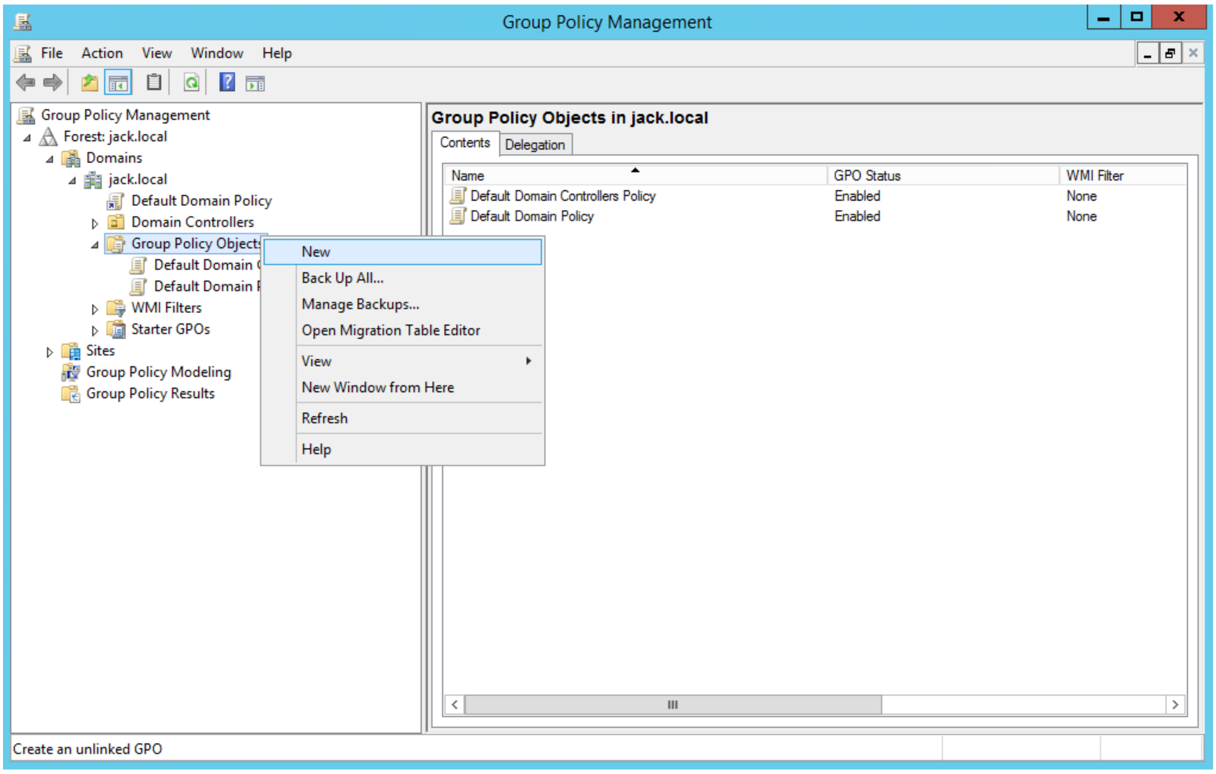
Processing Agent Configuration Settings...

Processing System Monitoring Settings...

Restore Finished

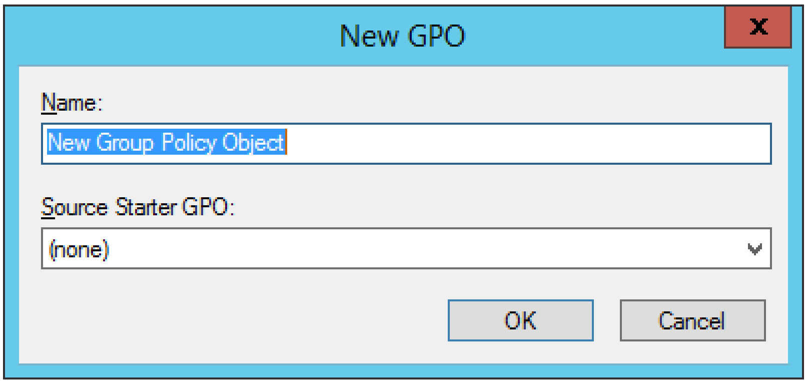
Step 6: Import group policy template

1. Open the **Group Policy Management** console on the domain controller.
2. In the console, right-click **Group Policy Objects** and select **New**.



Name	GPO Status	WMI Filter
Default Domain Controllers Policy	Enabled	None
Default Domain Policy	Enabled	None

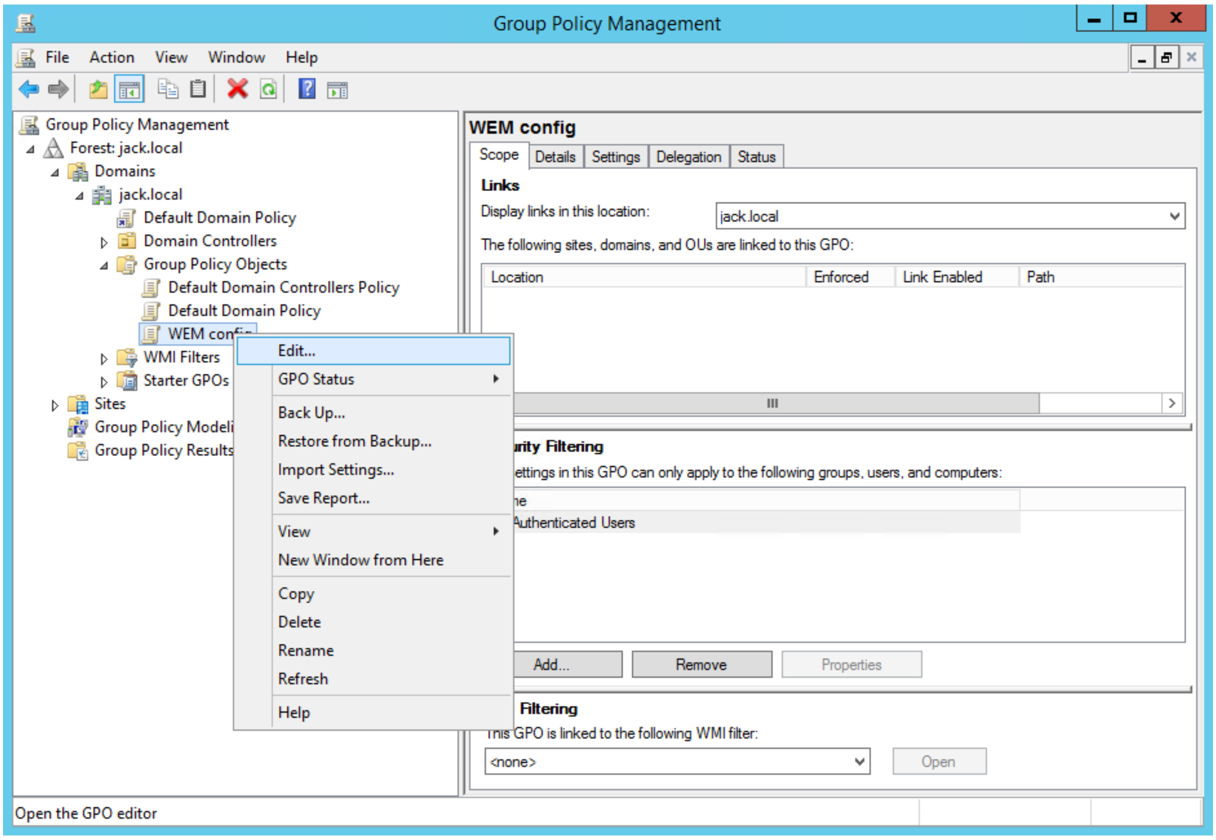
3. In the New GPO window, type the required information and then click **OK**.



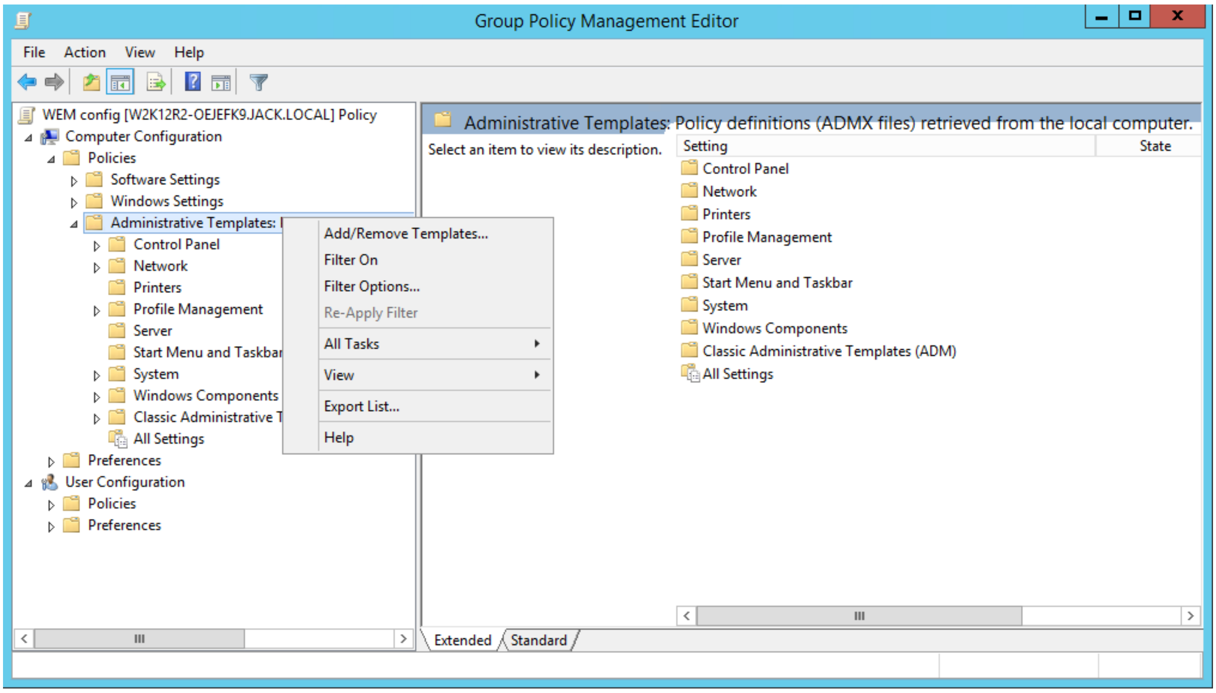
Name: New Group Policy Object

Source Starter GPO: (none)

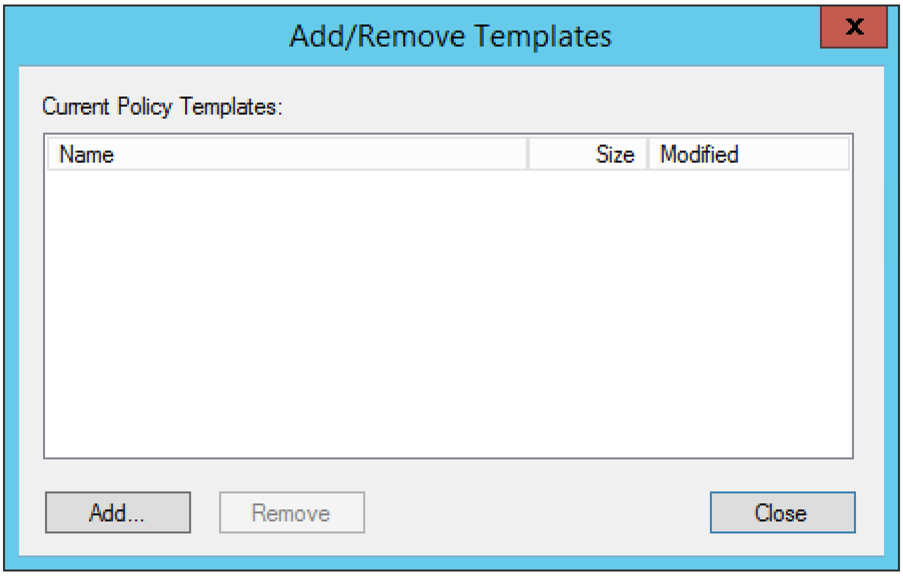
4. In the console, right-click the newly created GPO and select **Edit**.



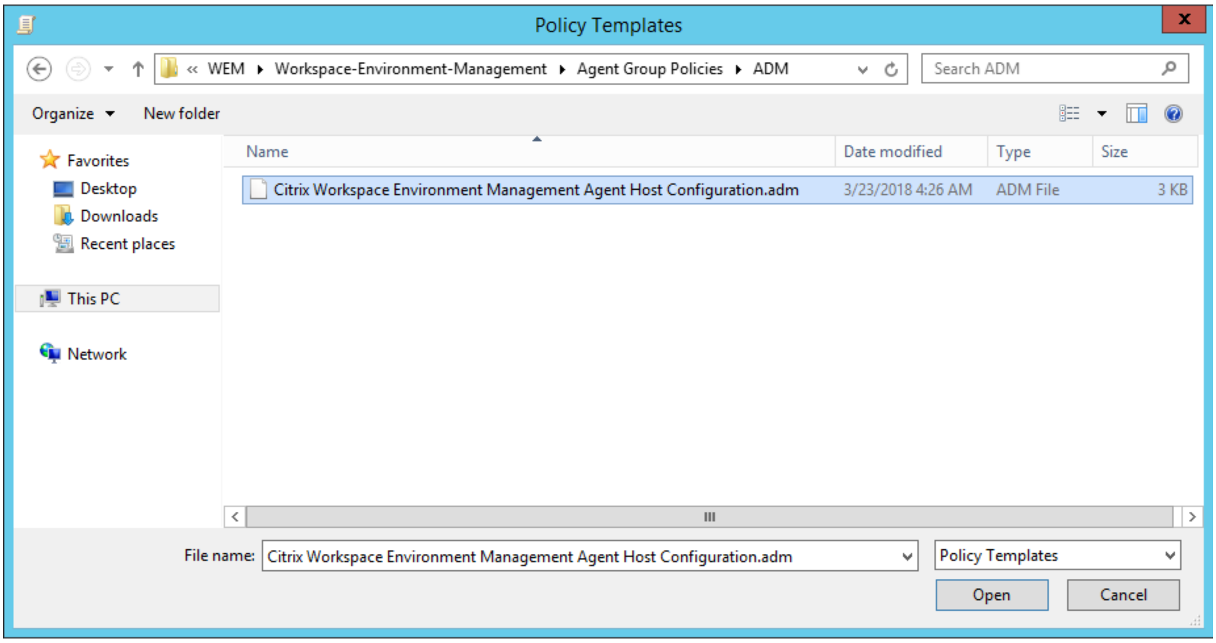
5. Right-click **Administrative Templates** (Computer Configuration > Policies > Administrative Templates), and select **Add/Remove Templates**.



6. In the Add/Remove Templates windows, Click **Add**.



7. Browse to the **Citrix Workspace Environment Management Agent Host Configuration.adm** template in the **Agent Group Policies** folder (provided with Workspace Environment Management installer), and then click **Open**.

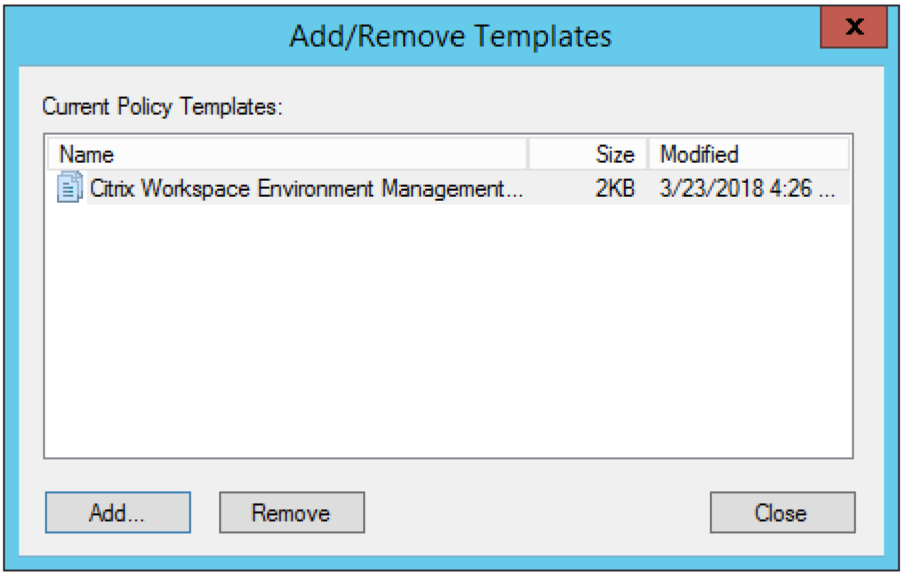


Name	Date modified	Type	Size
Citrix Workspace Environment Management Agent Host Configuration.adm	3/23/2018 4:26 AM	ADM File	3 KB

File name: Citrix Workspace Environment Management Agent Host Configuration.adm

Policy Templates

8. Click **Close**.

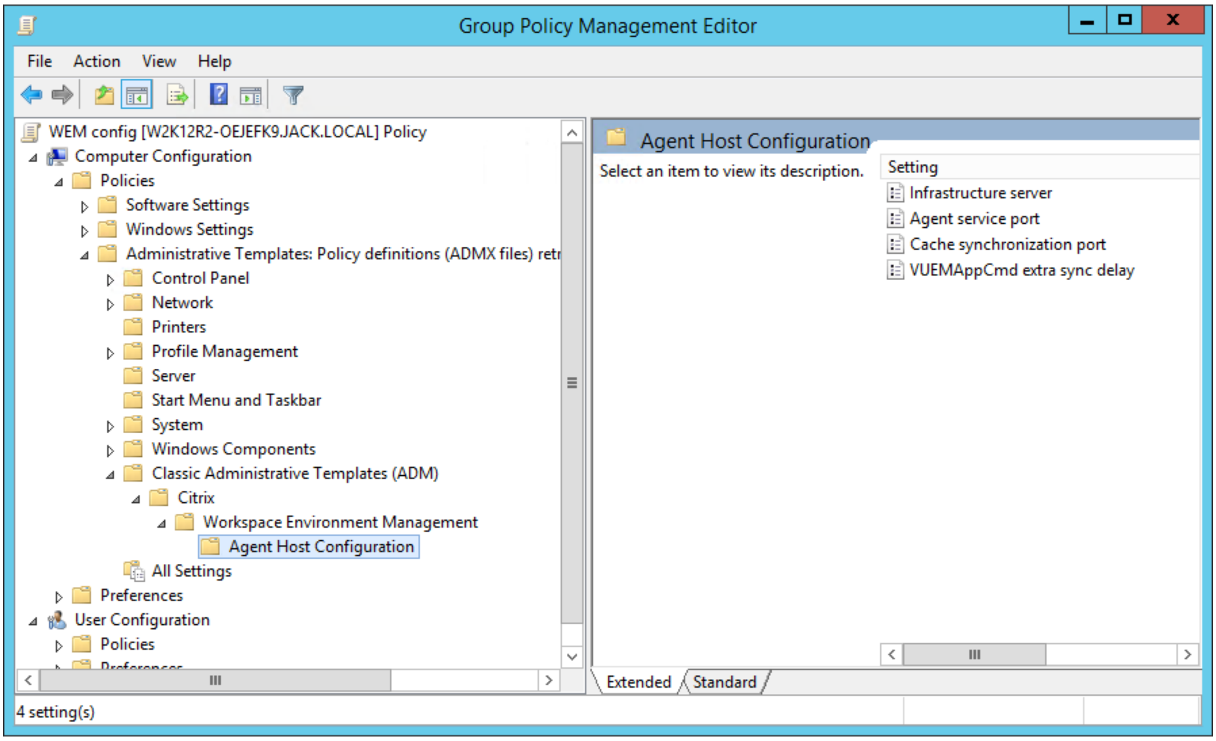


Add/Remove Templates

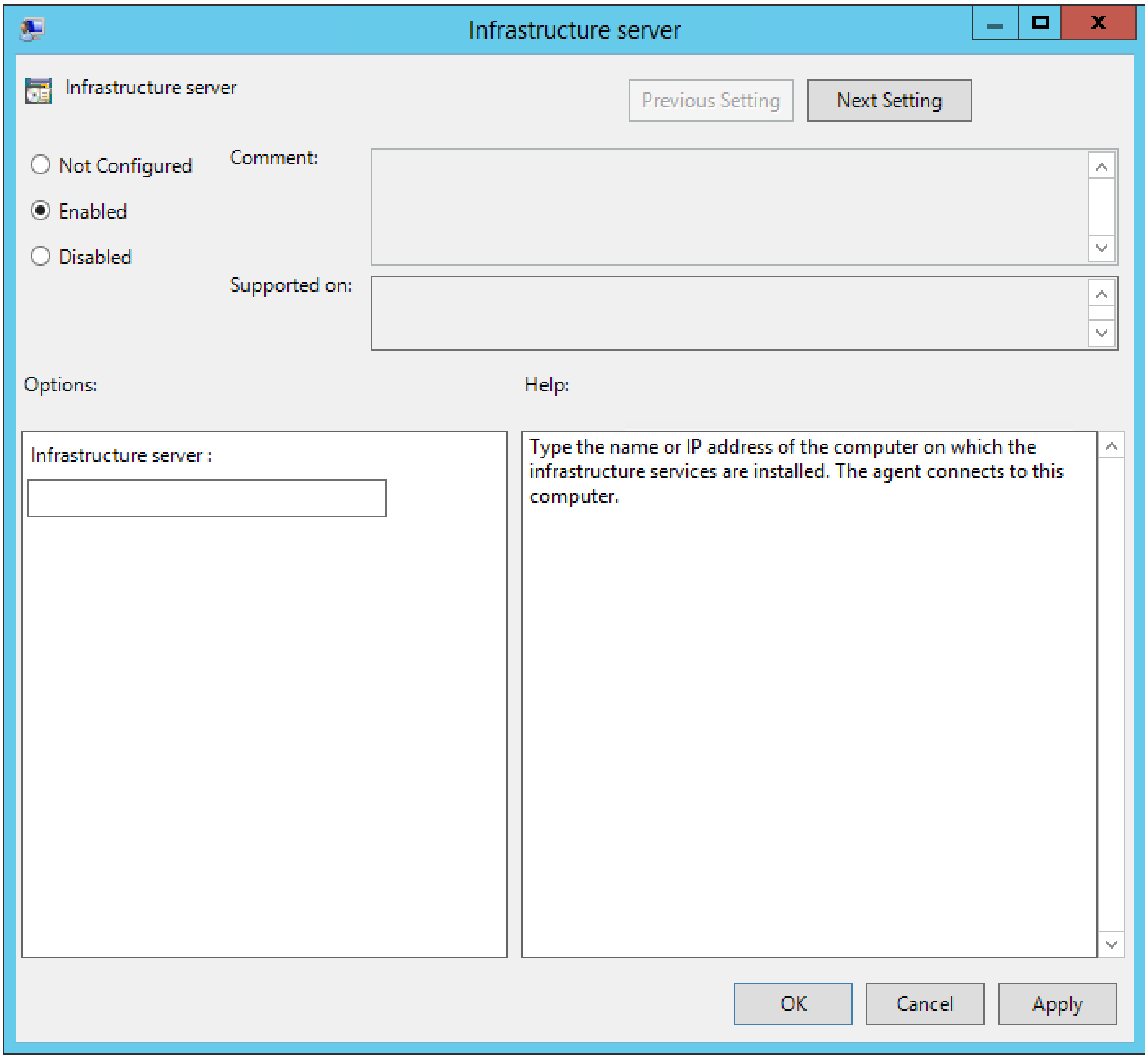
Current Policy Templates:

Name	Size	Modified
Citrix Workspace Environment Management...	2KB	3/23/2018 4:26 ...

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



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



○ Not Configured

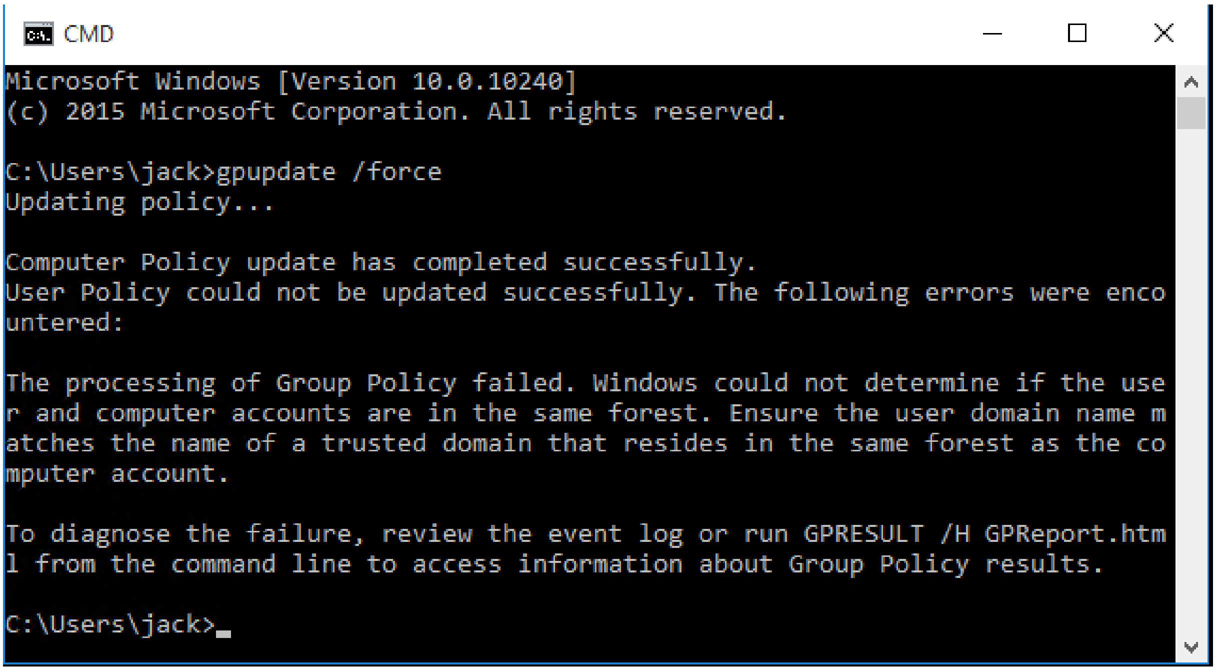
● Enabled

○ Disabled

Infrastructure server :

Type the name or IP address of the computer on which the infrastructure services are installed. The agent connects to this computer.

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

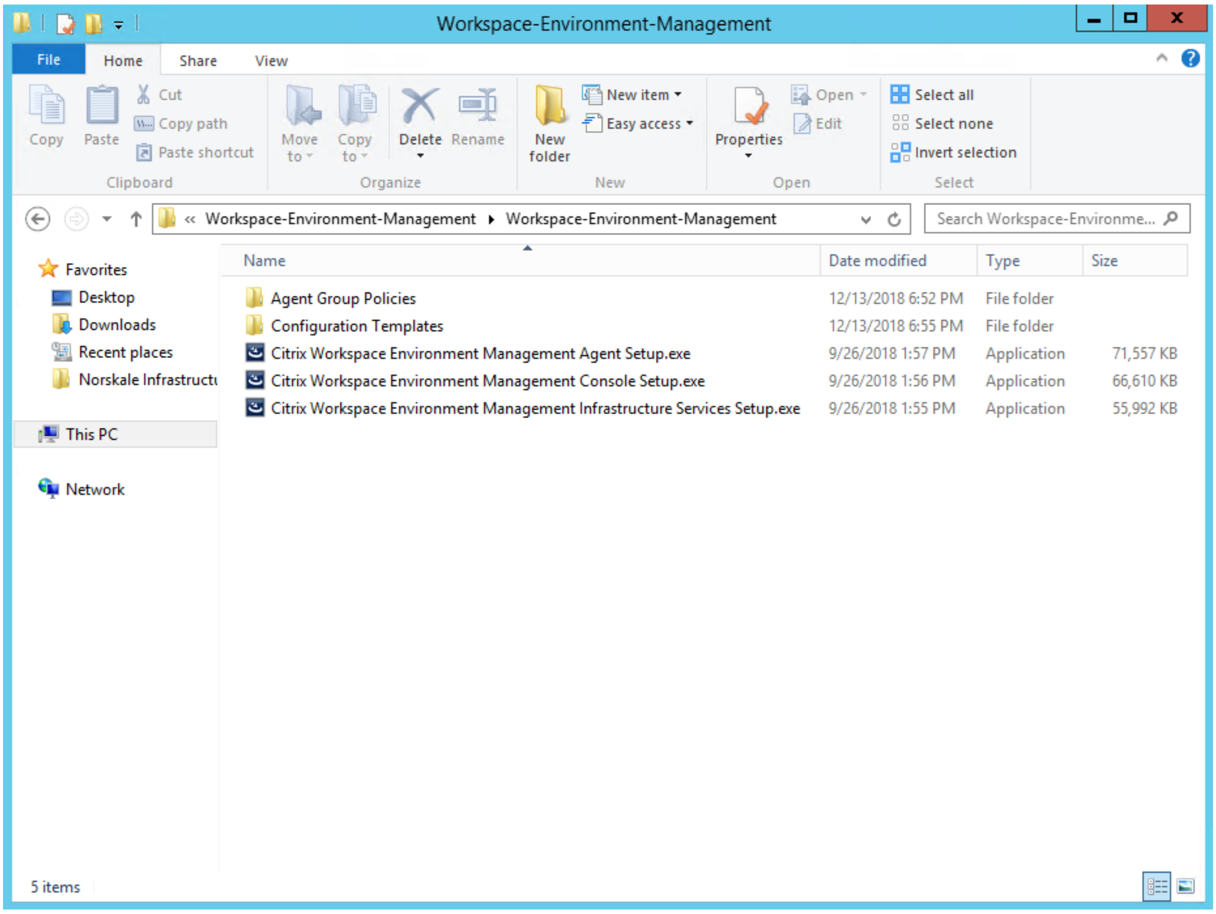


```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\jack>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy could not be updated successfully. The following errors were enco
untered:

The processing of Group Policy failed. Windows could not determine if the use
r and computer accounts are in the same forest. Ensure the user domain name m
atches the name of a trusted domain that resides in the same forest as the co
mputer account.

To diagnose the failure, review the event log or run GPRESULT /H GPReport.htm
l from the command line to access information about Group Policy results.

C:\Users\jack>
```

Step 7: Install the agent

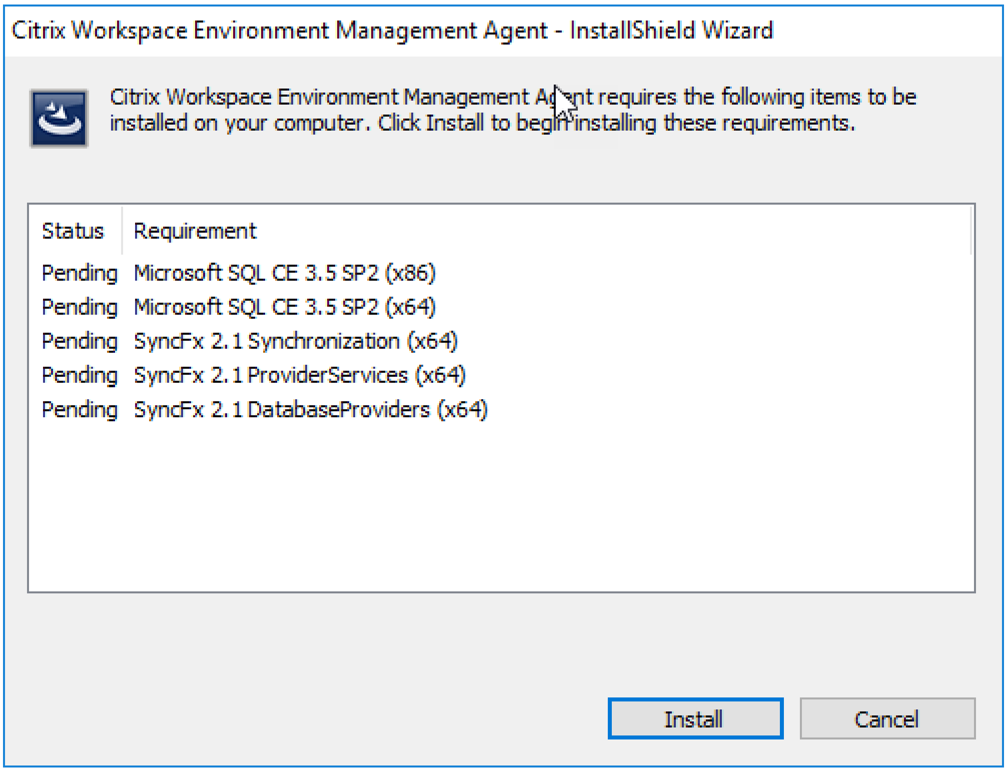
> **Important:**
>
> Do not install the WEM agent on the infrastructure server.

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



Name	Date modified	Type	Size
Agent Group Policies	12/13/2018 6:52 PM	File folder	
Configuration Templates	12/13/2018 6:55 PM	File folder	
Citrix Workspace Environment Management Agent Setup.exe	9/26/2018 1:57 PM	Application	71,557 KB
Citrix Workspace Environment Management Console Setup.exe	9/26/2018 1:56 PM	Application	66,610 KB
Citrix Workspace Environment Management Infrastructure Services Setup.exe	9/26/2018 1:55 PM	Application	55,992 KB

2. Click **Install**.

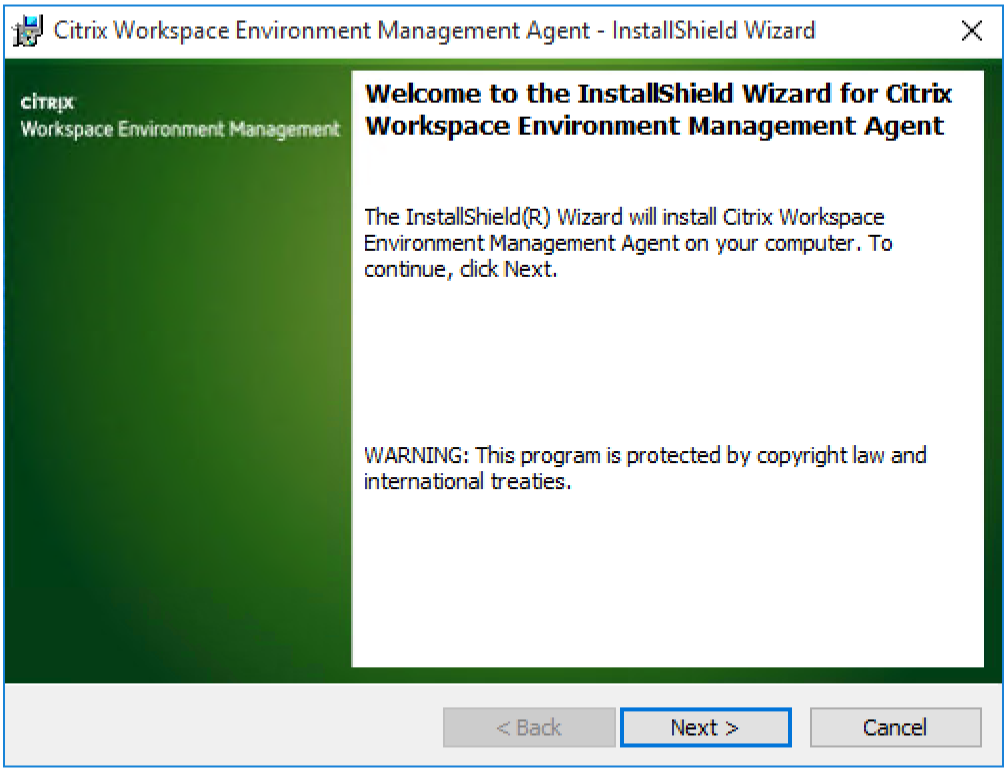


Citrix Workspace Environment Management Agent - InstallShield Wizard

Citrix Workspace Environment Management Agent requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	Microsoft SQL CE 3.5 SP2 (x86)
Pending	Microsoft SQL CE 3.5 SP2 (x64)
Pending	SyncFx 2.1 Synchronization (x64)
Pending	SyncFx 2.1 ProviderServices (x64)
Pending	SyncFx 2.1 DatabaseProviders (x64)

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



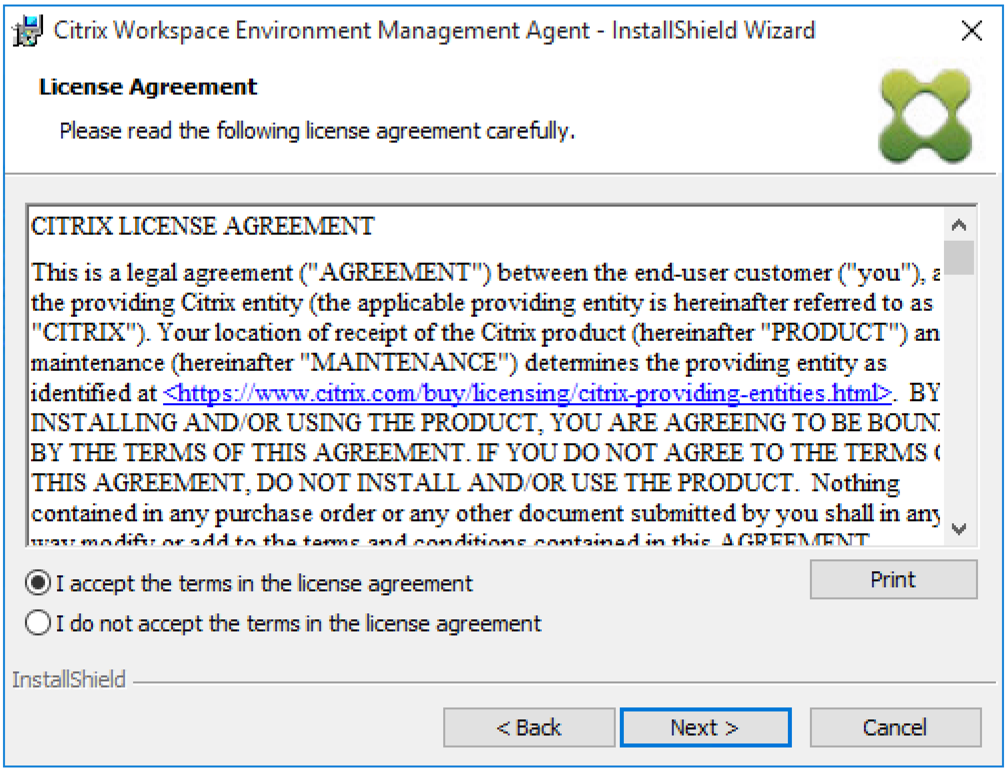
Citrix Workspace Environment Management Agent - InstallShield Wizard

Welcome to the InstallShield Wizard for Citrix Workspace Environment Management Agent

The InstallShield(R) Wizard will install Citrix Workspace Environment Management Agent on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

4. On the License agreement page, select "I accept the terms in the license agreement" and then click **Next**.



Citrix Workspace Environment Management Agent - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

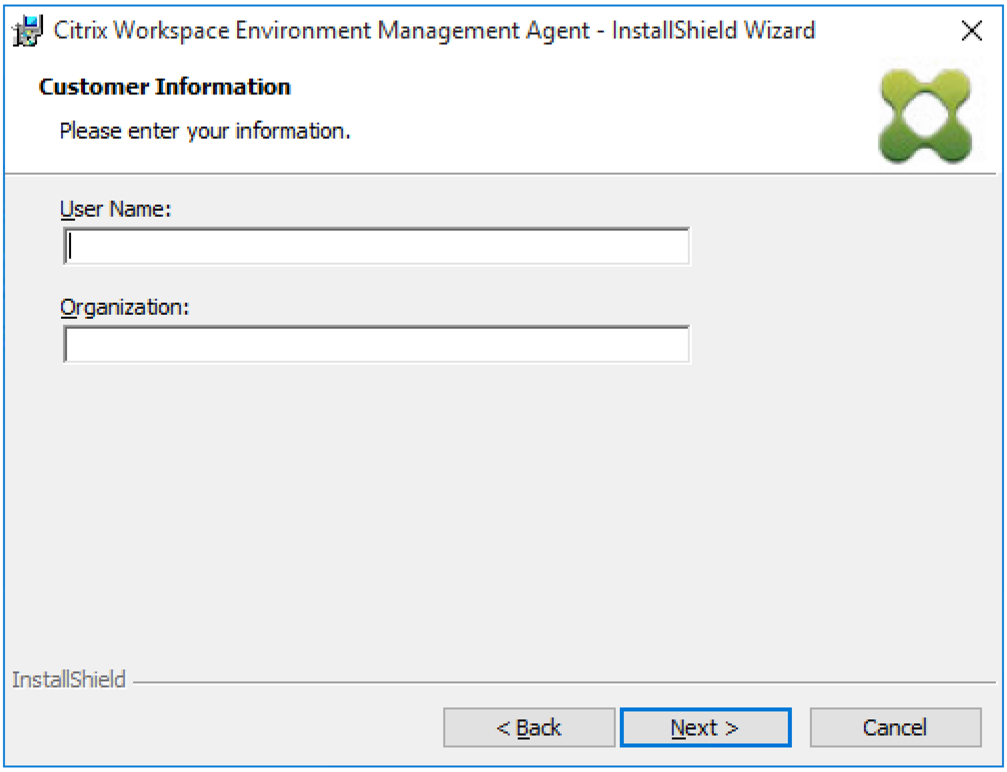
CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), a
the providing Citrix entity (the applicable providing entity is hereinafter referred to as
"CITRIX"). Your location of receipt of the Citrix product (hereinafter "PRODUCT") an
maintenance (hereinafter "MAINTENANCE") determines the providing entity as
identified at <https://www.citrix.com/buy/licensing/citrix-providing-entities.html>. BY
INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUN
BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS (
THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing
contained in any purchase order or any other document submitted by you shall in any
way modify or add to the terms and conditions contained in this AGREEMENT

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

5. On the Customer Information page, type the required information and then click **Next**.



Citrix Workspace Environment Management Agent - InstallShield Wizard

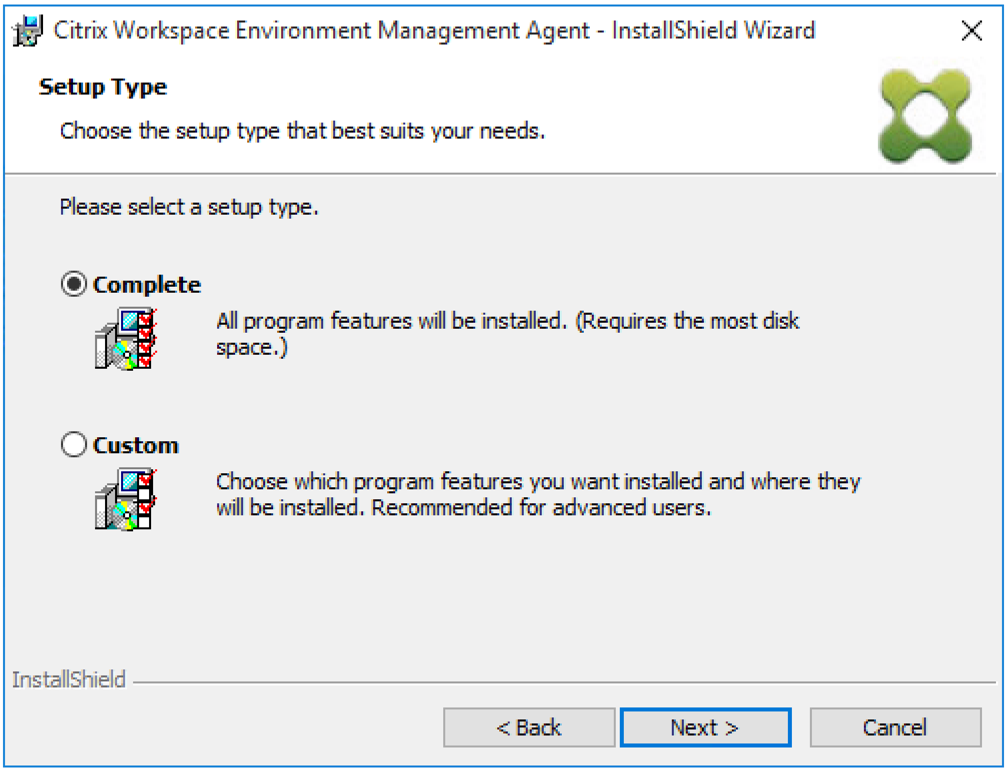
Customer Information

Please enter your information.

User Name:

Organization:

6. On the Setup Type page, select **Complete** and then click **Next**.



Citrix Workspace Environment Management Agent - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

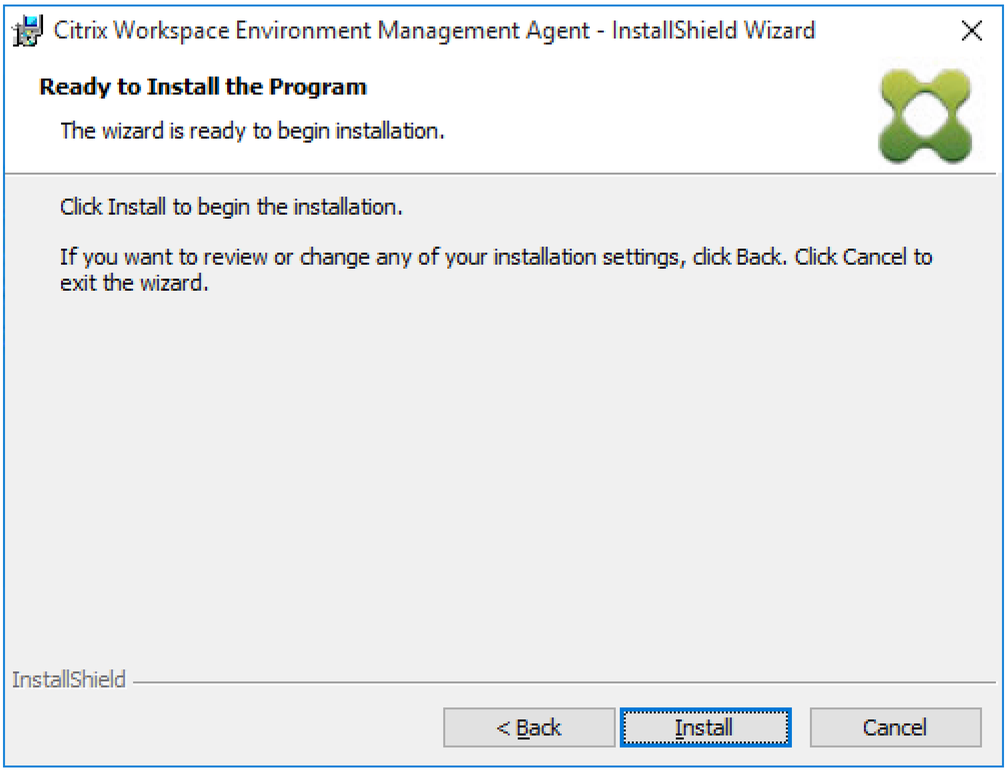
● **Complete**

All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

7. On the Ready to Install the Program page, click **Install**.



Citrix Workspace Environment Management Agent - InstallShield Wizard

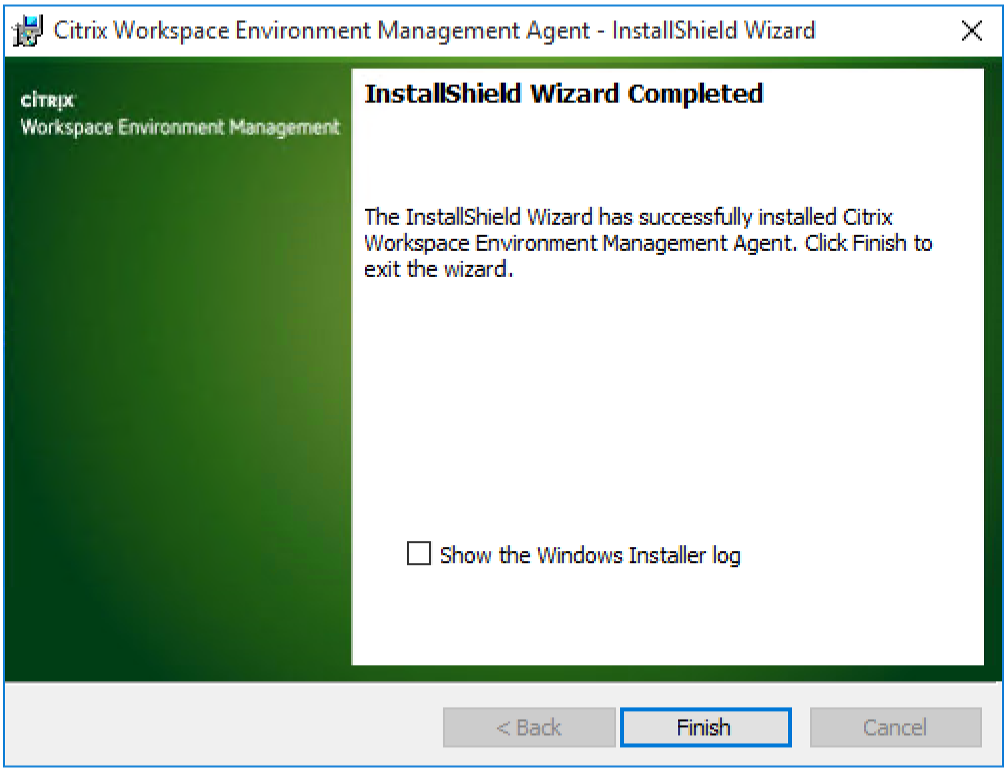
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

8. Click **Finish** to exit the wizard.



Citrix Workspace Environment Management Agent - InstallShield Wizard
citrix
Workspace Environment Management

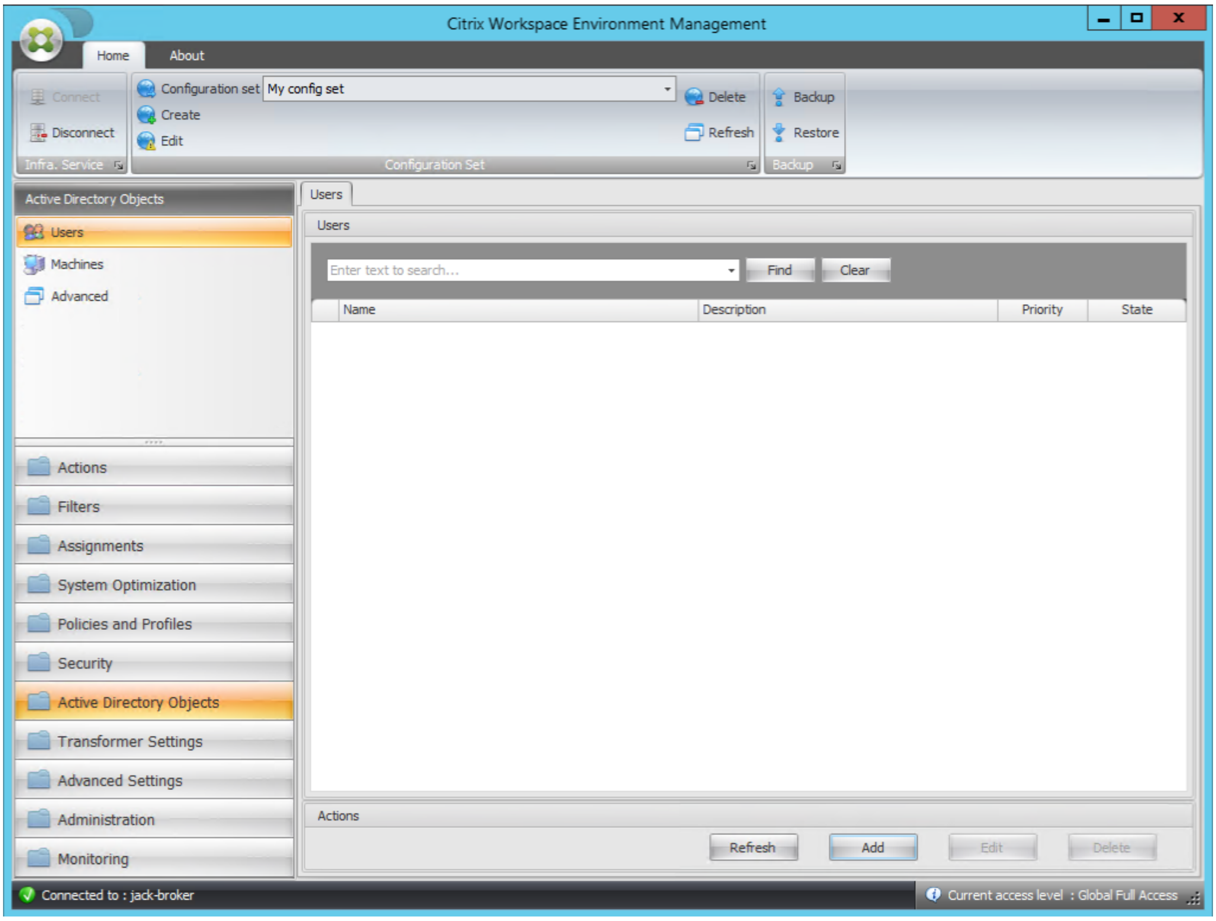
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Citrix Workspace Environment Management Agent. Click Finish to exit the wizard.

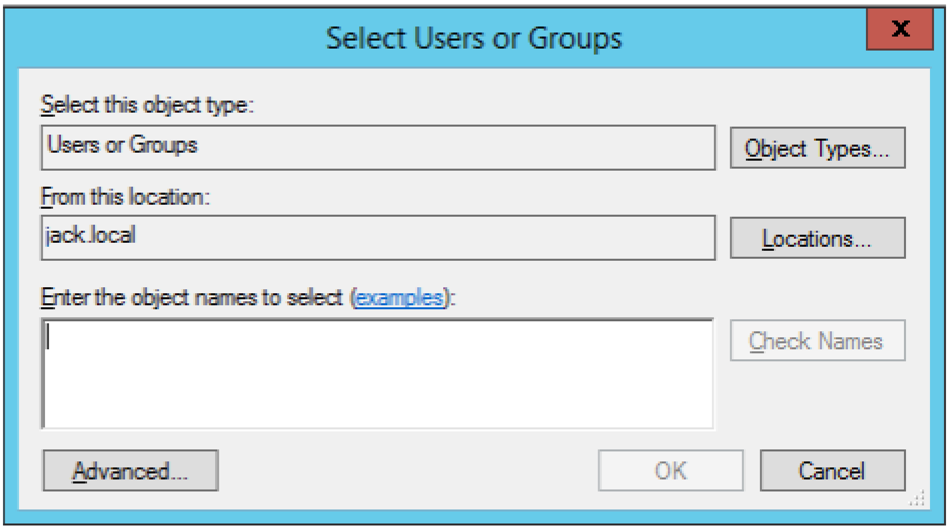
□ Show the Windows Installer log

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

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

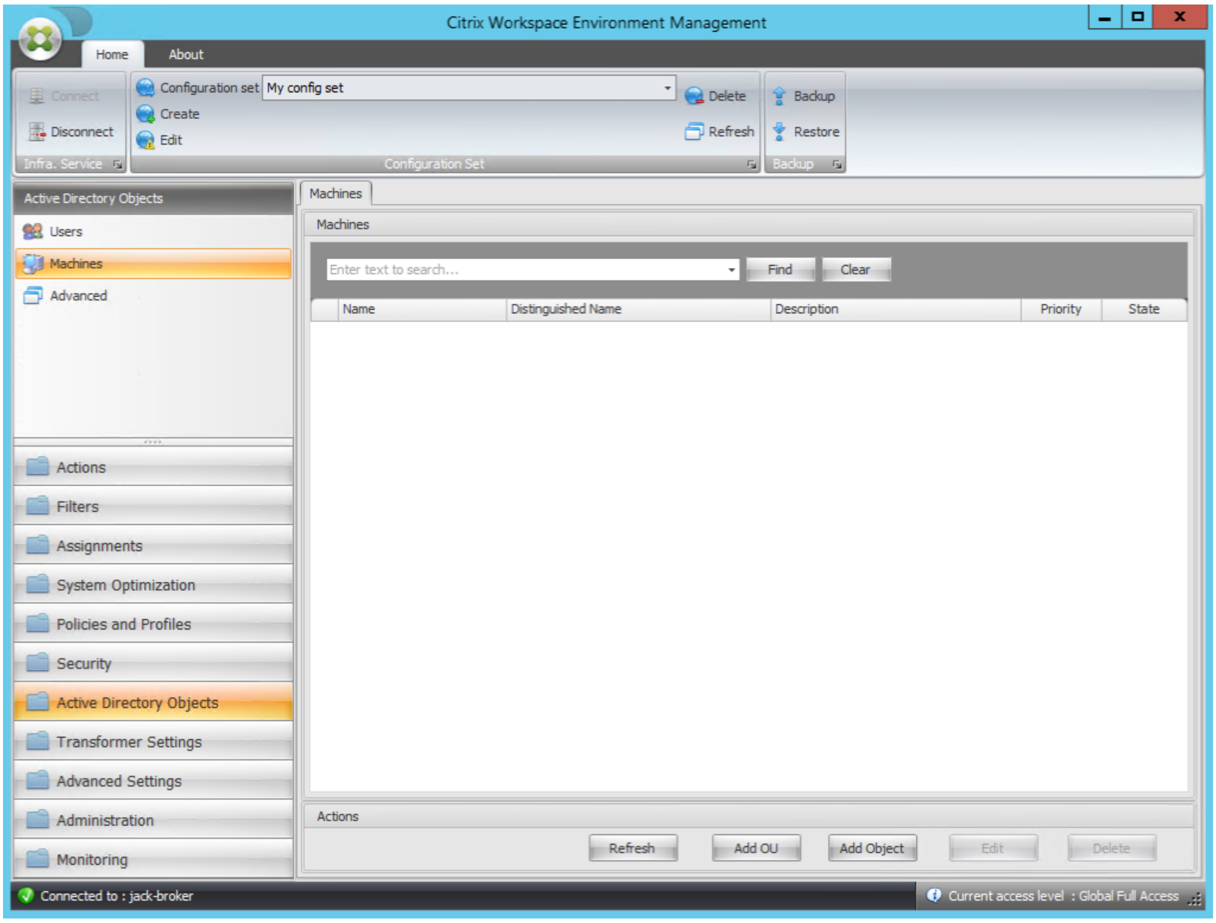


2. In the Select Users or Groups window, type the name, click **Check Names**, and then click **OK**.



Select this object type:
Users or Groups
From this location:
jack.local
Enter the object names to select (examples):

3. Click **Machines**.



Configuration set My config set

Connected to : jack-broker

Current access level : Global Full Access

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

System requirements

April 1, 2019

> **Note:**
>
> Learn about product name changes here.

Software prerequisites

.NET Framework 4.5.2 or later. This is the required by all Workspace Environment Management components.

Microsoft SQL Server Compact 3.5 SP2: SQL Server Compact is used by Workspace Environment Management to cache settings, primarily for use in offline mode. It must be installed on the infrastructure server. Install SQL Server Compact on any agent environment to allow the agent to cache settings and run when it is in offline mode. If SQL Server Compact is not already installed, it is installed during infrastructure services installation.

Microsoft Sync Framework 2.1. This is necessary for all Workspace Environment Management components. If not already installed, this prerequisite is installed during installation.

Microsoft SQL Server 2008 R2 or later: Workspace Environment Management requires **sysadmin access** to a SQL Server instance to create its database, and read/write access to this database to use it. The SQL Server instance must use case-insensitive collation, otherwise database creation or upgrade will fail.

Microsoft Active Directory: Workspace Environment Management requires **read access** to your Active Directory to push configured settings out to users. **Administrative access** is required to configure the agent.

> **Note:**
>
> - *External trust* relationships are not supported by WEM's global catalog, which stores a copy of all Active Directory objects in a forest. Instead you must use other relationship types, such as *forest trust* relationships.
> - WEM also does not support one-way forest trust relationship between forests.

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

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

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

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

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

Operating system prerequisites

Infrastructure services

Supported operating systems:

- Windows Server 2012 R2 Standard and Datacenter editions
- Windows Server 2016 Standard and Datacenter editions
- Windows Server 2019 Standard and Datacenter editions

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

Administration console

Supported operating systems:

- Windows 10 version 1607 and newer, 32- and 64-bit
- Windows Server 2012 R2 Standard and Datacenter editions
- Windows Server 2016 Standard and Datacenter editions
- Windows Server 2019 Standard and Datacenter editions

Agent

Supported operating systems:

- Windows 7 SP1 Professional, Enterprise, and Ultimate editions, 32- and 64-bit
- Windows 8.1 Professional, and Enterprise editions, 32- and 64-bit
- Windows 10 version 1607 and newer, 32- and 64-bit
- Windows Server 2008 R2 SP1 Standard, Enterprise, and Datacenter editions*
- Windows Server 2012 Standard and Datacenter editions*
- Windows Server 2012 R2 Standard and Datacenter editions*
- Windows Server 2016 Standard and Datacenter editions*
- Windows Server 2019 Standard and Datacenter editions*

* The Transformer feature is not supported on server operating systems.

In WEM 4.4, Windows XP was supported.

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

SQL Server Always On

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

Always On availability groups allows databases to automatically fail over if the hardware or software of a principal or primary SQL Server fails, which ensures that Workspace Environment Management continues to work as expected. The Always On availability groups feature requires that the SQL Server instances reside on the Windows Server failover Cluster (WSFC) nodes. For more information, see http://msdn.microsoft.com/en-us/library/hh510230.

To use Workspace Environment Management by using Always On availability groups:

1. Create an empty SQL database on your primary SQL Server and back it up.
2. Create the Workspace Environment Management database. Take care to:
   - choose option **Set vuemUser SQL user account password** and type a password for the vuemUser SQL user account. You need to provide this password when you add the database to the availability group.
   - for "Server and instance name", type the name of the availability group listener.
3. Add the Workspace Environment Management database to an availability group.

Before upgrading a Workspace Environment Management database which is deployed in an SQL Server Always On availability group, remove it from the availability group.

Hardware prerequisites

Infrastructure services (for up to 3,000 users): 4 vCPUs, 8 GB RAM, 80 GB of available disk space.

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

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

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

Service dependencies

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

Antivirus exclusions

Workspace Environment Management agent and infrastructure services are installed in the following default directories:

- C:\Program Files (x86)\Norskale\Norskale Agent Host (on 64-bit OS)
- C:\Program Files\Norskale\Norskale Agent Host (on 32-bit OS)
- C:\Program Files (x86)\Norskale\Norskale Infrastructure Services

On-access scanning must be disabled for the entire "Norskale" installation directory for both the Workspace Environment Management agent and infrastructure services. When this is not possible, the following processes must be excluded from on-access scanning:

In the infrastructure services installation directory

- Norskale Broker Service.exe
- Norskale Broker Service Configuration Utility.exe
- Norskale Database Management Utility.exe

In the agent installation directory

- Norskale Agent Host Service.exe
- VUEMUIAgent.exe
- Agent Log Parser.exe
- AgentCacheUtility.exe
- AppsMgmtUtil.exe
- PrnsMgmtUtil.exe
- VUEMAppCmd.exe
- VUEMAppCmdDbg.exe
- VUEMAppHide.exe
- VUEMCmdAgent.exe
- VUEMMaintMsg.exe
- VUEMRSAV.exe

Install and configure

September 4, 2018

> **Note:**
>
> Learn about product name changes here.

Install and configure the following components:

- Infrastructure services
- Administration console
- Agent

Infrastructure services

February 26, 2019

There is currently one Windows infrastructure service:

Norskale Infrastructure Service (NT SERVICE\Norskale Infrastructure Service): Manages WEM Infrastructure services. Account: LocalSystem or specified user account which belongs to the administrator user group on the infrastructure server.

Install the infrastructure services

> **Important:**
>
> - Workspace Environment Management infrastructure services cannot be installed on a domain controller. Kerberos authentication issues prevent the infrastructure service from working in this scenario.
> - Do not install the infrastructure services on the server where the Delivery Controller is installed.
>
> **Usage data collection notice:**
>
> - By default, the infrastructure service collects anonymous analytics on Workspace Environment Management usage each night and sends it immediately to the Google Analytics server via HTTPS. Analytics collection complies with the Citrix Privacy Policy.
> - Data collection is enabled by default when you install or upgrade the infrastructure service. To opt out, in the WEM Infrastructure Service Configuration dialog **Advanced Settings** tab, select the option **Do not help improve Workspace Environment Management using**

> **Google Analytics**.

To Install the infrastructure services, run **Citrix Workspace Environment Management Infrastructure Services Setup.exe** on your infrastucture server. The "Complete" setup option installs the PowerShell SDK module by default. You can use the "Custom" setup option to prevent SDK installation, or to change the installation folder. The infrastructure services install into the following default folder: C:\Program Files (x86)\Norskale\Norskale Infrastructure Services. The PowerShell SDK module installs into the following default folder: C:\Program Files (x86)\Norskale\Norskale Infrastructure Services\SDK. For SDK documentation see Citrix Developer Documentation.

You can customize your installation using the following arguments:

AgentPort: The infrastructure services setup runs a script that opens firewall ports locally, to ensure that the agent network traffic is not blocked. The AgentPort argument allows you to configure which port is opened. The default port is 8286. Any valid port is an accepted value.

AgentSyncPort: The infrastructure services setup runs a script that opens firewall ports locally, to ensure that the agent network traffic is not blocked. The AgentSyncPort argument allows you to configure which port is opened. The default port is 8285. Any valid port is an accepted value.

AdminPort: The infrastructure services setup program runs a script that opens firewall ports locally, to ensure that the agent network traffic is not blocked. The AdminPort argument allows you to configure which port is opened. The default port is 8284. Any valid port is an accepted value.

The syntax for these install arguments is:

```
”path:\\to\\Citrix Workspace Environment Management Infrastructure Services
 Setup.exe”/v”argument1=\\”value1\\”argument2=\\”value2\\””
```

Create SPNs

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

After the installer finishes, create a Service Principal Name (SPN) for the infrastructure service. In Workspace Environment Management, connection and communication between agent, infrastructure service, and domain controller are authenticated by Kerberos. SPNs are used by Kerberos authentication to associate a service instance with a service logon account. The relationship must be configured between the logon account of the infrastructure service instance and the account registered with the SPN. Therefore, to align with the Kerberos authentication requirements, you must configure the WEM SPN to associate it with a known AD account. Use the command that is applicable to your environment:

- You do not use Windows authentication or load balancing:

setspn -C -S Norskale/BrokerService [*hostname*]

where [*hostname*] is the name of the infrastructure server.

- You use Windows authentication or you use load balancing (which requires Windows authentication):

setspn -U -S Norskale/BrokerService [*accountname*]

where [*accountname*] is the name of the service account that is being used for Windows authentication.

SPNs are case-sensitive.

Configure load balancing

To configure Workspace Environment Management with a load balancing service:

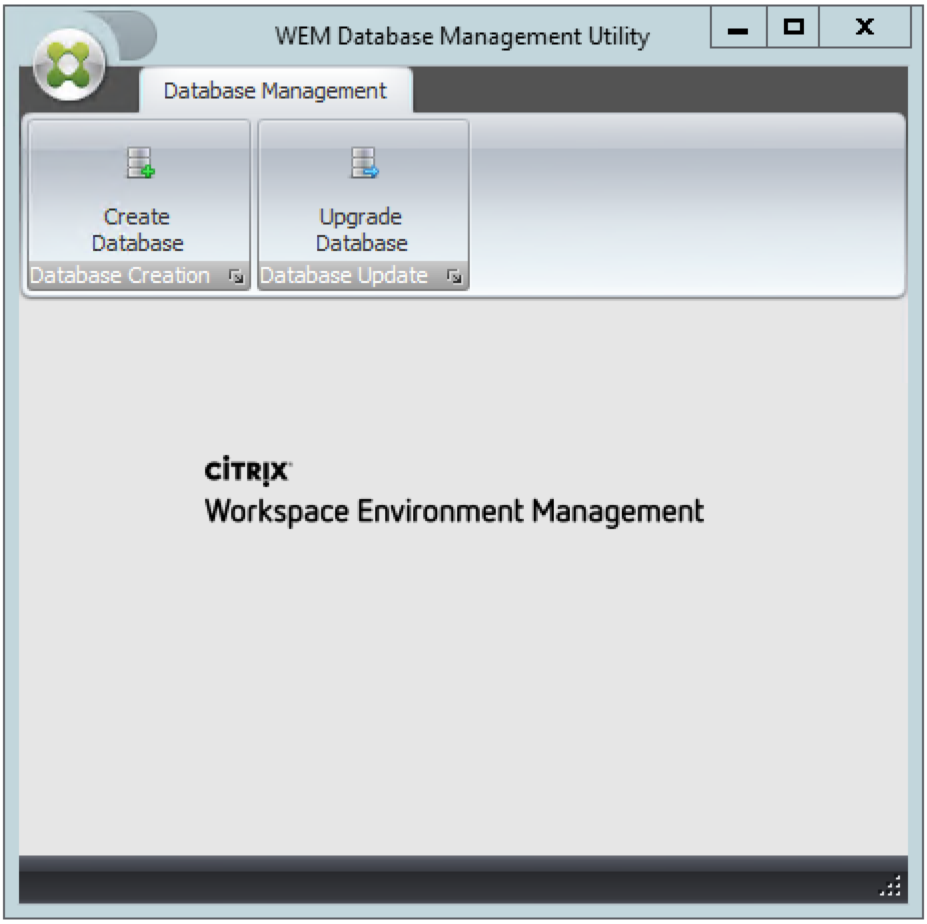
1. Create a Windows infrastructure service account for the Workspace Environment Management infrastructure service to connect to the Workspace Environment Management database.
2. When you create the Workspace Environment Management database, select the option **Use Windows authentication for infrastructure service database connection** and specify the infrastructure service account name. [See Create a Workspace Environment Management database.]
3. Configure each infrastructure service to connect to the SQL database using Windows authentication instead of SQL authentication: select the option **Enable Windows account impersonation** and provide the infrastructure service account credentials. [See Configure the Infrastructure Service.]
4. Configure the Service Principal Names (SPNs) for the Workspace Environment Management infrastructure services to use the infrastructure service account name. [See Create SPNs.]
5. Create a virtual IP address (VIP) that covers the number of infrastructure servers you want to put behind a VIP. All the infrastructure servers covered by a VIP are eligible when agents connect to the VIP.
6. When you configure the Agent Host Configuration GPO, set the infrastructure server setting to the VIP instead of the address for any individual infrastructure server. [See Configure the agent.]
7. Session persistence is required for the connection between administration consoles and the infrastructure service. (Session persistence between the agent and the infrastructure service is not required.) Citrix recommends that you directly connect each administration console to an infrastructure service server, rather than using the VIP.

Create a Workspace Environment Management database

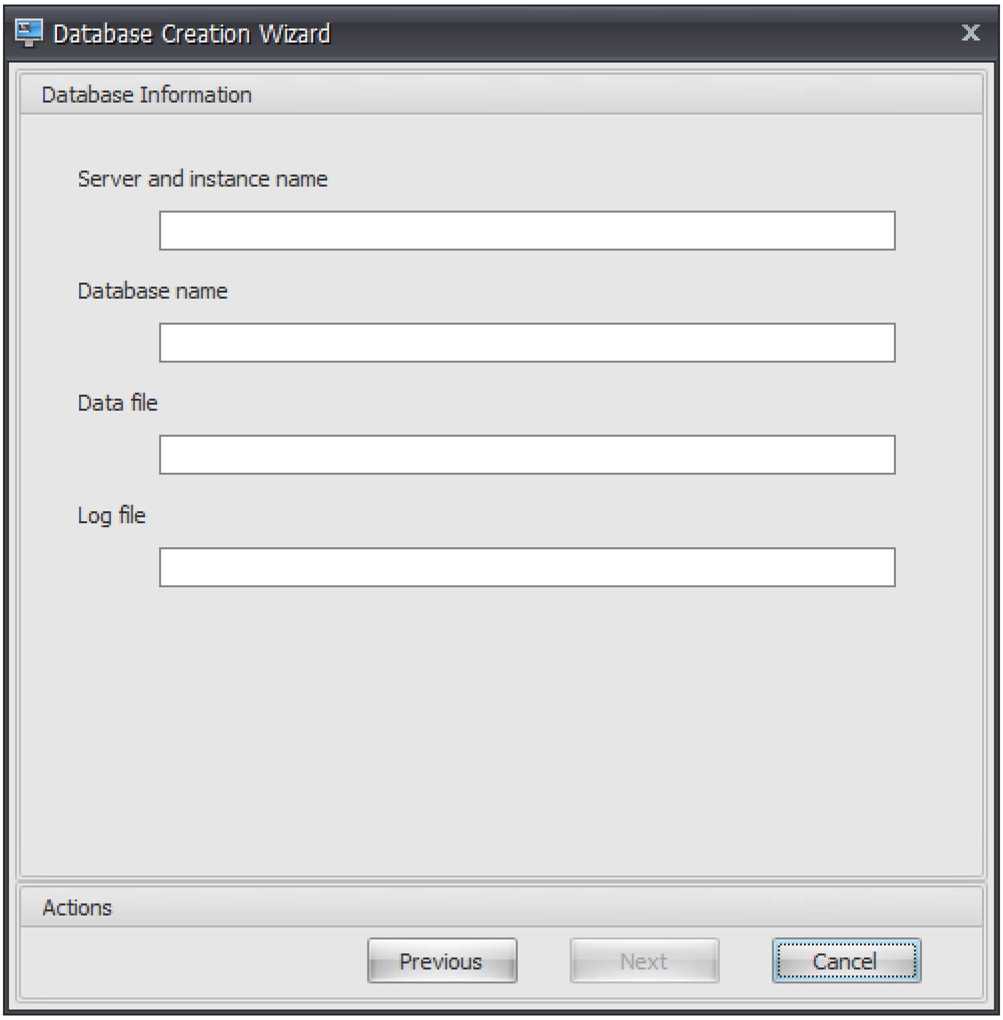
> **Tip:**
>
> You can also create the database using the Workspace Environment Management PowerShell SDK module. For SDK documentation see Citrix Developer Documentation.
>
> **Note:**
>
> - If you are using Windows authentication for your SQL Server, run the database creation utility under an identity that has sysadmin permissions.
> - Citrix recommends that you configure the primary file (.mdf file) of the WEM database with a default size of 50 MB.

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

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



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



Database Creation Wizard

Database Information

Server and and instance name

Database name

Data file

Log file

Actions

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

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

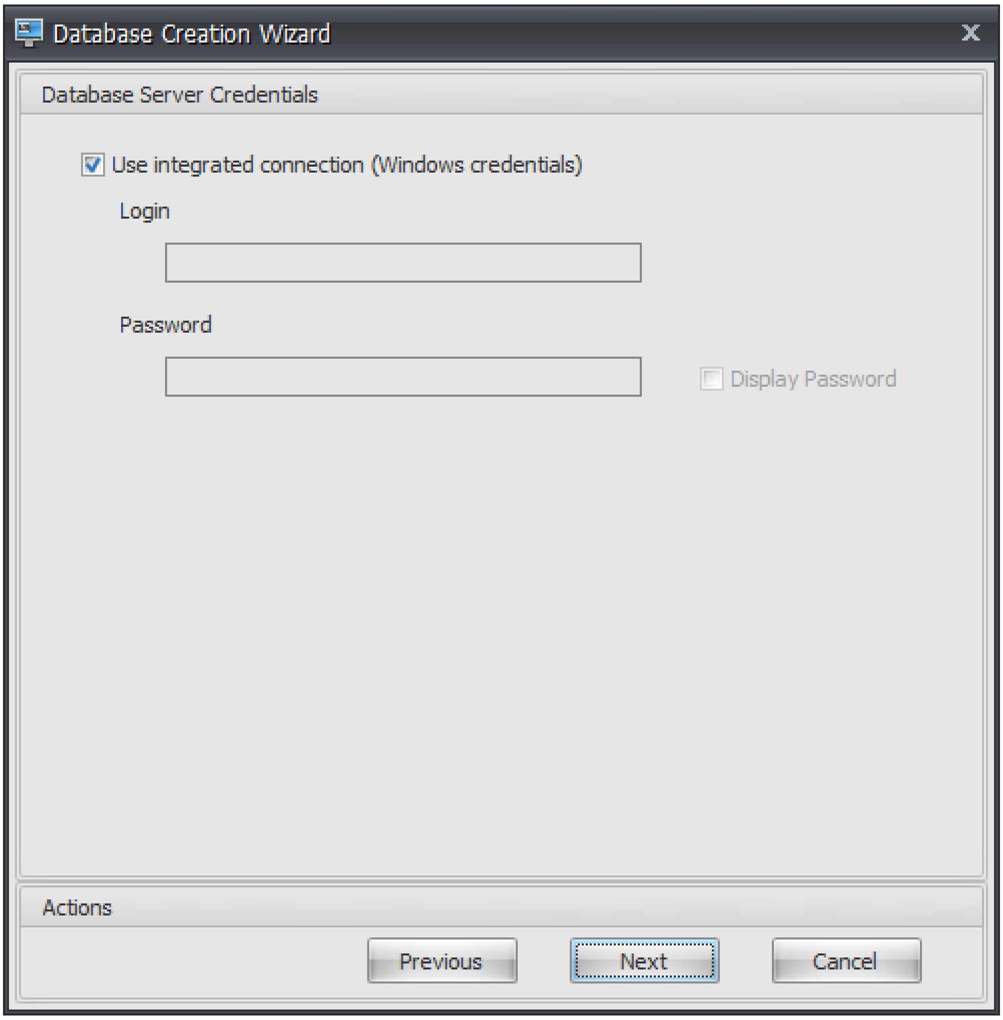
Database name. Name of the SQL database to create.

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

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

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

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



☑ Use integrated connection (Windows credentials)

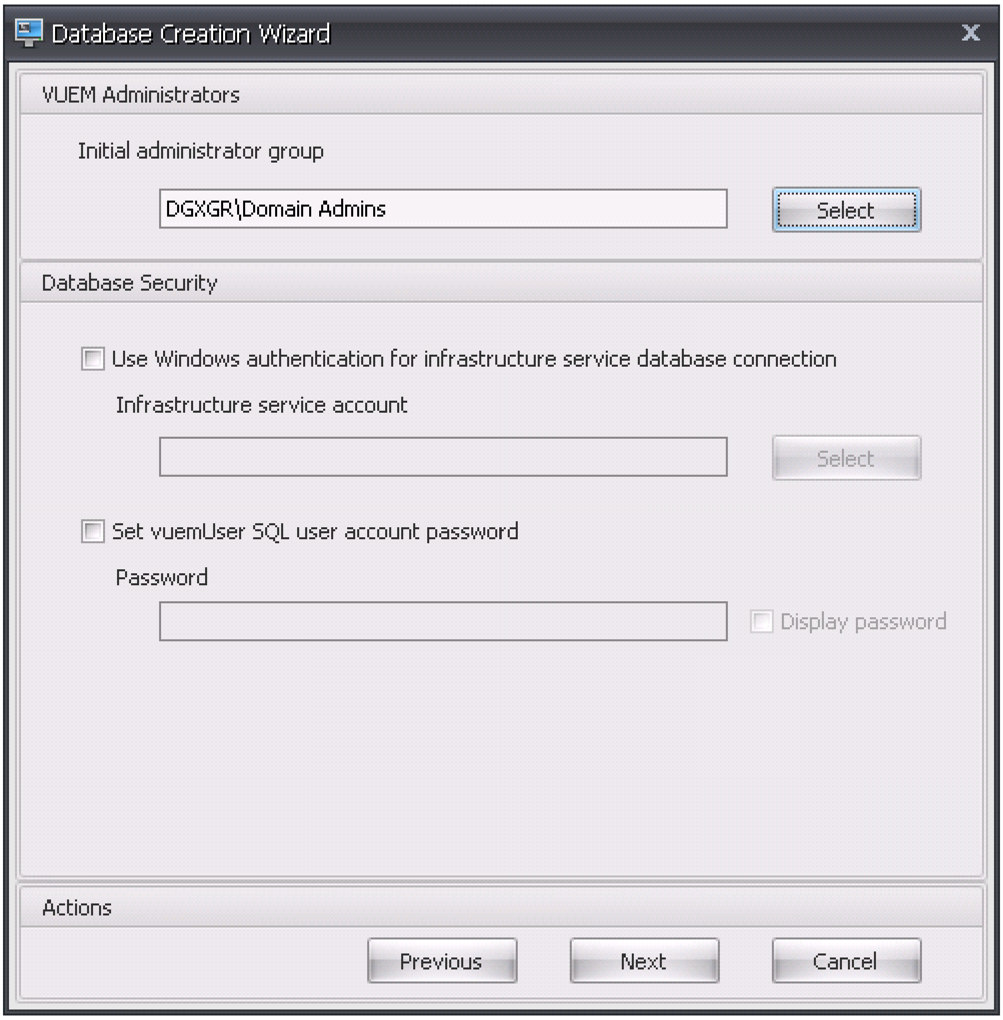
Login

Password

□ Display Password

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

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



Database Creation Wizard

VUEM Administrators

Initial administrator group: DGXGR\Domain Admins

Database Security

□ Use Windows authentication for infrastructure service database connection

Infrastructure service account:

□ Set vuemUser SQL user account password

Password:

□ Display password

Actions

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

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

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

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

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

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

6. In the summary pane, review the settings you have selected, and when you are satisfied click **Create Database**.

7. When you are notified that the database creation has completed successfully, click **Finish** to exit the wizard.

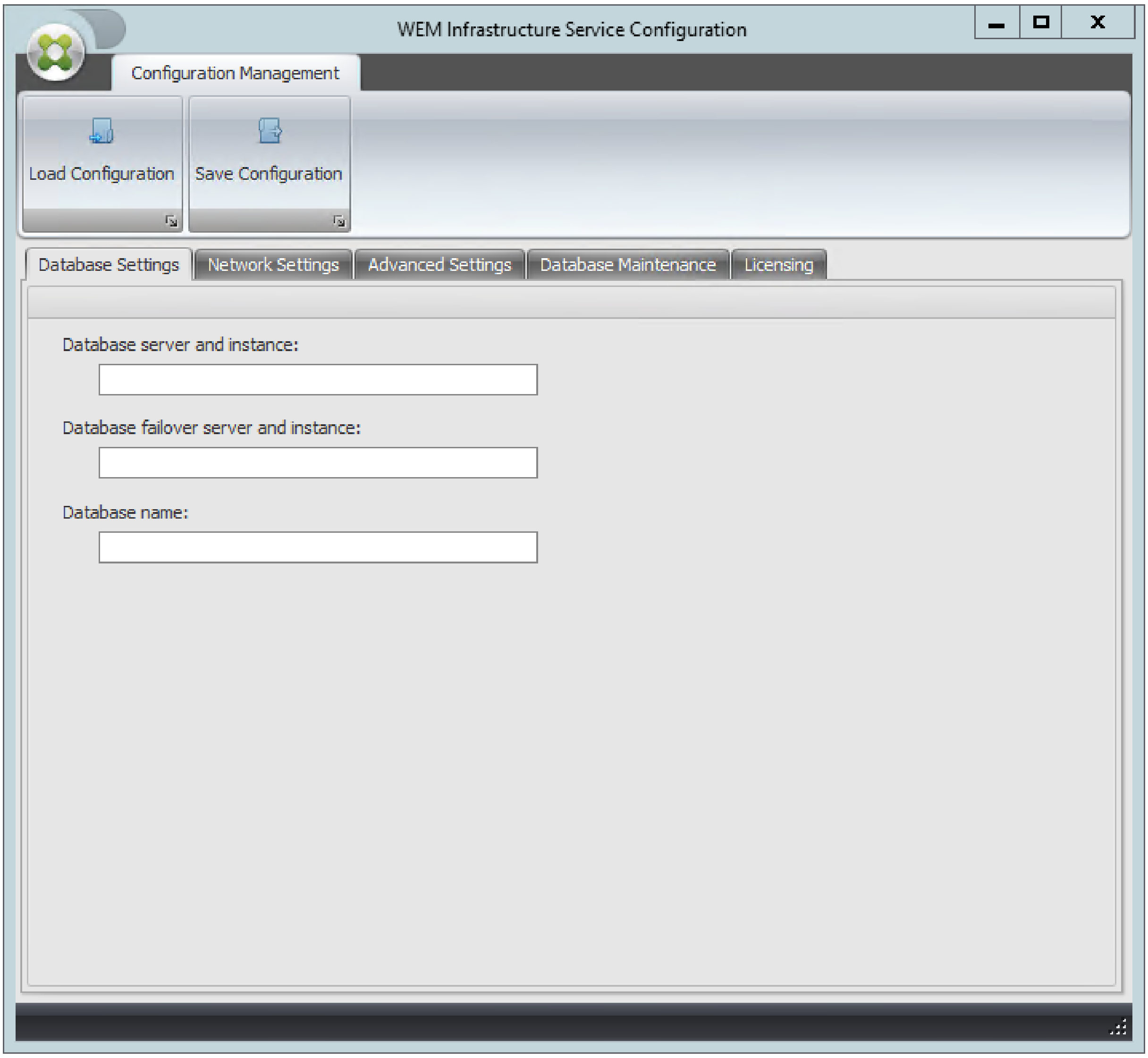
If an error occurs during the database creation, check the log file "Citrix WEM Database Management Utility Debug Log.log" in the infrastructure services installation directory.

Configure the infrastructure service

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

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

1. From the **Start** menu select **Citrix>Workspace Environment Management>WEM Infrastructure Service Configuration Utility**.



Database server and instance:

Database failover server and instance:

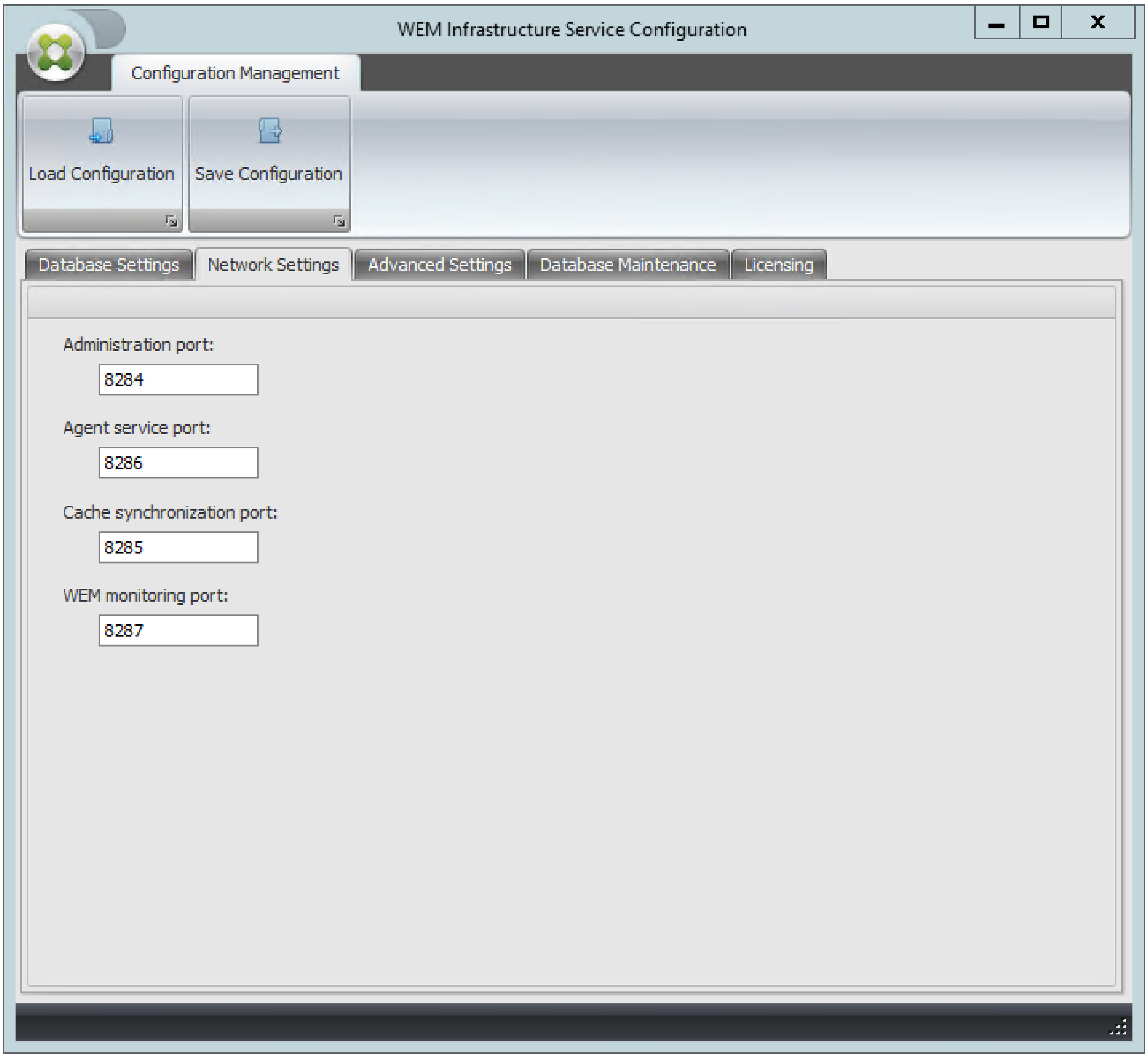
Database name:

2. In the **Database Settings** tab enter the following details:

Database server and instance. Address of the SQL Server instance on which the Workspace Environment Management database is hosted. This must be reachable exactly as typed from the infrastructure server. Specify a full instance address as “serveraddress,port\instancename”. If port is unspecified the default SQL port number (1433) is used.

Database failover server and instance. If you are using database mirroring, specify the failover server address here.

Database name. Name of the Workspace Environment Management database on the SQL instance.



Administration port: 8284

Agent service port: 8286

Cache synchronization port: 8285

WEM monitoring port: 8287

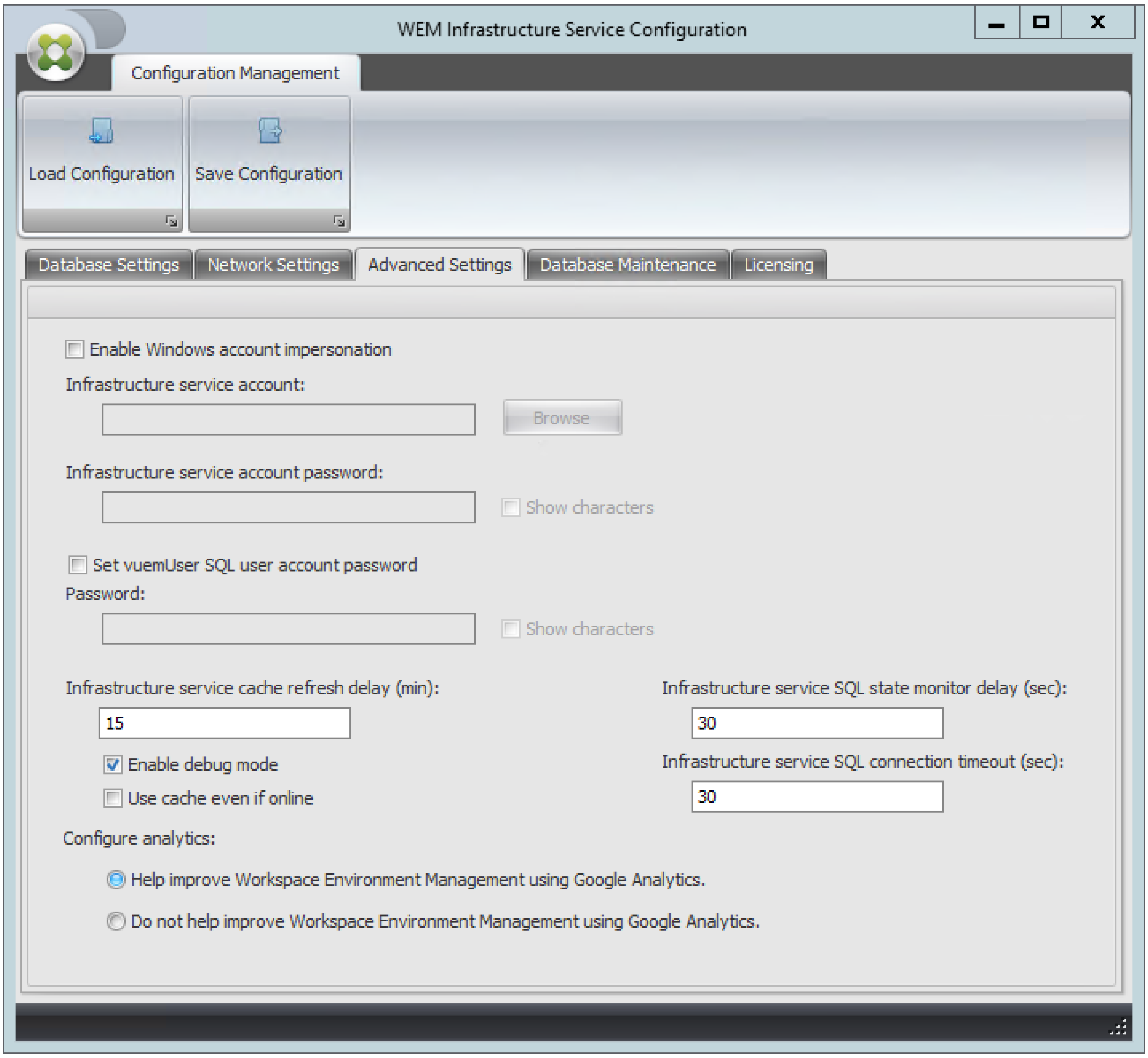
3. In the **Network Settings** tab type the ports the infrastructure service uses:

Administration port. This port is used by the administration console to connect to the infrastructure service.

Agent service port. This port is used by your agent hosts to connect to the infrastructure service.

Cache synchronization port. This port is used by the agent service to synchronize its cache with the infrastructure service.

WEM monitoring port. [Not currently used.]



□ Enable Windows account impersonation

Infrastructure service account:

Infrastructure service account password:

□ Show characters

□ Set vuemUser SQL user account password

Password:

□ Show characters

Infrastructure service cache refresh delay (min): 15

☑ Enable debug mode

□ Use cache even if online

Infrastructure service SQL state monitor delay (sec): 30

Infrastructure service SQL connection timeout (sec): 30

Configure analytics:

● Help improve Workspace Environment Management using Google Analytics.

○ Do not help improve Workspace Environment Management using Google Analytics.

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

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

Set vuemUser SQL user account password. Allows you to inform the infrastructure service of a custom password configured for the *vuemUser* SQL user during database creation. Only enable this option if you provided your own password during database creation.

Infrastructure service cache refresh delay. Time (in minutes) before the infrastructure service refreshes its cache. The cache is used if the infrastructure service is unable to connect to SQL.

Infrastructure service SQL state monitor delay. Time (in seconds) between each infrastructure service attempt to poll the SQL server.

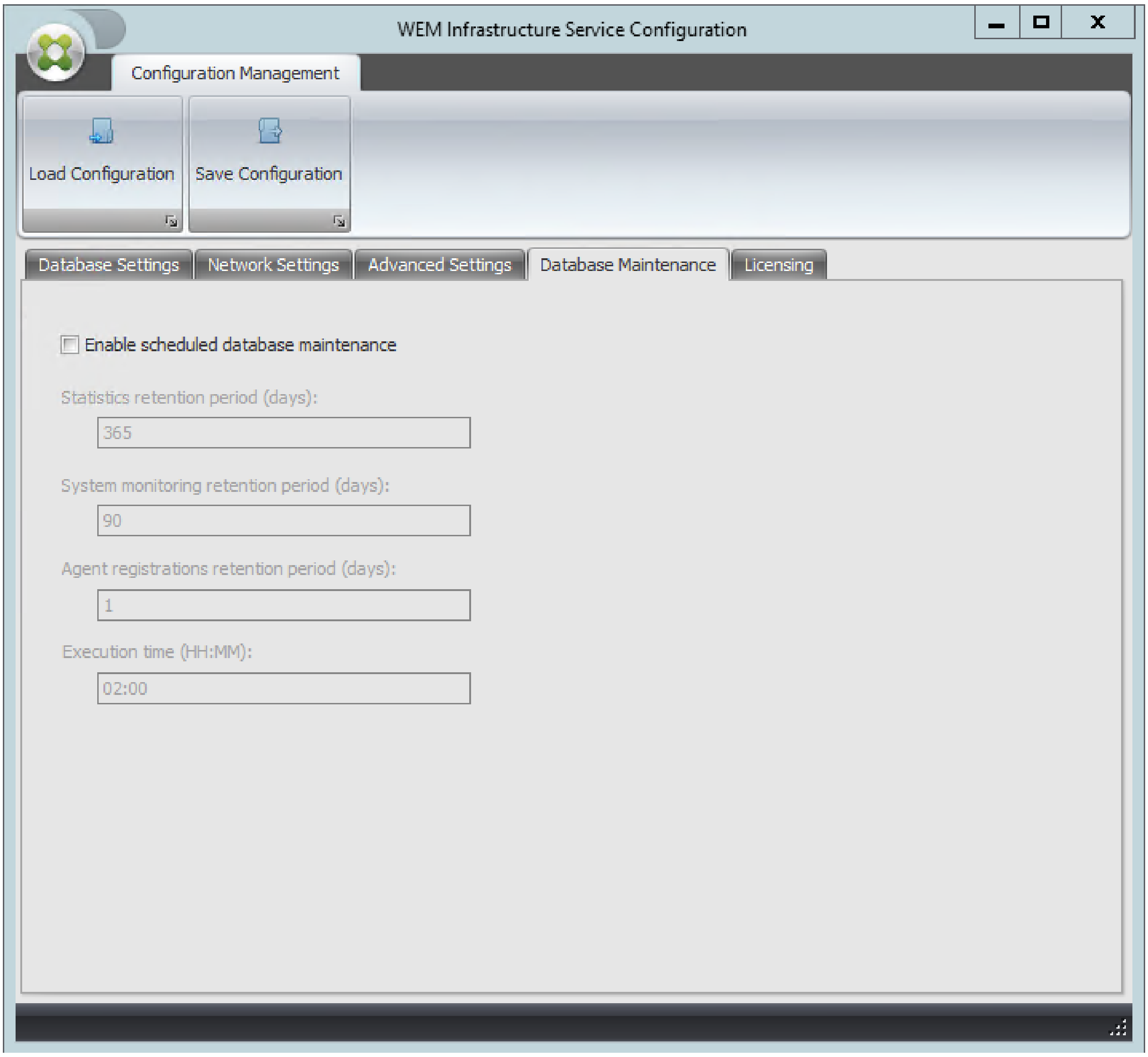
Infrastructure service SQL connection timeout. Time (in seconds) which the infrastructure service waits when trying to establish a connection with the SQL server before terminating the attempt and generating an error.

Enable debug mode. If enabled, the infrastructure service is set to verbose logging mode.

Use cache even if online. If enabled, the infrastructure service always reads site settings from its cache.

Help improve Workspace Environment Management using Google Analytics. If selected, the infrastructure service sends anonymous analytics to the Google Analytics server.

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



□ Enable scheduled database maintenance

Statistics retention period (days): 365

System monitoring retention period (days): 90

Agent registrations retention period (days): 1

Execution time (HH:MM): 02:00

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

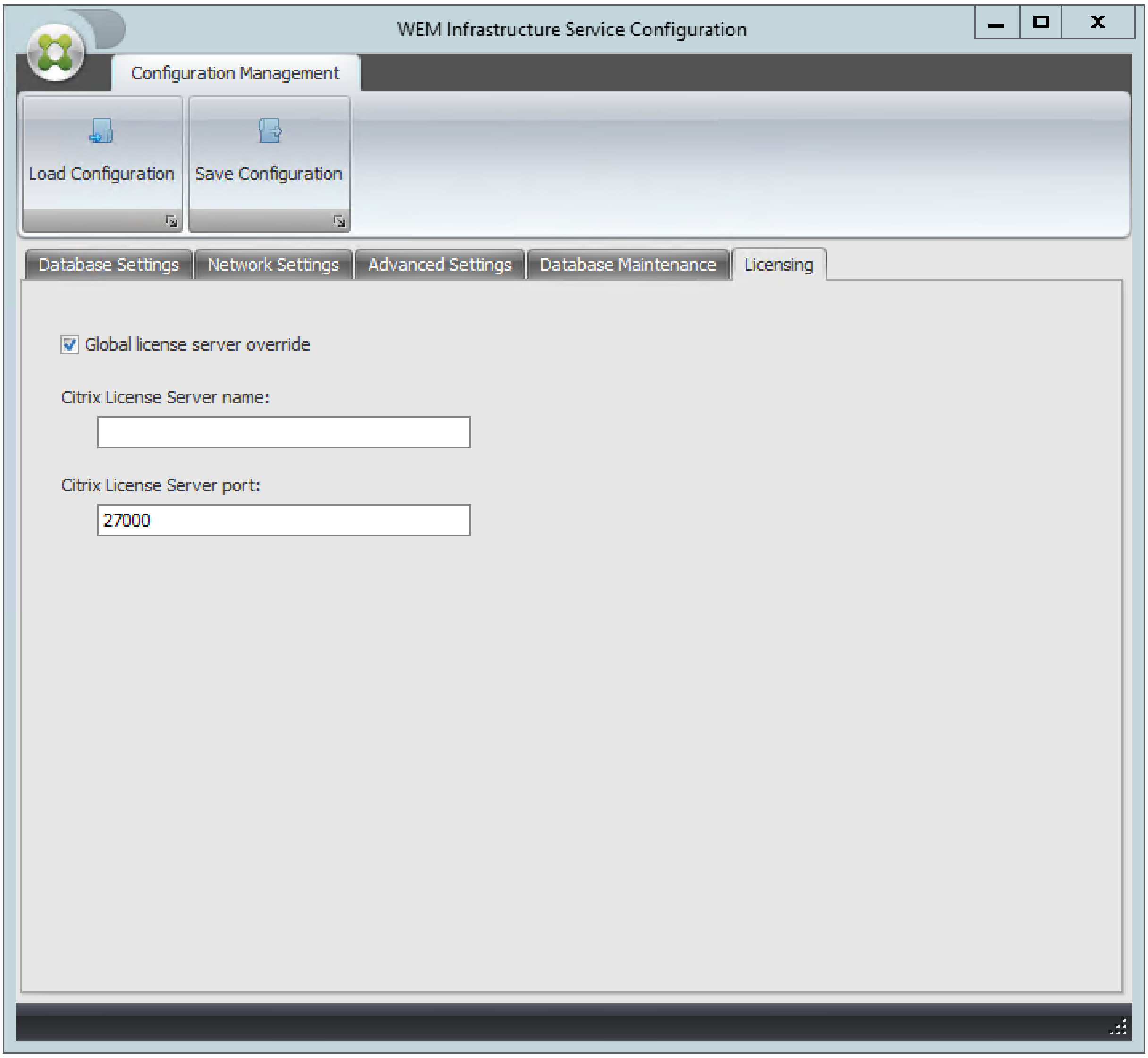
Enable scheduled database maintenance. If enabled, this setting deletes old statistics records from the database at periodic intervals.

Statistics retention period. Determines how long user and agent statistics are retained. Default is 365 days.

System monitoring retention period. Determines how long system optimization statistics are retained. Default is 90 days.

Agent registrations retention period. Determines how long agent registration logs are retained in the database. Default is 1 day.

Execution time. Determines the time at which the database maintenance action is performed. Default is 02:00.



☑ Global license server override

Citrix License Server name:

Citrix License Server port: 27000

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

Global license server override. Enable this option to type the name of the Citrix License Server used by Workspace Environment Management. The information you type here will override any Citrix License Server information already in the Workspace Environment Management database.

After the infrastructure services are configured to your satisfaction, click **Save Configuration** to save these settings and then exit the Infrastructure Services Configuration utility.

Administration console

December 24, 2018

Install the administration console

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

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

You can customize your installation using these arguments:

AgentPort: The administration console setup runs a script that opens firewall ports locally, to make sure the agent network traffic is not blocked. This argument allows you to configure which port is opened. If unspecified, the default port 8286 is used. Accepted values are any valid port.

AdminPort: The administration console setup runs a script that opens firewall ports locally, to make sure the agent network traffic is not blocked. This argument allows you to configure which port is opened. If unspecified, the default port 8284 is used. Accepted values are any valid port.

The syntax for these install arguments is as follows:

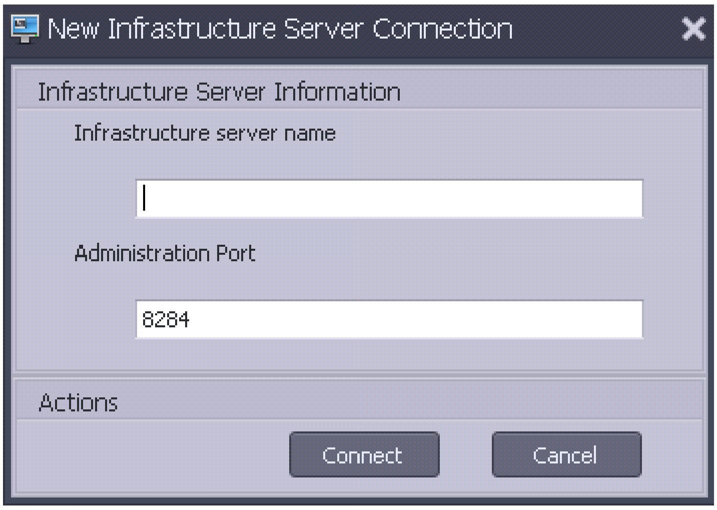
```
”path:\\to\\Citrix Workspace Environment Management Console Setup.exe ”/v”
argument=\\”value\\””
```

Configure the administration console

Create an infrastructure server connection

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

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

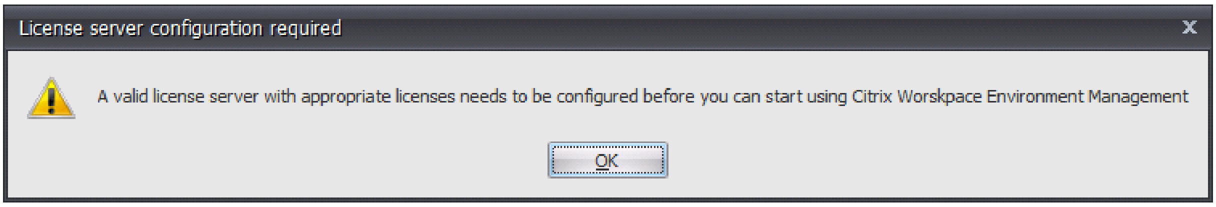

New Infrastructure Server Connection
Infrastructure Server Information
Infrastructure server name
Administration Port
8284
Actions
Connect
Cancel

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

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

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

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

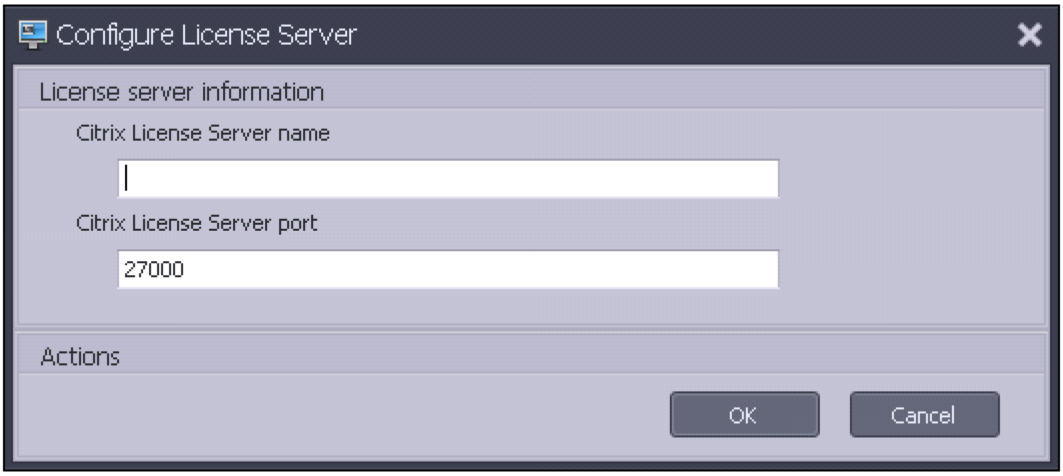


License server configuration required

A valid license server with appropriate licenses needs to be configured before you can start using Citrix Worskpace Environment Management

Configure the database with a license server

To configure the database with a license server, in the administration console ribbon click **About** then click **Configure License Server** and enter your Citrix License Server details. The Citrix License Server address must resolve from the administration console environment exactly as entered.



Configure License Server

License server information

Citrix License Server name

Citrix License Server port

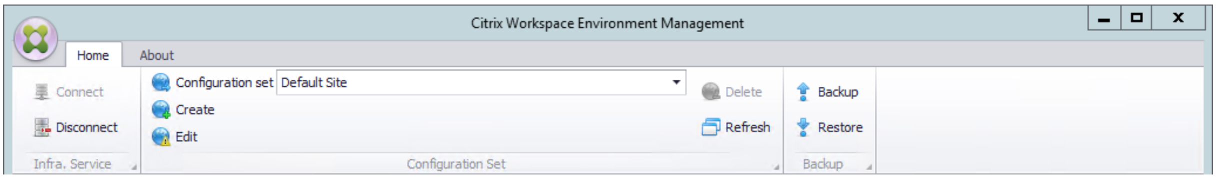
27000

Actions

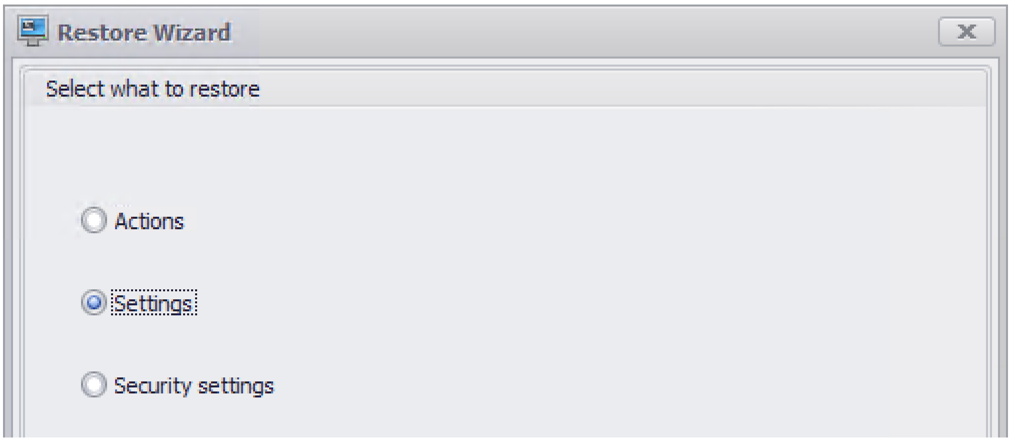
Import quickstart settings

Workspace Environment Management includes XML files which you can use to pre-configure your Workspace Environment Management database so that it is proof-of-concept-ready out of the box. The XML files are provided in the folder "Configuration Templates" in the Workspace Environment Management installer package.

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



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



Restore Wizard

Select what to restore

○ Actions

● Settings

○ Security settings

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

Agent

May 29, 2019

Configure the agent

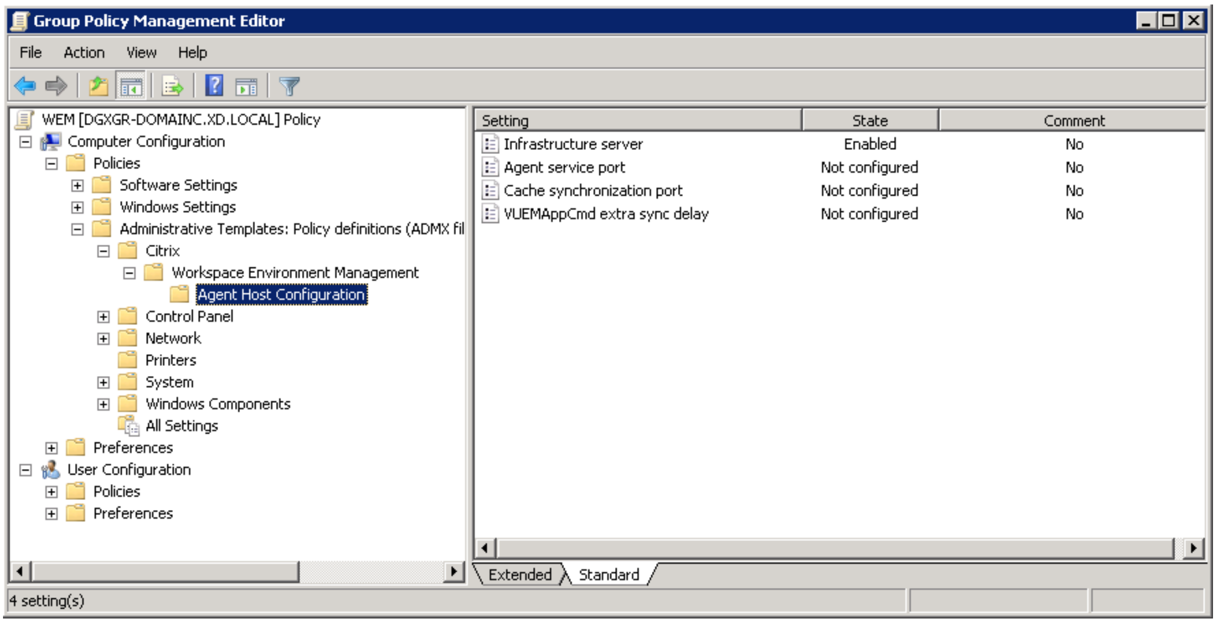
> **Note:**
>
> - The Workspace Environment Management agent cannot be installed on the infrastructure server.
> - Agent configuration requires administrative access to your Active Directory.
> - If you intend to assign resources published in Citrix StoreFront stores as application shortcuts in Workspace Environment Management from the administration console, ensure that Citrix Workspace app for Windows is installed on the administration console machine and on the agent host machine. For more information see System requirements.

Prerequisites

To configure the agent, use the **Workspace Environment Management Agent Host Configuration.adm** or the **Workspace Environment Management Agent Host Configuration.admx** administrative template (provided with Workspace Environment Management).

Configure group policies

The administrative template adds the Agent Host Configuration policy. Use the **Group Policy Management Editor** to configure a GPO with the following settings:



Setting	State	Comment
Infrastructure server	Enabled	No
Agent service port	Not configured	No
Cache synchronization port	Not configured	No
VUEMAppCmd extra sync delay	Not configured	No

Infrastructure server. The address of the Workspace Environment Management infrastructure server. It must be reachable exactly as typed from the user environment.

Agent service port. The default value is 8286. The agent service port must be the same as the port you configured for agent service port during infrastructure services configuration.

Cache synchronization port. The default value is 8285. The cache synchronization port must be the same as the port you configured for cache synchronization port during infrastructure services configuration.

VUEMAppCmd extra sync delay. The default value is 0. The delay interval in milliseconds for the agent application launcher (VUEMAppCmd.exe) to wait before Citrix Virtual Apps and Desktops published resources are started. This ensures that the necessary agent work has completed first.

Deploy the agent

There is one agent service:

Norskale Agent Host Service (NT SERVICE\Norskale Agent Host Service) : Manages WEM Agent. Account: LocalSystem. Changing this account is not supported. The agent service requires “log on as a local system” permission.

You can run **Citrix Workspace Environment Management Agent Setup** in your user environment. The installer accepts standard InstallShield deployment switches. The agent installs into the following default directory:

- C:\Program Files (x86)\Norskale\Norskale Agent Host (on 64-bit OS)
- C:\Program Files\Norskale\Norskale Agent Host (on 32-bit OS)

The **Citrix Workspace Environment Management Agent Setup** executable acknowledges the custom arguments below.

To ensure that the WEM agent service starts before the Windows logon screen appears, use the following three arguments:

- **WaitForNetwork**. Lets you configure whether the **WaitForNetwork** registry key created during installation is active. Accepted values: **0**, **1**. If not specified, the key will not be created during installation. If you configure this argument, the agent host waits for the network to be completely initialized and available.
- **SyncForegroundPolicy**. Lets you configure whether the **SyncForegroundPolicy** registry key created during installation is active. Accepted values: **0**, **1**. If not specified, the key will not be created during installation. The SyncForegroundPolicy argument configures the agent host to wait for complete network initialization before allowing a user to log on.
- **GpNetworkStartTimeoutPolicyValue**. Lets you configure the value of the GpNetworkStartTimeoutPolicyValue registry key created during installation, in seconds. By default, this value is 30, but the argument accepts any whole number. This argument specifies how long Group Policy waits for network availability notifications during policy processing on logon.

All three keys are created under
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon during the installation process, and are there 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 may lead to additional processing time prior to the login screen being displayed. Microsoft recommend setting the value of the **GpNetworkStartTimeoutPolicyValue** key to a minimum of 30 in order for it to have an impact.

AgentPort. The agent installer runs a script to open firewall ports locally, to make sure the agent network traffic is not blocked. This argument lets you configure which port is opened. If unspecified, the default port 8286 is used. Accepted values are any valid ports.

AgentSyncPort. The agent installer runs a script to open firewall ports locally, to make sure the agent network traffic is not blocked. This argument lets you configure which port is opened. If unspecified, the default port 8285 is used. Accepted values are any valid ports.

ServicesPipeTimeout. Lets you to configure the value of the ServicesPipeTimeout registry key, which is created during installation under
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet. This registry key adds a delay before the service control manager is allowed to report on the state of the Workspace Environment Management agent service, which prevents the agent from failing because the agent service launched before the network was initialized. This argument accepts any value, in milliseconds. If unspecified, a default value of 60000 (60 seconds) is used.

CmdLineToolsDebug. If the value of this argument is 1, the setup executable displays all arguments passed to the agent installer in a separate cmd window that will pause the installation until dismissed.

ARPSYSTEMCOMPONENT. Lets you designate the agent as a system component, which prevents it from appearing in Add/Remove Programs. Accepted values: **0**, **1**.

AgentCacheAlternateLocation. Lets you specify the value of the associated registry setting that must be expressed as a valid file path. If configured, the agent local cache file is saved in the designated location, instead of in the agent installation directory.

The syntax for these install arguments is as follows:

```
”path:\\to\\Citrix Workspace Environment Management Agent Setup.exe” /v ”argument=\\”value\\””
```

For example:

```
”C:\VUEM 4.04.00.00\Citrix Workspace Environment Management Agent Setup.exe” /v”WaitForNetwork=\”1\” GpNetworkStartTimeoutPolicyValue=\”45\””
```

Build the agent service cache

As an optional third step, or to build an image that includes the Workspace Environment Management Agent Host as pre-installed software, you can ensure that the agent service cache is built before the agent is run. (By default, the cache is built the first time the agent runs).

To create or rebuilds the agent Service cache, run the command line executable **AgentCacheUtility.exe** in the agent installation directory. The executable accepts the following command line arguments:

-help: displays a list of allowed arguments.

-refreshcache (or **-r**): triggers a cache build or refresh.

Upgrade a deployment

May 29, 2019

> **Note:**
>
> Learn about product name changes here.

Introduction

You can upgrade Workspace Environment Management deployments to newer versions without having to first set up new machines or sites; this is called an in-place upgrade. In-place upgrades from any of Workspace Environment Management 4.x to the latest released (current) version are supported.

> **Tip:**
>
> The Workspace Environment Management database, infrastructure service, and administration console must all be on the same version. If you need to roll-out Workspace Environment Management agents incrementally (for example, when upgrading), the use of agents which are no more than two versions older than the current release is supported but has not been tested.

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

1. Infrastructure services
2. Database
3. Administration console
4. Agent

Step 1: Upgrade the infrastructure services

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

> **Important:**
>
> After you upgrade the Infrastructure Services, you must reconfigure the Infrastructure Services using the WEM Infrastructure Service Configuration utility. See Configure the infrastructure service.

Infrastructure server OS upgrades

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

Step 2: Upgrade the database

> **Important:**
>
> - The database upgrade process is not reversible. Ensure that you have a valid database

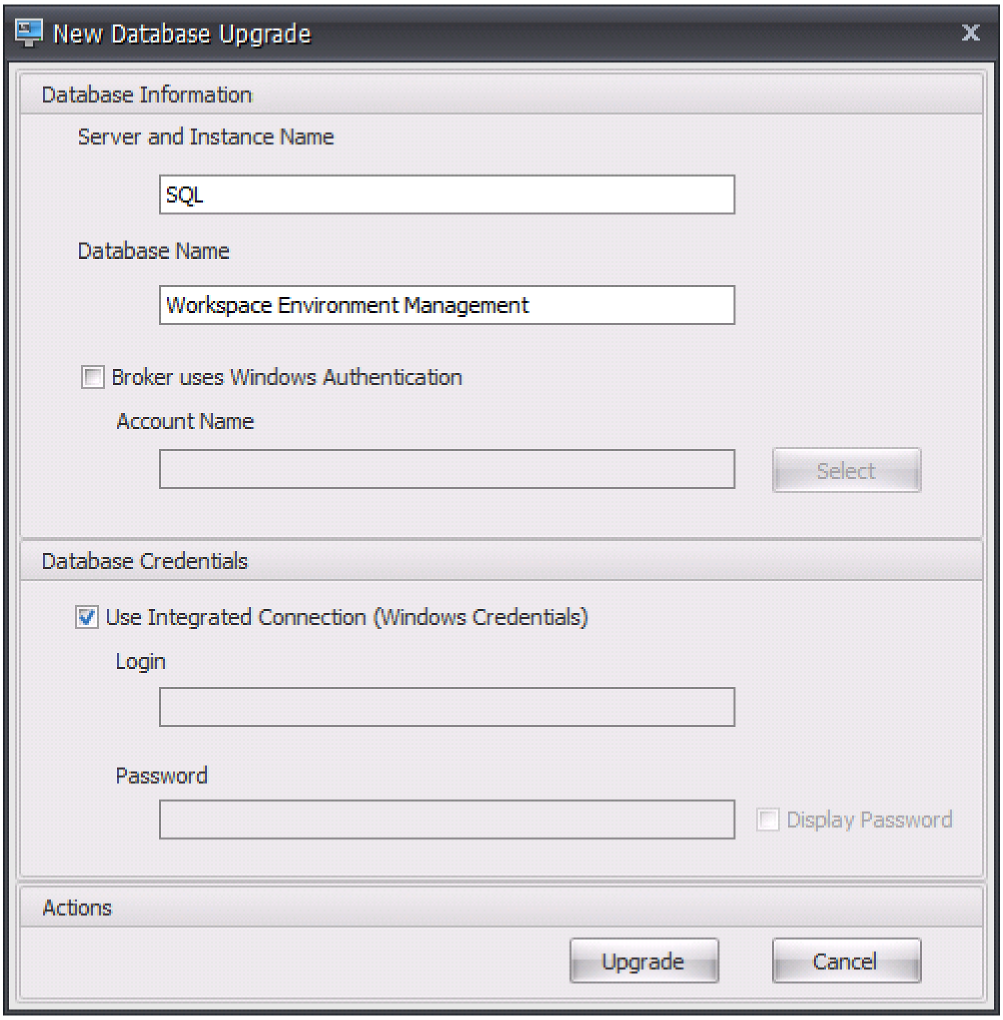
> backup before launching the upgrade process.
>
> - **SQL Server Always On availability groups**. If your Workspace Environment Management database is deployed in an SQL Server Always On availability group, before upgrading the database you must remove it from the availability group.
>
> **Tip:**
>
> You can also upgrade the database using the Workspace Environment Management PowerShell SDK module. For SDK documentation see Citrix Developer Documentation.

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

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

1. From the **Start** menu select **Citrix>Workspace Environment Management>WEM Database Management Utility**.

2. Click **Upgrade Database**.



New Database Upgrade

Database Information

Server and Instance Name: SQL

Database Name: Workspace Environment Management

□ Broker uses Windows Authentication

Account Name:

Database Credentials

☑ Use Integrated Connection (Windows Credentials)

Login:

Password:

□ Display Password

Server and instance name. Address of the SQL Server\instance on which the database is hosted. It must be reachable exactly as entered from the infrastructure server.

Database name. Name of the database to be upgraded.

Infrastructure service uses Windows authentication.

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

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

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

Click **Upgrade** to start the database upgrade process. Once you are notified that the database upgrade has completed successfully, you can exit the application.

If there are errors during the database upgrade, please check the **VUEM Database Management Utility Log** file in your Workspace Environment Management infrastructure services installation directory.

Step 3: Upgrade the administration console

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

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

Step 4: Upgrade the agent

> **Important:**
>
> Before upgrading an agent, make sure no users are logged in. This ensures that the upgrade process can modify the files on that machine.

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

By design, the WEM agents are backward compatible. Citrix recommends that you upgrade the agent to the latest version so that you can use the most recent features.

User experience

January 9, 2019

> **Note:**
>
> Learn about product name changes here.

Start the administration console

1. From the **Start** menu select **Citrix > Workspace Environment Management > WEM Administration Console**. By default, the administration console launches in a disconnected state.
2. On the administration console ribbon click **Connect**.

3. In the New Infrastructure Server Connection window, type the address of your infrastructure server and click **Connect**.

Configure your installation

In the administration console:

1. Click menu items in the lower-left-hand pane to display their sub-sections in the pane above them.
2. Click sub-section items to populate the main window area with appropriate content.
3. Change configuration as required. For more information about the settings you can use, see the user interface reference.

Ribbon

November 30, 2018

Home tab

The **Home tab** contains the following controls:

Connect. Connect administration console to specified infrastructure server. In the **New Infrastructure Server Connection** dialog specify:

- **Infrastructure server name**. Name of the infrastructure server you wish to connect to.
- **Administration port**. Port on which you wish to connect to the infrastructure service. Default value of 8284 is pre-populated.

Disconnect. Disconnect administration console from current infrastructure service. This allows the administrator to manage multiple infrastructure services from a single console, by disconnecting from one and connecting to another.

Configuration set. Switch from one Workspace Environment Management site (configuration set) to another.

Create. Open the Create configuration set window. Allows you to configure multiple Workspace Environment Management sites (configuration sets).

- **Name**. Site (configuration set) name as it will appear in the configuration set list in the Ribbon.
- **Description**. Site (configuration set) description as it appears in the site edition window.

- **Site State**. Toggles whether the site (configuration set) is Enabled or Disabled. When Disabled, Citrix Workspace Environment Management Agents cannot connect to the site (configuration set).

Edit. Open the Edit configuration set window, with similar options to the Create configuration set window.

Delete. Delete the site (configuration set). Note that you cannot delete "Default site" because it is required for Workspace Environment Management to function. You can, however, rename it.

Refresh. Refresh the site (configuration set) list. **Note**: The list does not refresh automatically when sites are created from different administration consoles.

Backup. Open the Backup wizard to save a backup copy of the current configuration to the WEM administration console machine. You can back up actions, settings, and security settings. Use **Restore** to restore (apply) the settings in this Citrix Cloud folder to your Workspace Environment Management service configuration.

- **Actions**. Back up selected Workspace Environment Management actions. Each type of action is exported as a separate XML file.
- **Settings**. Back up selected Workspace Environment Management settings. Each type of setting is exported as a separate XML file.
- **Security Settings**. Back up all Security tab settings in your current configuration set. Each type of rule is exported as a separate XML file.

Restore. Open the Restore wizard to restore settings already backed using **Backup** into your current configuration set. Select a folder containing Workspace Environment Management XML format backup files. Actions restored from backup are *added* to existing configuration set actions. Settings restored from backup *replace* existing configuration set settings.

- **Security Settings**. Restore all Security tab settings. The settings in the backup file(s) *replace* the existing settings in your current configuration set. When you switch to or refresh the Security tab, any invalid application security rules are detected. These rules are automatically deleted and listed in a report dialog, which you can export.

  In the ***Confirm Application Security Rule Assignment*** dialog, select **Yes** or **No** to indicate how you want restore to handle application security rule assignments:

  - if you select **Yes**, restore attempts to restore rule assignments to users and user groups in your current configuration set. Reassignment only succeeds if the backed up users or groups are present in your current configuration set or active directory. 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 current configuration.

About tab

The **About tab** contains the following controls:

Configure License Server. Allows you to specify the address of your Citrix License Server, without which the administration console will not let you modify any settings. Alternatively, you can use the **Licensing**tab in the Infrastructure Services Configuration utility to specify these credentials. Citrix License Server information is stored in the same location in the database in both cases.

Get Help. Opens the Citrix Product Documentation website in a web browser window.

Options. Opens the **Administration Console Options** dialog. These options are specific to this local instance of the administration console.

- **Auto Admin Logon**. If enabled, the administration console automatically connects to the last infrastructure service it connected to at startup.
- **Enable Debug Mode**. Enables verbose logging for the administration console. Logs are created in the root of the current user "Users" folder.
- **Console Skin**. Allows you to select from a variety of skins for the administration console only.
- **Port Number**. Allows you to customize the port on which the administration console connects to the infrastructure service. This port must match the port configured in the infrastructure services configuration.

About. Lists the current version of the administration console as well as licensing (license type, registration and count) and legal information.

Applications

December 24, 2018

Controls the creation of application shortcuts.

> **Tip:**
>
> - Use Citrix Studio to edit the application settings and add an executable file path that points to **VUEMAppCmd.exe** (located in the agent installation directory). The **VUEMAppCmd.exe** ensures that Workspace Environment Management agent has finished processing an environment before Citrix Virtual Apps and Desktops published applications are started.
> - You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Application List

A list of your existing application resources. You can use **Find** to filter the list by name or ID against a text string.

To add an application

1. Use the context menu **Add** command.
2. Enter details in the **New Application** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the application shortcut, as it appears in the application list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

Application Type. The type of application the shortcut starts, which can be one of **Installed application**, **File / Folder**, **URL**, or **StoreFront store**. These require the following values:

- **Command Line**. The path to the application executable as the client machine will see it. The **Browse** button allows you to browse to a locally installed executable.
- **Working Directory**. The shortcut working directory. Automatically filled out if you browse to the executable.
- **Parameters**. Any launch parameters for the application.
- **Target**. (File / Folder) The name of the target file or folder the application will open.
- **Shortcut URL**. (URL) The URL of the application shortcut you are adding.
- **Store URL**. (StoreFront store) The URL of the StoreFront store containing the resource you want to start from the shortcut.
- **Store Resource**. (StoreFront store) The resource on the StoreFront store which you want to start from the shortcut. The **Browse** button allows you to browse and select the resource.

Start Menu Integration. Select where the application shortcut is created in the Start Menu. By default, a new shortcut is created in Programs.

Select Icon. Allows you to browse to an icon file and select an icon for your application. By default, this uses the application executable's icon but you can select any valid icon. Icons are stored in the database as text.

High Resolution Icons Only. Only displays HD icons in the selection box.

Application State. Controls whether the application shortcut is enabled or not. When disabled, it is not processed by the agent even if assigned to a user.

Maintenance Mode. When active, this will prevent the user from running the application shortcut. The shortcut icon is modified to include a warning sign to denote that the icon is not available, and the user will receive a short message informing them the application is unavailable if they try to launch it. This allows you to proactively manage scenarios where published applications are in maintenance without having to disable or delete application shortcut resources.

Display Name. The name of the shortcut as it will appear in the user's environment.

Window Style. This controls what state the application starts in (minimized, maximized, or normal).

Self-Service Display. If selected, the resource will not be shown in the Workspace Environment Management agent self-service window.

Hotkey. Allows you to specify a hotkey for the user to launch the application with. Hotkeys are case sensitive and are entered in the following format (e.g.): Ctrl + Alt + S.

Action Type. Describes what type of action this resource is.

Enable Automatic Self-Healing. When selected, application shortcuts will automatically be recreated by the agent at refresh if they have been moved or deleted by the user.

Enforce Icon Location. Allows you to specify the exact location of the application shortcut on the user's desktop. Values are in pixels.

Windows Style. Controls whether the application opens minimized, or in a normal or maximized window on the end-user machine.

Do Not Show in Self Services. Hides the application from the self-service interface accessible from a status bar icon available to end-users when the session agent is running in UI mode. This includes hiding it in the context menu "My Applications" icon list, and in the Manage Applications form.
Create Shortcut in User Favorites Folder. Creates an application shortcut in the end-user Favorites folder.

To add an Application entry that is based on a StoreFront store, you must provide valid credentials, so that a list of published applications can be retrieved by Citrix Workspace app for Windows installed on the WEM administration console machine.

Start Menu View

Displays a tree view of your application shortcut resource locations in the Start Menu.

Refresh. Refreshes the application list.

Move. Opens up a wizard which allows you to select a location to move the application shortcut to.

Edit. Opens up the application edition wizard.

Delete. Deletes the selected application shortcut resource.

Printers

September 4, 2018

This tab controls the mapping of printers.

> **Tip:**
>
> You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Network Printer List

A list of your of your existing printer resources, with unique IDs. You can use **Find** to filter your printers list by name or ID against a text string. You can import printers using **Import Network Print Server** on the ribbon.

To add a printer

1. Use the context menu **Add** command.
2. Enter details in the **New Network Printer** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the printer, as it appears in the printer list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

Target Path. The path to the printer as it resolves in the user's environment.

Printer State. Toggles whether the printer is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

External Credentials. Allows you to state specific credentials with which to connect to the printer.

Self-Healing. Toggles whether the printer is automatically recreated for users when the agent refreshes.

Action Type. Describes what type of action this resource is. For **Use Device Mapping Printers File**, specify Target Path as the absolute path to an XML printer list file (see XML printer list configuration). When the agent refreshes it parses this XML file for printers to add to the action queue.

To import a printer

1. In the ribbon click **Import Network Print Server**.
2. Enter details in the **Import from Network Print Server** dialog, then click **OK**:

Fields and controls

Print Server Name. The name of the print server you wish to import printers from.

Use Alternate Credentials. By default, the import uses the credentials of the Windows account under whose identity the administration console is currently running. Select this option to specify different credentials for the connection to the print server.

Network Drives

May 20, 2019

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.

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

September 4, 2018

Controls the mapping of virtual drives. Virtual drives are Windows virtual drives or MS-DOS device names which 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

A list of your existing virtual drives, with a unique ID. You can use **Find** to filter the list by name or ID against a text string.

To add a virtual drive

1. Use the context menu **Add** command.
2. Enter details in the **New Virtual Drive** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the drive, as it appears in the virtual 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 virtual drive as it resolves in the user's environment.

Virtual Drive State. Toggles whether the virtual drive is enabled or disabled. When disabled, it will not be processed by the agent even if assigned to a user.

Parameters. Allows you to specify any launch parameters for the application.

External Credentials. Allows you to state specific credentials with which to connect to the printer.

Action Type. Describes what type of action this resource is.

Registry Entries

January 18, 2019

Controls the creation of registry entries.

> **Tip:**
>
> You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Registry Value List

A list of your existing registry entries. You can use **Find** to filter the list by name or ID against a text string.

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 will appear in the registry (e.g. NoNtSecurity).

Target Type. The type of registry entry that will be created.

Target Value. The value of the registry entry once created (e.g. 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.

To import registry files

1. In the ribbon click **Import Registry File**.
2. Enter details in the **Import from Registry** dialog, then click **OK**.

Fields and controls

Registry File Name. This field allows you to browse to browse to a **.reg** file containing the registry settings you want to import into Workspace Environment Management. For best results, the .reg file should be generated from a clean environment that has only the registry settings you wish to import applied to it.

Scan. This will scan the **.reg** file and display a list of registry settings contained inside it.

Registry Values List. This lists all of the registry values contained within your imported **.reg**.

Enable Imported Items. If disabled, newly-imported registry keys are disabled by default.

Prefix Imported Item Names. This adds a prefix to the name of all registry items imported via this wizard (e.g. “XP ONLY” or “finance”), to make it easier to organise your registry entries.

> **Note:**
>
> The wizard cannot import registry entries with duplicate names. If your **.reg** file contains more

> than one registry entry with the same name (as displayed in the Registry Values List), select one of these entries for import and rename it if you want to import the others.

Ports

September 28, 2018

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.

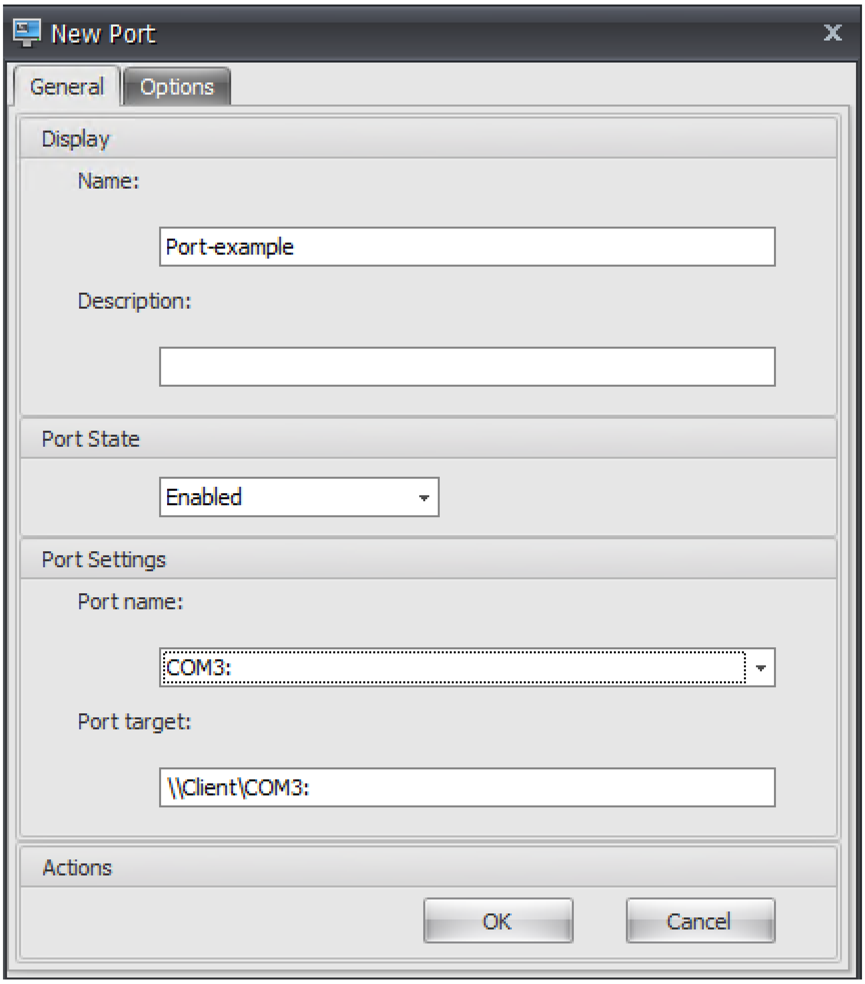
Port Target. The target port.

Options tab

Action Type. Describes what type of action this resource is.

For example, you can configure the port settings as follows:

- **Port name**: Select "COM3:"
- **Port target**: Enter `\\Client\COM3:`



New Port

Display

Name: Port-example

Description:

Port State: Enabled

Port Settings

Port name: COM3:

Port target: \\Client\COM3:

Ini Files

September 4, 2018

Controls the creation of **.ini** file operations, which allow you to modify **.ini** files.

> **Tip:**
>
> You can use dynamic tokens to extend Workspace Environment Management actions to make

> them more powerful.

Ini files operation list

A list of your existing ini file operations. You can use **Find** to filter the list by name or ID against a text string.

To add an .ini files operation

1. Use the context menu **Add** command.
2. Enter details in the **New Ini Files Operation** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the .ini file operation, as it appears in the **Ini File Operations** list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

.ini File Operation State. Toggles whether the .ini file operation is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Target Path. This specifies the location of the .ini file that will be modified as it resolves in the user's environment.

Target Section. This specifies which section of the .ini file is targeted by this operation. If you specify a non-existent section, it will be created.

Target Value Name. This specifies the name of the value that will be added.

Target Value. This specifies the value itself.

Run Once. By default, Workspace Environment Management performs a .ini file operation every time the agent refreshes. Tick this box to make Workspace Environment Management only perform the operation once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many .ini file operations assigned to your users.

Action Type. Describes what type of action this resource is.

External Tasks

September 4, 2018

Controls the execution of external tasks such as running **.vbs** or **.cmd** scripts.

> **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 by name or ID against a text string.

To add an external task

1. Use the context menu **Add** command.
2. Enter details in the **New External Task** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the external task, as it appears in the external task 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 external task script as it resolves in the user's environment.

Target Arguments. Allows you to specify any launch parameters or arguments.

External Task State. Toggles whether the external task is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Run Hidden. If selected, the external task runs in the background and is not shown to the user.

Run Once. By default, Workspace Environment Management runs an external task every time the agent refreshes. Tick this box to make Workspace Environment Management only run the external task once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many external tasks assigned to your users.

Wait for Task Completion. This toggles whether or not the agent waits for the external task to complete. The Timeout value controls the maximum wait time.

Execute Only at Logon. If selected, the external task will only be run at logon rather than during every single refresh.

External Task Execution Order. This allows you to specify a priority for each individual external task, in case multiple tasks are assigned to one user and some tasks rely on results from others to run successfully.

Action Type. Describes what type of action this resource is.

File System Operations

September 4, 2018

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. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

Filesystem Operation State. Toggles whether the file system operation is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Source Path. The path to the source file or folder that is copied.

Target Path. The destination path for the source file or folder that is copied.

Overwrite Target if Existing. Toggles 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. Tick this box to make Workspace Environment Management only run the operation once, rather than at 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. Please note that for symbolic link creation, you will need to give users the `SeCreateSymbolicLinkPrivilege` privilege for Windows to allow symbolic link creation.

User DSN

September 4, 2018

Controls the creation of user DSNs.

> **Tip:**
>
> You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

User DSN list

A list of your existing user DSNs. You can use **Find** to filter the list by name or ID against a text string.

To add a user DSN

1. Use the context menu **Add** command.
2. Enter details in the **New User DSN** dialog tabs, then click **OK**.

Fields and controls

Name. The display name of the user DSN, as it appears in the user DSN list.

Description. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.

User DSN State. Toggles whether the user DSN is enabled or disabled. When disabled, it will not be processed by the agent even if assigned to a user.

DSN Name. The functional name of the user DSN.

Driver. The DSN driver. At present, only SQL server DSNs are supported.

Server Name. The name of the SQL server to which the user DSN is connecting.

Database Name. The name of the SQL database to which the user DSN is connecting.

Connect Using Specific Credentials. Allows you to specify credentials with which to connect to the server/database.

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

April 29, 2019

Controls the creation of file 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 against a text string.

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 association. If you select a file extension from the list, the ProgID field automatically populates (providing that the file type is present on the machine the administration console is running on). You can also type the extension directly.
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.
Action. Allows you to select the action type: open, edit or print.

Target. Allows you to specify the executable used with this file extension.

Command. Allows you to state any specific commands the executable should follow.

Set as Default Action. Toggles whether the association is set as a default for that file extension or not.

Overwrite. Toggles whether or not this file association will overwrite any existing associations for the specified extension.

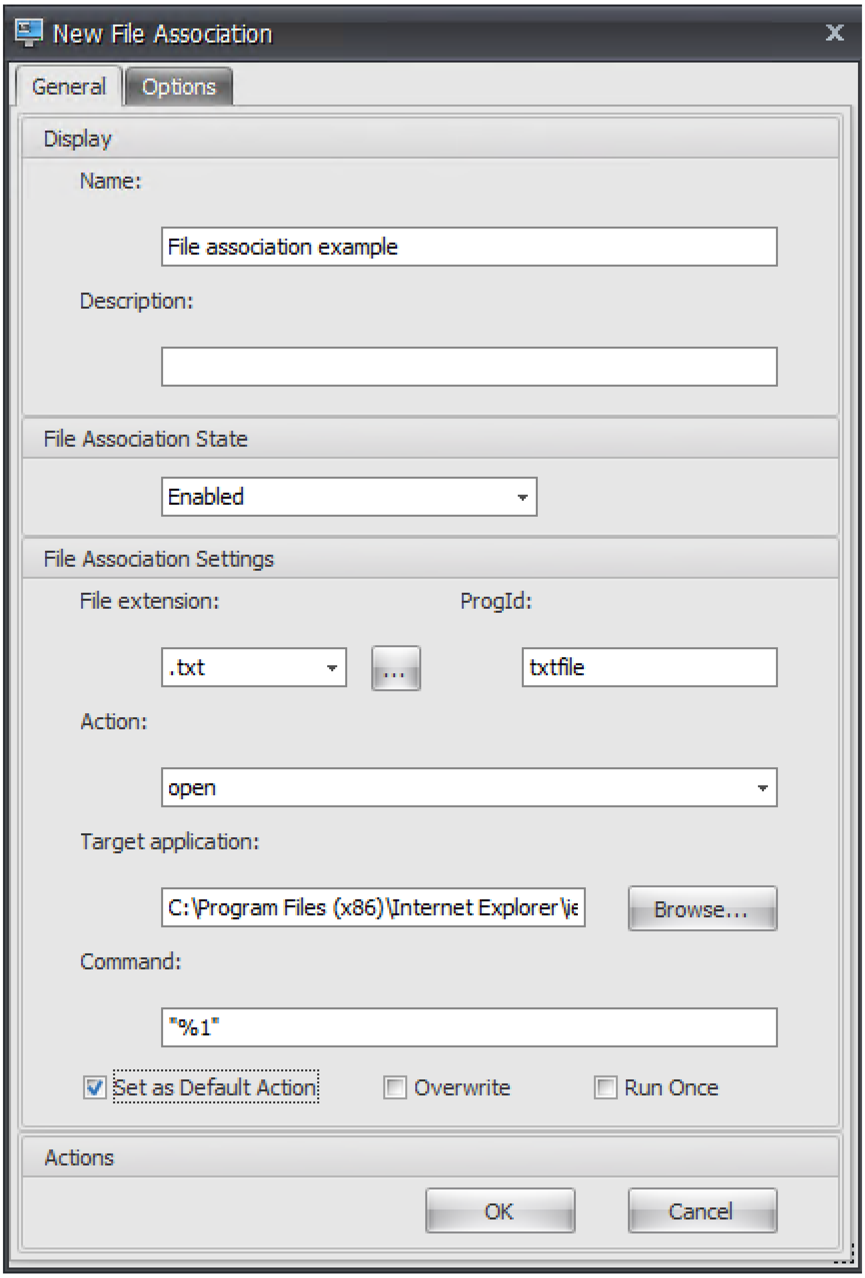
Run Once. By default, Workspace Environment Management creates a file association every time the agent refreshes. Select this option to create the file association once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many file associations assigned to your 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), follow the steps below.

Step 1. On the **Administration Console > Actions > File Associations > File Association List** tab, click **Add**.

Step 2. In the **New File Association** window, type the information and then click **OK**.



Name: File association example

Description:

Enabled

File extension: .txt

ProgId: txtfile

Action: open

Target application: C:\Program Files (x86)\Internet Explorer\ie

Command: "%1"

☑ Set as Default Action □ Overwrite □ Run Once

> **Note:**
>
> - **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**.

Step 3. Go to the **Administration Console > Assignments > Action Assignment** tab.

Step 4. Double-click the user or user group to which you want to assign the action.

Step 5. Go to the **Administration Console > Administration > Agents > Statistics** tab and then click **Refresh**.

Step 6. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.

Step 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.

Filters

August 24, 2018

Filters contains rules and conditions which allow you to make actions available (assign) to users. Set up rules and conditions before assigning actions to users.

Rules

Rules are composed of multiple conditions. You use rules to define when an action is assigned to a user.

Filter rule list

A list of your existing rules. You can use **Find** to filter the list by name or ID against a text string

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.

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**.

Assignments

November 30, 2018

> **Tip:**
>
> Before assigning actions to users you need to perform the following steps in the order given:
>
> - Configure users, see Users in Active Directory Objects.
> - Define conditions, see Conditions.
> - Define filter rules, see Rules.
> - Configure actions, described here.

Use assignments to make actions available to your users. This allows you to 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. You can use **Find** to filter the list by name or ID against a text string.

> **Tip:**
>
> To simplify assigning actions for all users in Active Directory, use the 'Everyone' default group to assign the actions. Note that 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

Allows you to assign actions to the selected user/group. You can use **Find** to filter the list by name or ID against a text string.

Available. These are the actions available to you to assign to this user or group.

Double-clicking an action or clicking the arrow buttons will assign/unassign it. When you assign an action, you are prompted to select the rule you wish to use to contextualize it.

Assigned. These are the 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 on a user/group. This populates the Assignments lists.
2. In the **Available** list, select an action and click the right-arrow (**>**) button.
3. In the **Assign Filter** dialog, select a **Filter Rule** and click **OK**.
4. In the **Assigned list**, you can use the **Enable** and **Disable** context actions to fine-tune the behaviour of the assignment.

> **Note:**
>
> If you want to enable the PinToStartMenu option for an application in the Assigned list, you must enable the Create Start Menu option as well, otherwise the application fails to appear in the Start menu after refreshing the agent.

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 load is complete).

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 wish to model.

Resultant Actions. The actions assigned to the user (whether individually or to groups the user belongs to).

User Groups. The groups the user belongs to.

System Optimization

September 4, 2018

Workspace Environment Management system optimization consists of the following:

- Fast Logoff
- CPU Management
- Memory Management
- I/O Management

These settings are designed to lower resource usage on the agent host machine. They help to ensure that freed-up resources are available for other applications, increasing user density by supporting more users on the same server.

Although 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 Spikes Protection in User A's session, the event is recorded for User A only. When User B starts the same process, process optimization behavior is determined only by process triggers in User B's session.

> **Tip:**
>
> When your virtual machines have different hardware configurations, consider creating multiple configuration sets for them, and configuring the system optimization settings differently for each configuration set. Machines can only belong to one configuration set.

CPU Management

September 4, 2018

These settings allow you to 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, CPU Management Settings allow you to limit how much CPU capacity treats individual process can use. CPU Spikes Protection is not designed to reduce overall CPU usage. CPU Spikes Protection is designed to reduce the impact on user experience by processes that consume an excessive percentage of CPU Usage.

When CPU Spikes Protection is enabled, if any process reaches a configurable 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 Spikes Protection examines each process in quick "snapshot". If the average load of a process exceeds the configured usage limit for a configurable sample time, its priority is immediately reduced. After a configurable time, the process' CPU priority returns to its previous value. Note that the process is not "throttled", like in CPU Clamping; only its priority is reduced.

CPU Spikes Protection is not triggered until one instance of an individual process exceeds the threshold. In other words, even if total CPU consumption exceeds the specified threshold, CPU Spikes Protection does not trigger unless any single process instance exceeds the threshold. But as soon as a single process instance triggers, new instances of the same process are (CPU) optimized when the option "Enable Intelligent CPU Optimization" is enabled.

Whenever a specific process triggers 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 User A does not affect the behavior of the same process for User B.

For example, if Internet Explorer is sometimes consuming 50–60% of CPU, you can use CPU Spikes Protection to target only those iexplore.exe instances that are threatening VDA performance. (By contrast, CPU clamping would apply to all processes.)

We recommend that you experiment with the sample time to decide the optimal value for your environment which does not affect other users logged into the same VDA.

CPU Spikes 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 to be 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 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 server OS VDA VMs. Each VM is configured with two 4-cores CPUs (8 logical processors). To restrict processes that trigger CPU Spikes 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).

Enable CPU Spikes Protection. Lowers the CPU priority of any process which exceeds the configured percentage of CPU usage, for a configurable period of time.

- **CPU Usage Limit**. The percentage CPU usage that any process instance needs to reach to trigger CPU Spikes Protection. This limit is global across all logical processors in the server, and is determined on a process instance-by-process instance basis. Multiple instances of the same process do not have their CPU usage percentages added when determining CPU Spikes Protection triggers.

  If a process instance never reaches this limit, CPU Spikes 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 Spikes Protection will never trigger unless you set CPU Usage Limit at or below 35%.

- **Limit Sample Time**. This is the time for which a process must exceed the CPU Usage Limit before its CPU priority is lowered.

- **Idle Priority Time**. This is the length of time the process' priority is lowered. After this time expires, the process CPU Priority returns to its original level.

Limit CPU/Core Usage. Confines processes that trigger CPU Spikes Protection to a selected number of logical processors in the machine. When enabled, limits the maximum consumption of any isolated process to 100 * (number of core(s) selected / total number of cores)%.

- **CPU / Core Usage Limit**. The number of logical processors in the machine to which processes which trigger CPU Spikes Protection are restricted. Note: to restrict processes running on a VM, this means the number of logical processors in the VM, not in the underlying physical hardware.

Enable Intelligent CPU Optimization. When enabled, the agent intelligently optimizes the CPU priority of processes which have triggered CPU Spikes Protection. Processes that repeatedly trigger CPU Spikes Protection are assigned progressively lower CPU priority at launch than processes which behave correctly.

Enable Intelligent I/O Optimization. When enabled, the agent intelligently optimizes the process I/O priority of processes which have triggered CPU Spikes Protection. Processes that repeatedly trigger CPU Spikes Protection are assigned progressively lower I/O priority at launch than processes which 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 Spikes 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 Spikes Protection, and process CPU priority is lowered, Workspace Environment Management logs a warning each time it lowers the CPU priority of a process. In the Event Log, in Application and Services Logs, Norskale Agent Service, look for "**Initializing process limitation thread for process**".

CPU Priority

These settings take effect if processes are competing for a resource. They allow you to optimize the CPU priority level of specific processes, so that processes which are contending for CPU processor time do not cause performance bottlenecks. When processes are in competition 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, the more 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, this option enables manual setting of process CPU priority.

To add a process to the CPU priority process list

1. Click **Add** and type details in the **Add Process CPU Priority** dialog.
2. Click **OK** to close the dialog.
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 next 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, the more processor time it gets. Select from Realtime, High, Above Normal, Normal, Below Normal, and 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**.

CPU Affinity

Enable Process Affinity. When enabled, allows you to define how many "logical processors" a process will use. 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 configurable percentage of the CPU's processing power. Workspace Environment Management "throttles" (or "clamps") that process when it reaches the specified CPU % you set. This lets you prevent processes from consuming large amounts of CPU.

> **Note:**
>
> CPU clamping is a brute force approach which is computationally expensive. To keep the CPU usage of a troublesome process artificially low, it is better to use CPU Spikes Protection, at the

> same time as assigning static CPU priorities and CPU affinities to such processes. CPU clamping is best reserved for controlling processes which are notoriously bad at resource management, but which cannot stand to be dropped in priority.

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 Workspace Environment Management 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 CPU Clamping is working by looking at process monitor, and confirming that CPU consumption never rises above the clamping percentage.

Memory Management

May 18, 2018

These settings allow you to optimize application RAM usage.

If these settings are enabled, Workspace Environment Management (WEM) calculates how much RAM a process is using, and the minimum amount of RAM a process needs, without losing stability. WEM considers the difference as *excess RAM*. When the process becomes idle—usually when the application is minimized to the Task Bar—WEM releases the process's excess RAM to the page file, and optimizes the process for subsequent launches.

When applications are restored from the Task Bar, they initially run in their optimized state but can still go on to consume additional RAM as needed.

WEM optimizes *all* applications that a user is using during their desktop session in a similar way. If there are multiple processes over multiple user sessions, all RAM that is freed up is available for other processes. This increases user density by supporting a greater number of users on the same server.

Enable Working Set Optimization. Forces applications which have been idle for a configurable time to release excess memory until they are no longer idle.

Idle Sample Time (min). Time for which an application must be idle before it is forced to release excess memory. During this time period, WEM calculates how much RAM a process is using, and minimum amount of RAM a process needs, without losing stability. The default value is 120 min.

Idle State Limit (percent). The percentage of CPU usage under which a process is considered to be idle. The default value is 1%. Citrix do not recommend using a value above 5%: otherwise a process being actively used can be mistaken for an idle process, resulting in its memory being released.

Exclude Specified Processes. Allows you to exclude processes from memory management by name (for example, notepad.exe).

I/O Management

May 18, 2018

These settings allow you to optimize the I/O priority of specific processes, so that processes which are contending for disk and network I/O access do not cause performance bottlenecks. For example, you can use I/O Management settings to throttle back a disk-bandwidth-hungry application.

The process priority you set here establishes the "base priority" for all of the threads in the process. The actual, or "current," priority of a thread might be higher (but is never lower than the base). In general, Windows give access to threads of higher priority before threads of lower priority.

I/O Priority

Enable Process I/O Priority. Enables manual setting of process I/O priority.

To add a process to the I/O priority list

1. Click **Add** and type details in the **Add Process I/O Priority** dialog.
2. Click **OK** to close the dialog.
3. Click **Apply** to apply the settings. Process I/O priorities you set here take effect when the agent receives the new settings and the process is next restarted.

Process Name. The process executable name without the extension. For example, for Windows Explorer (explorer.exe) type "explorer".

I/O Priority. The "base" priority of all threads in the process. The higher the I/O priority of a process, the sooner its threads get I/O access. Choose from High, Normal, Low, Very Low.

To edit a process I/O priority item

Select the process name and click **Edit**.

To remove a process from the I/O priority list

Select the process name and click **Remove**.

Fast Logoff

August 17, 2018

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.

Policies and Profiles

June 18, 2018

These settings allow you to replace user GPOs and configure user profiles.

- Environmental Settings
- Microsoft USV Settings
- Citrix Profile Management Settings
- VMware Persona settings

Environmental Settings

March 13, 2019

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 checkbox toggles whether or not the agent processes environmental settings. If it is cleared, no environmental settings are processed.

Exclude Administrators. If enabled, environmental settings are not processed for administrators, even if the agent is launched.

User Interface: Start Menu. These settings control which Start Menu functions are disabled by the agent.

> **Important:**
>
> On operating systems other than Windows 7, the options under **User Interface: Start Menu** might not work, except **Hide System Clock** and **Hide Turnoff Computer**.

User Interface: Appearance. These settings allow you to customize the user's Windows theme and desktop. Paths to resources must be entered as they are accessed from the user's environment.

Desktop

User Interface: Desktop. These settings control which desktop elements are disabled by the agent.

User Interface: Edge UI. These settings allow you to disable aspects of the Windows 8.x Edge user interface.

Windows Explorer

These settings control which Windows Explorer functionalities are disabled by the agent.

User Interface: Explorer. These options allow you to disable access to **regedit** or **cmd**, and hide certain elements in Windows Explorer.

Hide Specified Drives. 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. If enabled, the listed drives are blocked. Neither the user 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 user has access to his Windows control panel.

Show only specified Control Panel Applets. If enabled, all control panel applets except the ones listed here are hidden from the user. Additional applets are added using their canonical name.

Hide specified Control Panel Applets. If enabled, only the listed control panel applets are hidden. Additional applets are added using their canonical name.

See Common Control Panel applets along with their canonical names.

Known Folders Management

Disable Specified Known Folders. Prevents the creation of the specified user profile known folders at profile creation.

SBC/HVD Tuning

SBC/HVD (Session-Based Computing/Hosted Virtual Desktop) tuning allows you to optimize the performance of sessions running on Citrix Virtual Apps and Desktops. While designed to improve performance, some of the options might result in slight degradation of the user experience.

User Environment: Advanced Tuning. These options allow you to optimize performance in SBC/HVD environments.

Disable Drag Full Windows. Disables dragging maximized windows.

Disable SmoothScroll. Disables the smooth scrolling effect while browsing pages.

Disable Cursor Blink. Disables the cursor flickering effect.

Disable MinAnimate. Disables the animation effect when minimizing or maximizing windows.

Enable AutoEndTasks. Automatically ends the tasks after they time out.

WaitToKillApp Timeout. The timeout value (in milliseconds) for ending the applications. The default value is 20,000 milliseconds.

Set Cursor Blink Rate. Changes the cursor blink rate.

Set Menu Show Delay. Specifies a delay (in milliseconds) before the menu appears after logon.

Set Interactive Delay. Specifies a delay (in milliseconds) before a submenu appears.

Microsoft USV Settings

April 24, 2019

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 USV Configuration. Controls whether the agent processes USV settings. If it is cleared, no USV settings are processed.

Set Windows Roaming Profile Path. The path to your Windows profiles.

Set RDS Roaming Profiles Path. The path to your RDS roaming profiles.

Set RDS Home Drive Path. The path to your RDS home drive, as well as the drive letter it appears with in the user environment.

Roaming Profiles Advanced Configuration

These 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.

Folder Redirection

Process Folder Redirection Configuration. This checkbox 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

June 4, 2019

Workspace Environment Management supports the features and operation of the current version of Citrix Profile Management. In the Workspace Environment Management administration console, the **Citrix Profile Management Settings** (in Policies and Profiles) supports configuring all settings for the current version of Citrix Profile Management.

If you wish to configure Citrix Profile Management features, you should do so using AD GPO, Citrix Studio policies, or .INI files on the VDA.

> **Note:**
>
> Some options only work with specific versions of Profile Management; please consult the relevant Citrix documentation for detailed instructions.

Main Citrix Profile Management Settings

These settings control the main Citrix Profile Management parameters.

Enable Profile Management Configuration. This checkbox toggles whether or not the agent processes Citrix Profile Management settings. If cleared, none of the Profile Management settings are processed.

Enable Profile Management. This checkbox toggles whether or not the agent processes the settings in the Profile Management section of this page. If disabled, the agent does not process any of these.

Set processed groups. Allows you to specify which groups are processed by Profile Management. Only the specified groups have their Profile Management settings processed. If left blank, all groups are processed.

Set excluded groups. Allows you to specify which groups are excluded from Profile Management.

Process logons of local administrators. If enabled, local administrator logons are treated the same was as non-admin logons for Profile Management.

Set path to user store. This field allows you to specify the path to the user store directory.

Enable active write back. If enabled, profiles are written back to the user store during the user's session. This helps prevent data loss.

Enable Offline profile support. If enabled, profiles are cached locally for use while not connected.

Enable active write back registry. If enabled, registry entries are written back to the user store during the user's session. This helps prevent data loss.

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. Allows you to specify a delay (in seconds) before cached profiles are deleted at log-off.

Enable Migration of Existing Profiles. If enabled, existing Windows profiles are migrated to Profile Management at login.

Enable local profile conflict handling. This setting configures how Citrix Workspace Environment Management handles cases where Profile Management and Windows profiles conflict.

Enable template profile. If enabled, this will use a template profile at the indicated location.

Template profile overrides local profile. If enabled, the template profile will override local profiles.

Template profile overrides roaming profile. If enabled, the template profile will override roaming profiles.

Template profile used as Citrix mandatory profile for all logons. If enabled, the template profile will override all other profiles.

Advanced Settings

These options control advanced UPM settings.

Set number of retries when accessing locked files. Configures the number of times the Agent will retry accessing locked files.

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, will delete local copies of redirected folders.

Disable automatic configuration. If enabled, dynamic configuration will be 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 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.

Log Settings

These options control Profile Management logging.

Enable Logging. Enables/disables logging of Profile Management operations.

Configure Log Settings. Allows you to specify which types of events to include in the logs.

Set Maximum Size of Log File. Allows you to specify a maximum size in bytes for the log file.

Set Path to Log File. Allows you to specify the location at which the log file will be 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 Panagement 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 will synchronize these excluded files or folders from the user store to local profile when a user logs on.

Ignore excluded files or folders. Profile Management ignores the excluded files or folders in the user store when a user logs on.

Delete excluded files or folder. Profile Management deletes the excluded files or folders in the user store when a user logs on.

Enable Default Exclusion List - Directories. Default list of directories ignored during synchronization. If selected, folders which are selected in this list are excluded from the Profile Management synchronization.

Enable File Exclusions. If enabled, the listed files are not included in a user's Profile Management profile. This allows you to exclude specific folders known to contain large amounts of data which the user does not need to have as part of their Profile Management profile. The list is pre-populated with default Windows 7 exclusions, and can be pre-populated with default Windows XP exclusions instead.

Enable Folder Exclusions. If enabled, the listed folders are not included in a user's Profile Management profile. This allows you to exclude specific folders known to contain large amounts of data which the user does not need to have as part of their Profile Management profile. The list is pre-populated with default Windows 7 exclusions, and can be pre-populated with default Windows XP exclusions instead.

Profile Cleansing. Opens the **Profiles Cleanser** wizard, which allows you to delete existing profiles.

To delete existing profiles, click **Browse** to navigate to the folder where user profiles are stored, click **Scan Profiles Folder**, and then select the profile folder that you want to clean up in the Profiles Cleanser window. After that, click **Cleanse Profiles** to start the cleanup.

Cleanse Profiles. 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.

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 will be kept in the user store.

Enable Folder Mirroring. If enabled, the listed folders are mirrored to the user store on logoff, ensuring that files and subfolders in mirrored folders stored in the user store are exactly the same as the local versions. See below for more information about how folder mirroring works.

- Files in mirrored folders will always overwrite files stored in the user store on session logoff, irrespective of whether they are modified.
- If extra files or subfolders are present in the user store compared to the local versions in mirrored folders, those extra files and subfolders will be deleted from the user store on session logoff.

Enable Large File Handling. If enabled, large files are redirected to the user store, thereby eliminating the need to synchronize those files over the network.

> **Note:**
>
> Some applications do not allow concurrent file access. Citrix recommends that you take application behavior into consideration when you define your large file handling policy.

Streamed User Profiles

These options control streamed user profile settings.

Enable Profile Streaming. If disabled, none of the settings in this section are processed.

Always cache. If enabled, files of the specified size (in megabytes) 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, in the event that 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.

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. Allows you to specify the user groups for which cross-platform profiles are used.

Set path to cross-platform definitions. Allows you to specify the path to your cross-platform definition files.

Set path to cross-platform setting store. Allows you to specify the path to your cross-platform setting store.

Enable source for creating cross-platform settings. Enables a source platform for cross-platform settings.

VMware Persona settings

May 18, 2018

These settings control Workspace Environment Management's integration with VMware View Persona Management. Please note that some options only work with specific versions of View Persona Management; please consult the relevant VMware documentation for detailed instructions.

Main VMware Persona Settings

These settings control the main Persona parameters.

Enable VMware Persona Settings Management. This checkbox controls whether the Agent processes Persona settings management instructions. If it is cleared, none of the Persona settings are processed.

Manage User Persona. When enabled, the user's persona settings are managed dynamically. The profile upload interval is used to determine how often to upload profile changes to the network.

Enable Persona Repository Location. This setting controls the UNC path to the repository where user profiles are stored.

Override Active Directory User Profile Path. If enabled, the AD user profile path is overridden with the Persona repository location if both have been configured.

Remove Local Persona at Logoff. When enabled, each user's locally stored profile is removed at log off.

Remove Locally Stored Personas When Users Log Off. If enabled, Local Settings and AppData\Local are deleted when the persona is removed.

Roam Local Settings Folders. When enabled, the local settings folders are roamed along with the rest of the user's profile.

Enable Background Download for Laptops. When enabled, laptop users are allowed to background download their profile.

Cleanup CLFS Files. If enabled, CLFS logs are removed at logoff.

Desktop UI/Logging

Hide Local Offline File Icon. When enabled, the offline icon is hidden when locally viewing most offline persona files.

Show Progress When Downloading Large Files. When enabled, a progress window is shown when downloading large files from the persona repository. The minimum file size required to show the progress window can be specified as well.

Show Critical Errors to Users. When enabled, critical tray icon alerts pertaining to replication or network connectivity failure are displayed to the user.

Set Logging Filename. The full pathname of the local View Persona Management log file. This path should include the file name, and cannot be a UNC path.

Set Logging Destination. These settings allow you to specify whether to send log messages to the local log file or the debug port.

Set Logging Flags. These settings allow you to control what messages are logged.

Set Debug Flags. These settings allow you to control what messages are logged in debug mode.

Files and Folders to Preload

Enable Files and Folders to Preload. When enabled, the selected file and folder paths are downloaded at user logon and replicated when files are changed. Exceptions can also be configured.

Windows Roaming Profile Synchronization

Enable Windows Roaming Profile Synchronisation. When enabled, the selected file and folder paths are downloaded at user logon and replicated during logoff. Exceptions can also be configured.

Files and Folders Excluded from Roaming

Enable Files and Folders Excluded from Roaming. When enabled, the selected file and folder paths are completely excluded from roaming. Exceptions can also be configured to select subfolders and files within the folders excluded from roaming that need to be roamed.

Folders to Background Download/Excluded Processes

Enable Folders to Background Download. When enabled, the selected file and folder paths are downloaded in the background after users log on. Exceptions can also be configured.

Enable Excluded Processes. When enabled, the selected processes' I/O is ignored by Persona.

Folder Redirection

These settings allow you to configure redirection for individual user profile folders.

Files and Folders Excluded from Folder Redirection

Enable Files and Folders Excluded from Redirection. When enabled, the selected file and folder paths are completely excluded from redirection. Exceptions can also be configured to select subfolders and files within the folders excluded from redirection that need to be redirected.

Security

September 28, 2018

These settings allow you to control end-user activity within Workspace Environment Management.

Application Security

> **Important:**
>
> To control which applications end users can run, you can use either the Windows AppLocker interface, or Workspace Environment Management to manage Windows AppLocker rules. You can switch between these approaches at any time but we recommend that you do not use both approaches at the same time.

These settings allow you to control the applications users are permitted to run by defining rules. This functionality is similar to Windows AppLocker. When you use Workspace Environment Management to manage Windows AppLocker rules, the agent processes (converts) Application Security tab rules into Windows AppLocker rules on the agent host. If you stop the agent processing rules, they are preserved in the configuration set and AppLocker continues running by using the last set of instructions processed by the agent.

Application Security

This tab lists the application security rules in the current Workspace Environment Management configuration set. You can use **Find** to filter the list according to a text string.

When you select the top-level item "Application Security" in the Security tab, the following options become available to enable or disable rule processing:

Process Application Security Rules. When selected, the Application Security tab controls are enabled and the agent processes rules in the current configuration set, converting them into AppLocker rules on the agent host. When not selected, the Application Security tab controls are disabled and the agent does not process rules into AppLocker rules. (In this case AppLocker rules are not updated.)

> **Note:**
>
> This option is not available if the Workspace Environment Management administration console is installed on Windows 7 SP1 or Windows Server 2008 R2 SP1 (or earlier versions).

Process DLL Rules. When selected, the agent processes DLL rules in the current configuration set into AppLocker DLL rules on the agent host. This option is only available when you select **Process Application Security Rules**.

> **Important:**
>
> If you use DLL rules, you must create a DLL rule with "Allow" permission for each DLL that is used by all the allowed apps.
>
> **Caution:**
>
> If you use DLL rules, users may experience a reduction in performance. This happens because AppLocker checks each DLL that an app loads before it is allowed to run.

Rule collections

Rules belong to AppLocker rule collections. Each collection name indicates how many rules it contains, for example (12). Click a collection name to filter the rule list to one of the following collections:

- **Executable Rules**. Rules which include files with the .exe and .com extensions that are associated with an application.
- **Windows Rules**. Rules which include installer file formats (.msi, .msp, .mst) which control the installation of files on client computers and servers.
- **Script Rules**. Rules which include files of the following formats: .ps1, .bat, .cmd, .vbs, .js.
- **Packaged Rules**. Rules which include packaged apps, also known as Universal Windows apps. In packaged apps, all files within the app package share the same identity. Therefore, one rule can control the entire app. Workspace Environment Management supports only publisher rules for packaged apps.
- **DLL Rules**. Rules which include files of the following formats: .dll, .ocx.

When you filter the rule list to a collection, the **Rule enforcement** option is available to control how AppLocker enforces all rules in that collection on the agent host. The following rule enforcement values are possible:

Off (default). Rules are created and set to "off," which means they are not applied.

On. Rules are created and set to "enforce," which means they are active on the agent host.

Audit. Rules are created and set to "audit," which means they are on the agent host in an inactive state. Windows logs when things are started that would violate these rules were they enforced.

To import AppLocker rules

You can import rules already 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, which you can export.

1. In the ribbon click **Import AppLocker Rules**.

2. Browse to the XML file exported from AppLocker containing your AppLocker rules.

3. Click **Import**.

The rules are added to the Application Security rules list.

To add a rule

1. Select a rule collection name in the sidebar. For example, to add an executable rule select the "Executable Rules" collection.

2. Click **Add Rule**.

3. In the Display section, type the following details:

Name. The display name of the rule as it appears in the rule list.

Description. Additional information about the resource (optional).

4. In the Type section click an option:

Path. The rule matches a file path or folder path.

Publisher. The rule matches a selected publisher.

Hash. The rule matches a specific hash code.

5. In the Permissions section, click whether this rule will **Allow** or **Deny** applications from running.

6. To assign this rule to users or user groups, in the Assignments pane, choose users or groups to assign this rule to. The "Assigned" column shows a "check" icon for assigned users or groups.

Tip: You can use the usual Windows selection modifier keys to make multiple selections, or use **Select All** to select all rows.

Tip: Users must already be in the Workspace Environment Management Users list.

Tip: You can assign rules after the rule is created.

7. Click **Next**.

8. Specify the criteria the rule matches, depending on the rule type you choose:

Path. Specify a file path or folder path the rule to match. When you choose a folder, the rule matches all files inside and below that folder.

Publisher. Specify a signed reference file, and then use the Publisher Info slider to tune the level of property matching.

Hash. Specify a file. The rule matches the hash code of the file.

9. Click **Next**.

10. Add any exceptions you require (optional). In Add exception, choose an exception type then click **Add**. (You can **Edit** and **Remove** exceptions as required.)

11. To save the rule, click **Create**.

To assign rules to users

Select one or more rules in the list, then click **Edit** in the toolbar or context menu. In the editor, select the rows containing the users and user groups you want to assign the rule to, then click **OK**. You can also unassign the selected rules from everyone using **Select All** to clear all selections.

Note: If you select multiple rules and click **Edit**, any rule assignment changes for those rules are applied to all users and user groups you select. In other words, existing rule assignments are merged across those rules.

To add default rules

Click **Add Default Rules**. A set of AppLocker default rules are added to the list.

To edit rules

Select one or more rules in the list, then click **Edit** in the toolbar or context menu. The editor appears allowing you to adjust settings which apply to the selection you made.

To delete rules

Select one or more rules in the list, then click **Delete** in the toolbar or context menu.

To back up application security rules

You can back up all application security rules in your current configuration set. Rules are all exported as a single XML file. You can use **Restore** to restore the rules to any configuration set.
In the ribbon, click **Backup** then select **Security Settings**.

To restore application security rules

You can restore application security rules from XML files created by the Workspace Environment Management Backup command. The restore process replaces the rules in the current configuration set with those rules in the backup. When you switch to or refresh the Security tab, any invalid application security rules are detected. Invalid rules are automatically deleted and listed in a report dialog, which you can export.

During the restore process, you can choose whether you want to restore rule assignments to users and user groups in your current configuration set. Reassignment only succeeds if the backed-up users/groups are present in your current configuration set/active directory. Any mismatched rules are restored but remain unassigned. After restore, they are listed in a report dialog which you can export in CSV format.

1. In the ribbon, click **Restore** to start the restore wizard.

2. Select Security settings, then click **Next** twice.

3. In **Restore from folder**, browse to the folder containing the backup file.

4. Select **AppLocker Rule Settings**, then click **Next**.

5. Confirm whether you want to restore rule assignments or not:

Yes. Restore rules and reassign them to the same users and user groups in your current configuration set.

No. Restore rules and leave them unassigned.

6. To start restoring, click **Restore Settings**.

Process Management

These settings allow you to whitelist or blacklist specific processes.

Process Management

Enable Process Management. This toggles whether process whitelists/blacklists are in effect. If disabled, none of the settings on the **Process BlackList** and **Process WhileList** tabs are taken into account.

> **Note:**
>
> This option only works if the session agent is running in the user's session. To do this use the **Main Configuration** Agent settings to set the **Launch Agent** options (**at Logon**/**at Reconnect**/**for Admins**) to launch according to the user/session type, and set **Agent Type** to "UI". These options are described in Advanced Settings.

Process BlackList

These settings allow you to blacklist specific processes.

Enable Process Blacklist. This enables process blacklisting. Processes must be added by executable name (for example, cmd.exe).

Exclude Local Administrators. Excludes local administrator accounts from the process blacklisting.

Exclude Specified Groups. Allows you to exclude specific user groups from process blacklisting.

Process WhiteList

These settings allow you to whitelist specific processes. Process blacklists and process whitelists are mutually exclusive.

Enable Process Whitelist. This enables process whitelisting. Processes must be added by executable name (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 whitelisting (they are able to run all processes).

Exclude Specified Groups. Allows you to exclude specific user groups from process whitelisting (they are able to run all processes).

Active Directory Objects

September 27, 2018

Use this page to specify the users, computers, groups, and organizational units you want to be managed by Workspace Environment Management.

> **Note:**
>
> You must add users, computers, groups and OUs to Workspace Environment Management 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

1. Select **Add** from the context menu.
2. Enter a user or group name in the Windows Select Users dialog, then click **OK**.

Name. The name of the user or group.

Description. This field is only shown in the **Edit Item** dialog and allows you to specify additional information about the user or group.

Item Priority. This allows you to configure priority between different groups and user accounts. In case of conflict (for example, when mapping network drives), the group or user account with the higher priority will win out.

Item State. This allows you to choose whether a user/group is enabled or disabled. If disabled, it is not available to assign actions to.

To add multiple users

1. Select **Add** from the context menu.
2. Add multiple users or group names in the textbox, separate them with semicolons, and then click **OK**.

Machines

A list of computers which have been added to the current site (configuration set). Only computers listed here are managed by Workspace Environment Management. When agents on these computers register with the infrastructure server it sends them the necessary machine-dependent settings for the configuration set. You can use **Find** to filter the list by name or ID against a text string.

> **Tip:**
>
> To check whether agents on these machines are correctly registered with the infrastructure server, see Agents in the Administration section.

To add a computer or computer group to the current configuration set

1. Use the **Add Object** context menu command or button.
2. In the Select Computers or Groups dialog, select a computer or computer group, then click **OK**.

To add computers in an organizational unit to the configuration set

1. Use the **Add OU** context menu command or button.
2. In the Organizational Units dialog, select an organizational unit, then click **OK**.

To edit computer, computer group, or OU details

1. Select an item in the list.
2. Use the **Edit** context menu command or button.
3. In the Edit item dialog, any of the following details (which are not read-only), then click **OK**.

Name*. The computer, computer group, or OU name.

Distinguished Name*. The distinguished name (DN) of the selected computer or computer group. This field allows you to differentiate different OUs if they have the same Name.

Description. Additional information about the computer, computer group, or OU.

Type*. The selected type (Computer, Group or Organizational Unit)

Item State. The state of the computer, computer group, or OU (enabled or disabled). If disabled, the computer, computer group, or OU is not available to assign actions to.

Item Priority. The priority of the computer, computer group, or OU. In cases of conflict (for example, when mapping network drives), the machine or OU with the higher priority wins.

* Read-only details reported from Active Directory.

Advanced

Options for configuring Active Directory behavior.

Active Directory search timeout. The time period (msec) for Active Directory searches to be performed before they time out. The default value is 1000 msec. We recommend using a timeout value of at least 500 msec to avoid timeouts before searches complete.

Transformer settings

January 31, 2019

These options allow you to configure the Transformer feature. Transformer allows agents to connect as web/application launchers which redirect users to the configured remote desktop interface. Use

Transformer to convert any Windows PC into a high performance thin client using a fully reversible "kiosk" mode.

General

General Settings

These settings control the appearance and basic settings for Transformer.

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/application launcher that redirects the user to the configured remote desktop interface. The user environment is completely 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 frontend for the user's virtual desktop. This is the access URL for your Citrix Virtual Apps or Citrix Virtual Desktops environment.

Custom Title. If enabled, the Workspace Environment Management Agent kiosk window is given a custom title-bar.

Enable Window Mode. If enabled, the Workspace Environment Management Agent kiosk starts in windowed mode. The user is still locked out of their Windows environment.

Allow Language Selection. If enabled, allows users to select what language the Transformer interface is in.

Show Navigation Buttons. If enabled, the "Forward", "Back" and "Home" web navigation buttons display on 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 relaunched.

Process Command Line. Allows you to enter the command line for a specific process (for example, the path to mstsc.exe to launch an RDP connection).

Process Arguments. Allows you to specify any arguments to the command line listed above (for example, in the case of mstsc.exe, the IP address of the machine to connect to).

Clear Last Username for VMware View. If enabled, clears the user name of the previous user on the logon screen when you launch a VMware desktop session.

Enable VMware View Mode. If enabled, allows the process launcher to monitor the virtual applications or desktops running on a user's machine in VMware View mode and to execute **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 execute **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 execute **End of Session Options** when they are all closed.

Advanced & Administration Settings

Fix Browser Rendering. If enabled, forces the kiosk window to run in a browser mode compatible with the version of Internet Explorer (IE) that is currently installed on agent host machines. By default, this forces the kiosk window to run in IE7 compatibility mode.

Log Off Screen Redirection. If enabled, automatically redirects the user to the logon page whenever they land on the logoff page.

Suppress Script Errors. If enabled, suppresses any script errors it encounters.

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, displays the kiosk admin menu at all times – this gives all users access to the kiosk admin menu.

Hide Taskbar & Start Button. If enabled, hides the user’s taskbar and start menu. Otherwise, the user is still able to access their desktop.

Lock Alt-Tab. If enabled, ignores alt tab commands, preventing the user from switching away from the agent.

Fix Z-Order. If enabled, adds a “hide” button to the kiosk interface that allows the user to push the kiosk to the background.

Lock Citrix Desktop Viewer. If enabled, switches the desktop viewer to a locked down mode. This is equivalent to the lockdown that happens when Citrix Workspace app for Windows Desktop Lock is installed. This allows better integration with local applications.

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.

Logon/Logoff & 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 frontend 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

June 11, 2019

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 or not the agent processes actions configured in the Actions tab. These settings apply at login, automatic refresh, or manual (user or administrator triggered) refresh.

Process Applications. When selected, the agent processes application actions.

Process Printers. When selected, the agent processes printer actions.

Process Network Drives. When selected, the agent processes network drives actions.

Process Virtual Drives. When selected, the agent processes virtual drive actions. (Virtual drives are Windows virtual drives or MS-DOS device names which map a local file path to a drive letter.)

Process Registry Values. When selected, the agent processes registry entry actions.

Process Environment Variables. When selected, the agent processes environment variable actions.

Process Ports. When selected, the agent processes port actions.

Process Ini Files Operations. When selected, the agent processes .ini file actions.

Process External Tasks. When selected, the agent processes external task actions.

Process File System Operations. When selected, the agent processes file system operation actions.

Process File Associations. When selected, the agent processes file association actions.

Process User DSNs. When selected, the agent processes user DSN actions.

Agent Service Actions. These settings determine when the agent service processes its instructions.

Launch Agent at Logon. Determines whether or not the agent runs at logon.

Launch Agent at Reconnect. Determines whether or not the agent runs when reconnecting to a published desktop.

Launch Agent for Admins. Determines whether agent runs when a user is an administrator.

Agent Type. Determines whether the user is presented with a user interface (UI) or not (CMD) when interacting with the Agent.

Enable (Virtual) Desktop Compatibility. This setting is necessary for the agent to be launched when the user is logged in to session 1. If you have any users on physical desktops or VDI, select this option.

Execute only CMD Agent in Published Applications. If enabled, the agent will launch in command line mode (CMD) when launching a published application, rather than in UI mode. CMD mode displays a command prompt instead of an agent splash screen.

Cleanup Actions

Options present on this tab control whether the agent deletes the shortcuts or other items (network drives and printers) when the agent refreshes. If you assign actions to a user or user group, you might find that you can also control the creation of the shortcuts or items. You can do so by configuring the options for the actions in the **Assigned** pane of the **Assignments > Action Assignment > Action Assignment** tab. Workspace Environment Management processes these options according to a specific priority:

1. The options present on the **Cleanup Actions** tab
2. The options configured for the assigned actions in the **Assigned** pane

For example, suppose you have enabled the **Create Desktop** option for the assigned application in the **Assigned** pane, and the application shortcut is already created on the desktop. The shortcut is still on the desktop when the agent refreshes, even though you enabled the **Delete Desktop Shortcuts** option on the **Cleanup Actions** tab.

Shortcut Deletion at Startup. The agent deletes all shortcuts of the selected types when it refreshes.

Delete Network Drives at Startup. If enabled, the agent deletes all network drives whenever it refreshes.

Delete Network Printers at Startup. If enabled, the agent deletes all network printers whenever it refreshes.

Preserve Auto-created Printers. If enabled, the agent does not delete auto-created printers.

Preserve Specific Printers. If enabled, the agent does not delete any of the printers in this list.

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 this is disabled, the agent does not fall back on its cache if it cannot connect to the infrastructure service. **Note** In order for Offline Mode to work, SQL Server Compact Edition 3.5 SP2 must be installed in the user environment and on the Workspace Environment Management infrastructure server.

Use Cache Even if Online. If enabled, the agent always reads its settings and actions from its cache (which is built whenever the agent service cycles).

Refresh Settings. If enabled, the agent triggers a Windows refresh when an agent refresh occurs.

Refresh on Environmental Setting Change. If enabled, the agent triggers a Windows refresh when an environmental setting is modified.

Asynchronous Printer Processing. If enabled, the agent processes printers asynchronously from other actions.

Asynchronous Network Drive Processing. If enabled, the agent processes network drives asynchronously from other actions.

Initial Environment/Desktop Cleanup. If enabled, the agent cleans up the environment/desktop at first login only.

Check Application Existence. If enabled, the agent checks that an application is available to the user/group before creating a shortcut to that application.

Expand App Variables. If enabled, variables are expanded by default (see Environment variables for normal behavior when the agent encounters a variable).

Enable Cross-Domain User Group Search. If enabled, the agent queries user groups in all Active Directory domains. **Note**: This is an extremely time-intensive process which should only be selected if necessary.

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 2000 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 2000 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, etc. In most cases this value does not need changing.

Advanced Options

Enforce Execution of Agent Actions. If these settings are enabled, the Agent Host will always refresh those actions, even if no changes have been made.

Revert Unassigned Actions. If these settings are enabled, the Agent Host will delete any unassigned actions when it next refreshes.

Automatic Refresh. If enabled, the Agent Host will refresh automatically. By default, the refresh delay is 30 minutes.

Reconnection Actions

Action Processing on Reconnection. These settings control what actions the Agent Host processes upon reconnection to the user environment.

Advanced Processing

Filter Processing Enforcement. If enabled, these options will force the Agent Host to re-process filters at every refresh.

Service Options

These settings configure the Agent Host service.

Agent Cache Refresh Delay. This setting controls how long the Agent Host service will wait to refresh its cache.

SQL Settings Refresh Delay. This setting controls how long the Agent Host service will wait to refresh its SQL connection settings.

Agent Extra Launch Delay. This setting controls how long the Agent Host service will wait to launch the Agent Host executable.

Enable Debug Mode. This enables verbose logging for all Agent Hosts connecting to this site.

Bypass ie4uinit Check. By default, the Agent Host service will wait for 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 Workspace Environment Management Agent Host will not be 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.

StoreFront

Use this tab to add StoreFront stores to the Workspace Environment Management configuration. You can then assign an Applications Action tab to define shortcuts to applications from in that those stores. For Transformer kiosk-enabled machines, assigned StoreFront Applications Actions appear in the Applications tab in the Transformer kiosk. For more information on StoreFront stores, see StoreFront documentation.

To add a store

1. Click **Add**.
2. Enter details in the **Add Store** dialog, then click **OK**. The store is saved in your configuration set.

Store URL. The URL of the store on which you want to access resources using Workspace Environment Management. The URL must be specified in the form http[s]://hostname[:port], where hostname is the fully qualified domain name of the store and port is the port used for communication with the store if the default port for the protocol is not available.

Description. Optional text describing the store.

To edit a store

Select a store in the list and click **Edit** to change the store URL or description.

To remove a store

Select a store in the list and click **Remove** to remove a store from your configuration set.

To apply changes

Click **Apply** to apply store settings immediately to your agents.

UI Agent Personalization

These options allow you to personalize the look and feel of the Citrix Workspace Environment Management session agent in UI mode, as well as help desk and self-service facilities.

> **Note:**
>
> These options apply to the session agent in UI mode only. They do not apply to the session agent in CMD mode.

UI Agent Options

These settings let you customize the appearance of the session agent (in UI mode only) in the user's environment.

Custom Background Image Path. If entered, will display a custom image when the session agent launches/refreshes, rather than the Citrix Workspace Environment Management logo. The image used must be accessible from the user environment. It is recommended you use a 400*200px .bmp file.

Loading Circle Color. Allows you to modify the color of the loading circle to fit your custom background.

Text Label Color. Allows you to modify the color of the loading text to fit your custom background.

UI Agent Skin. Allows you to select a preconfigured skin to use for dialogs and self service forms (printers/applications). **Note**: This does not change the splash screen.

Hide Agent Splashscreen. If enabled, hides the splash screen when the session agent is loading/refreshing. This takes effect after the session agent has refreshed while the setting is enabled.

Hide Agent Icon in Published Applications. If enabled, published applications do not show the Citrix Workspace Environment Management session agent.

Hide Agent Splashscreen in Published Applications. If enabled, hides the session agent splash screen for published apps running through it.

Only Admins Can Close Agent. If enabled, only administrators can shut down the Citrix Workspace Environment Management session agent.

Allow Users to Manage Printers. If enabled, users can access the Citrix Workspace Environment Management session agent **Manage Printers** menu to assign a default printer and modify print preferences.

Allow Users to Manage Applications. If enabled, users can access the Citrix Workspace Environment Management session agent **Manage Applications** menu to manage where their application shortcuts are created. Shortcuts created in self-healing mode cannot be deleted using this menu.

Prevent Admins to Close Agent. If enabled, administrators cannot shut down the Citrix Workspace Environment Management session agent.

Enable Applications Shortcuts. If enabled, users can run applications from the Manage Applications menu.

Disable Administrative Refresh Feedback. When Administrators force a session agent to refresh from the Administration Console, this options prevents a notification tooltip appearing in the user environment.

Helpdesk Options

These options control the Agent Host's help desk functionalities.

Help Link Action. This field controls what happens when the user clicks on the **Help** command in the Citrix Workspace Environment Management Agent Host.

Custom Link Action. This field controls what happens when the user clicks on the **Support** command in the Citrix Workspace Environment Management Agent Host.

Enable Screen Capture. If enabled, users are given the option to open a screen capture utility. This allows the user to screenshot any errors in their environment, which they can then send to your support staff.

Enable Send to Support Option. If enabled, the user is able to send screenshots and log files directly to the nominated support email address, with the specified template. This requires a working, configured email client.

Custom Subject. If enabled, the support email generated by the Citrix Workspace Environment Management Agent Host screen capture utility is sent with the specified subject.

Email Template. This field allows you to specify a template for the support email generated by the Citrix Workspace Environment Management Agent Host screen capture utility. Note you must configure the email template to include useful information.

See Dynamic tokens for a list of hash-tags which can be used in the email template. **Note** Users are only presented with the option to enter a comment if the **##UserScreenCaptureComment## hashtag** is included in the email template.

Use SMTP to Send Email. If enabled, this will send the support email using SMTP instead of MAPI.

Test SMTP. Tests your SMTP settings as entered above to verify that they are correct.

Power Saving

Shut Down At Specified Time. If enabled, the Agent Host will automatically shut off the environment it is running in at the specified local time.

Shut Down When Idle. If enabled, the Agent Host will automatically shut off the environment it is running in after running idle (no user input) for the specified length of time.

Administration

December 21, 2018

These settings control administrative functions such as delegation, user statistics, and change logging.

Administrators

These options allow you to define Workspace Environment Management administrators (users or groups) and give them permissions to access sites (configuration sets) via the administration console.

Configured Administrators List

A list of configured administrators showing their permission level (**Full Access**, **Read Only** or **Granular Access**, see details below). You can use **Find** to filter the list by name or ID against a text string.

To add an administrator

1. Use the context menu **Add** command.
2. Enter details in the Select Users or Groups dialog, then click **OK**.

Name. The name of the user or group you are currently editing.

Description. Additional information about the user or group.

Global Administrator. Select to specify that the selected user/group is a Global Administrator. Clear to specify that the selected user/group is a Site Administrator. Global Administrators have their permissions applied to all sites (configuration sets). Site Administrators have their permissions configured on a per-site basis.

Permissions. This allows you to specify one of the following levels of access to the selected user/-group. **Note**: Administrators can only view settings which they have access to.

Full Access administrators have full control over every aspect of the specified sites (configuration sets). Only Global Administrators with Full Access can add/delete Workspace Environment Management administrators. Only Global Full Access and Global Read Only administrators can see the **Administration** tab.

Read Only administrators can view the entire console, but cannot modify any settings at all. Only Global Full Access and Global Read Only administrators can see the **Administration** tab.

Granular Access indicates that the administrator has one or more of the following permission sets:

Action Creators can create and manage actions.

Action Managers can create, manage, and assign actions. They cannot edit or delete actions.

Filter Managers can create and manage conditions and rules. Rules that are in use on assigned applications cannot be edited or deleted by Filter Managers.

Assignment Managers can assign resources to users or groups.

System Utilities Managers can manage the System Utilities settings (CPU, RAM and process management).

Policies and Profiles Managers can manage Policies and Profiles settings.

Configured Users Managers can add, edit, and remove users or groups from the configured users list. Users or groups with assigned actions cannot be edited or deleted by Configured Users Managers.

Transformer Managers can manage Transformer settings.

Advanced Settings Managers can manage advanced settings (enabling or disabling action processing, cleanup actions, and so on).

Security Managers can access all controls in the Security tab.

State. This controls whether the selected user/group is enabled or disabled. When disabled, the user/-group is not considered to be a Workspace Environment Management administrator and cannot use the administration console.

Type. This field is read only and indicates whether the selected entity is a user or a group.

If the **Global Administrator** is cleared, the following controls are enabled:

Site Name. All Workspace Environment Management sites (configuration sets) belonging to the database this infrastructure service is connected to.

Enabled. Select to enable this administrator for the specified Workspace Environment Management site (configuration set). When disabled, the user/group is not considered to be an administrator for that site and cannot access it.

Permissions. Select a permission level for the selected user/group for each Workspace Environment Management site (configuration set) attached to this infrastructure service.

Users

This page displays statistics about your Workspace Environment Management installation.

Statistics

This page displays a summary of users whose agent hosts have connected to the database.

Users Summary. Displays a count of total users who have reserved a Workspace Environment Management license, for both the current site (configuration set) and all sites (configuration sets). Also displays a count of new users in the last 24 hours and in the last month.

Users History. This displays connection information for all the users associated with the current site (configuration set), including the last connection time, the name of the machine from which they last connected and the session agent type (UI or CMD) and version. You can use **Find** to filter the list by name or ID against a text string.

Agents

This page displays statistics about the agents in your Workspace Environment Management installation.

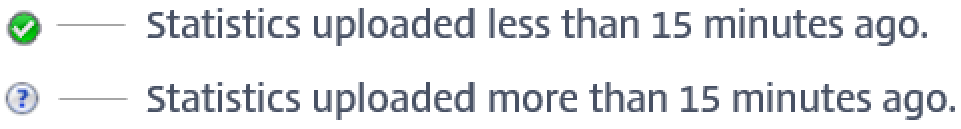
Statistics

This page displays a summary of the Workspace Environment Management agents recorded in the Workspace Environment Management database.

Agents Summary. Displays a count of total agents who have reserved a Workspace Environment Management license, for both the current site (configuration set) and all sites (configuration sets). It also reports agents added in the last 24 hours and in the last month.

Agents History. This displays connection information for all agents registered with this site (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 against a text string.

In the **Synchronization State** column, the following icons indicate when the agent last uploaded statistics to the infrastructure service.



✓ —— Statistics uploaded less than 15 minutes ago.

? —— Statistics uploaded more than 15 minutes ago.

> **Note:**
>
> These icons do *not* indicate that the agent cache is synchronized with the Workspace Environment Management database.)

In the **Profile Management Health Status** column, you can view the health status of Profile Management in 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 warrant action on your part.
- Error (X icon). Indicates that Profile Management is configured incorrectly, which causes Profile Management not to function properly.
- Unavailable (question mark icon). Appears when Profile Management is not found, or not enabled, or the WEM agent is not the latest version.

If the status checks do not reflect your experience or if they do not detect the issues you are having, contact Citrix Technical Support.

To refresh agents

When you refresh an agent it communicates with the infrastructure server. The infrastructure server validates the agent host identity with the Workspace Environment Management database.

1. Click **Refresh** to update the list of agents.
2. In the context menu select **Refresh Workspace Agent(s)**.

Options in the context menu

Refresh Cache. Triggers a refresh of the agent offline cache database. To optimize Windows performance, WEM has an offline cache database that includes a per-machine cache that stores non-user parameters (Microsoft USV, Citrix Profile Management), and a per-user cache that stores user parameters (assigned actions, start menu settings, etc.).

Refresh Agent Host Settings. Triggers an immediate update of the WEM agent host settings.

Refresh Workspace Agent(s). Applies the settings to the agent(s) running on your machine(s).

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**, and then click **Refresh**.

> **Note:**
>
> If the settings are not applied to the agent after configuring **Reset Profile Management Settings** from the WEM administration console, see CTX219086 for a workaround.

Reset Vmware Persona Settings. Clears the registry cache and updates the associated configuration settings. If VMware Persona Settings are not applied to your agent, click **Reset Vmware Persona Settings**, and then click **Refresh**.

Reset Microsoft Usv Settings. Clears the registry cache and updates the associated configuration settings. If Microsoft USV Settings are not applied to your agent, click **Reset Microsoft Usv Settings**, and then click **Refresh**.

Refresh Profile Management Configuration Check. Performs status checks on your agent host(s) to determine whether Profile Management is configured optimally.

Delete Record. Enables deletion of the agent record from the database. If the agent is still active, this option is grayed out.

Registrations

This page shows the registration status of the Workspace Environment Management agents recorded in the database.

> **Important:**
>
> Agents must only be registered with 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).

Agent is bound to multiple sites. The infrastructure server cannot resolve a site (configuration set) for this agent because the agent is bound to more than one site (configuration set).

To resolve registration errors

Either

- edit the Active Directory hierarchy (relations between computers, computer groups, and OUs)

OR

- edit the Workspace Environment Management hierarchy (in the Active Directory Objects section of the administration console) so that a computer binds to only one site (configuration set).

After making these changes, refresh agents with the infrastructure server.

Logging

Administrative

This tab displays a list of all changes made to the Workspace Environment Management settings in the database. By default, the log is unpopulated until the log is refreshed manually.

Filtering Options. These options allow you to filter the log by site (configuration set), and date range.

Export Log. Exports the log in XLS format.

Refresh Log. Refreshes the log.

Clear Log. Clears the log for all configuration sets. ***This cannot be undone***. Clearing the log adds one event in the new log indicating this has been done. This option is only available to Global Full Access administrators.

Agent

This tab lists all changes made to your Workspace Environment Management agents. The log is unpopulated until you click **Refresh**.

Filtering Options. These options allow you to filter the log by site (configuration set), and date range.

Export Log. Exports the log in XLS format.

Refresh Log. Refreshes the log.

Clear Log. Clears the log for all configuration sets. ***This cannot be undone***. Clearing the log adds one event in the new log indicating this has been done. This option is only available to Global Full Access administrators.

Monitoring

May 18, 2018

These pages contain detailed user login and machine boot reports. You can **Export** all reports in various formats.

Daily Reports

Daily Login Report. A daily summary of login times across all users connected to this site. You can double-click a category for a detailed view showing individual logon times for each user on each device.

Daily Boot Report. A daily summary of boot times across all devices connected to this site. You can double-click a category for a detailed view showing individual boot times for each device.

User Trends

Login Trends Report. This report displays overall login trends for each day over the selected period. You can double-click each category of each day for a detailed view.

Boot Trends Report. This report displays overall boot trends for each day over the selected period. You can double-click each category of each day for a detailed view.

Device Types. This report displays a daily count of the number of devices of each listed operating system connecting to this site. You can double-click each device type for a detailed view.

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.

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.

Port information

September 25, 2018

Workspace Environment Management uses the following ports.

Source	Destination	Type	Port	Details
Infrastructure service	Agent host	TCP	49752	“Agent port”. Listening port on the agent host which receives instructions from the infrastructure service.
Administration console	Infrastructure service	TCP	8284	“Administration port”. Port on which the administration console connects to the infrastructure service.
Agent	Infrastructure service	TCP	8286	“Agent service port”. Port on which the agent connects to the infrastructure server.

Source	Destination	Type	Port	Details
Agent cache synchronization process	Infrastructure service	TCP	8285	"Cache synchronization port". Port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server.
Infrastructure service	Citrix License Server	TCP	27000	"Citrix License Server port". The port on which the Citrix License Server is listening and to which the infrastructure service then connects to validate licensing.
Infrastructure service	Citrix License Server	TCP	7279	The port used by the dedicated Citrix component (daemon) in the Citrix License Server to validate licensing.

Source	Destination	Type	Port	Details
Monitoring service	Infrastructure service	TCP	8287	“WEM monitoring port”. Listening port on the infrastructure server used by the monitoring service. (Not yet implemented.)

Dynamic tokens

February 21, 2019

You can use dynamic tokens in any Workspace Environment Management actions to make them more powerful.

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:

```
#Left(string,length)#
#Right(string,length)#
#Truncate(string,length)#

&Trim(string)&
&RemoveSpaces(string)&
&Expand(string)&

$Split(string,[splitter],index)$

#Mid(string,startindex)#
!Mid(string,startindex,length)!
```

> **Note:**
>
> All Operators are case sensitive. String operations are also supported with hashtags and Active Directory attributes. In cases where your string operations are nested, **Mid** operations are always performed last.

Hashtags

Hash-tags are a replacement feature widely in Workspace Environment Management item processing. 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.

The following hash-tags have been implemented for general use:

```
##UserName##
##UserProfile##
##FullUserName##
##UserInitials##
##UserAppData##
##UserPersonal##
##UserDocuments##
##UserDesktop##
##UserFavorites##
##UserTemplates##
##UserStartMenu##
##UserStartMenuPrograms##
##ComputerName##
##ClientName##
##ClientIPAddress##
##ADSite##
##DefaultRegValue##
##UserLDAPPath##
##VUEMAgentFolder##
##RDSSessionID##
##RDSSessionName##
##ClientRemoteOS##
##ClientOSInfos##
```

Hash-tag **##UserScreenCaptureComment##** is implemented for use in specific parts of the product. This tag can be included in the Email Template under **Advanced Settings** > **UI Agent Personalization** > **Helpdesk Options**. When included, users are presented with a comment field located below the screen capture in the agent screen capture utility. The comment is included in the support email at the location at which you placed the tag in the email template.

> **Note:**
>
> All Hashtags are case sensitive.

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 organizatioanl 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:**
>
> - All **AD** attributes are case sensitive.
> - 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 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##.

Common Control Panel applets

May 18, 2018

The following Control Panel applets are common in Windows:

Applet name	**Canonical name**
Action Center	Microsoft.ActionCenter
Administrative Tools	Microsoft.AdministrativeTools
AutoPlay	Microsoft.AutoPlay
Biometric Devices	Microsoft.BiometricDevices
BitLocker Drive Encryption	Microsoft.BitLockerDriveEncryption
Color Management	Microsoft.ColorManagement
Credential Manager	Microsoft.CredentialManager
Date and Time	Microsoft.DateAndTime
Default Programs	Microsoft.DefaultPrograms
Device Manager	Microsoft.DeviceManager
Devices and Printers	Microsoft.DevicesAndPrinters
Display	Microsoft.Display
Ease of Access Center	Microsoft.EaseOfAccessCenter
Family Safety	Microsoft.ParentalControls
File History	Microsoft.FileHistory
Folder Options	Microsoft.FolderOptions
Fonts	Microsoft.Fonts

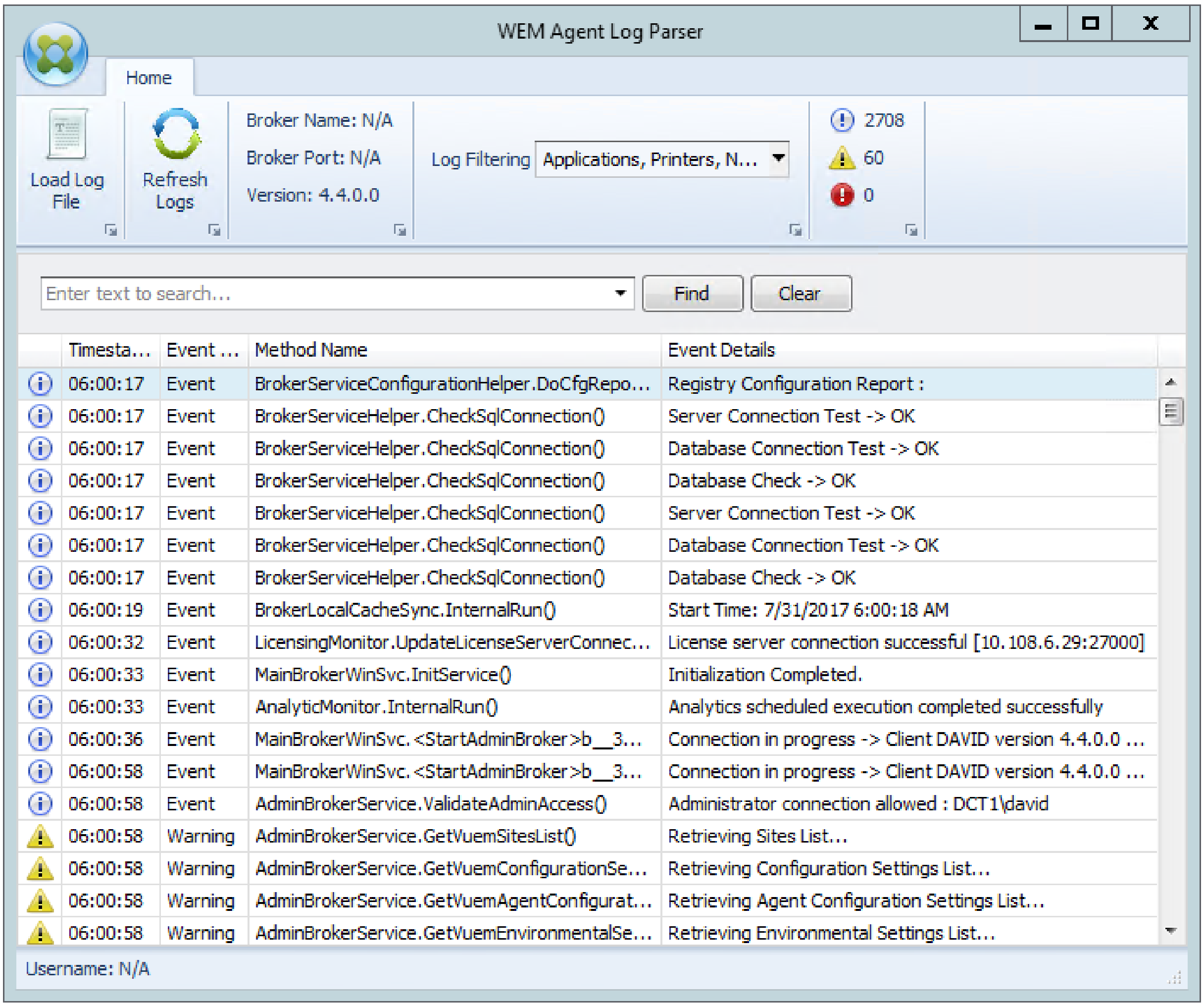
HomeGroup	Microsoft.HomeGroup
Indexing Options	Microsoft.IndexingOptions
Infrared	Microsoft.Infrared
Internet Options	Microsoft.InternetOptions
iSCSI Initiator	Microsoft.iSCSIInitiator
iSNS Server	Microsoft.iSNSServer
Keyboard	Microsoft.Keyboard
Language	Microsoft.Language
Location Settings	Microsoft.LocationSettings
Mouse	Microsoft.Mouse
MPIOConfiguration	Microsoft.MPIOConfiguration
Network and Sharing Center	Microsoft.NetworkAndSharingCenter
Notification Area Icons	Microsoft.NotificationAreaIcons
Pen and Touch	Microsoft.PenAndTouch
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

Log parser

June 16, 2018

Workspace Environment Management includes a log parser application which is located in the agent installation directory:



Broker Name: N/A
Broker Port: N/A
Version: 4.4.0.0

Log Filtering: Applications, Printers, N...

ⓘ 2708
⚠ 60
❗ 0

Enter text to search...

	Timesta...	Event ...	Method Name	Event Details
ⓘ	06:00:17	Event	BrokerServiceConfigurationHelper.DoCfgRepo...	Registry Configuration Report :
ⓘ	06:00:17	Event	BrokerServiceHelper.CheckSqlConnection()	Server Connection Test -> OK
ⓘ	06:00:17	Event	BrokerServiceHelper.CheckSqlConnection()	Database Connection Test -> OK
ⓘ	06:00:17	Event	BrokerServiceHelper.CheckSqlConnection()	Database Check -> OK
ⓘ	06:00:17	Event	BrokerServiceHelper.CheckSqlConnection()	Server Connection Test -> OK
ⓘ	06:00:17	Event	BrokerServiceHelper.CheckSqlConnection()	Database Connection Test -> OK
ⓘ	06:00:17	Event	BrokerServiceHelper.CheckSqlConnection()	Database Check -> OK
ⓘ	06:00:19	Event	BrokerLocalCacheSync.InternalRun()	Start Time: 7/31/2017 6:00:18 AM
ⓘ	06:00:32	Event	LicensingMonitor.UpdateLicenseServerConnec...	License server connection successful [10.108.6.29:27000]
ⓘ	06:00:33	Event	MainBrokerWinSvc.InitService()	Initialization Completed.
ⓘ	06:00:33	Event	AnalyticMonitor.InternalRun()	Analytics scheduled execution completed successfully
ⓘ	06:00:36	Event	MainBrokerWinSvc.<StartAdminBroker>b__3...	Connection in progress -> Client DAVID version 4.4.0.0 ...
ⓘ	06:00:58	Event	MainBrokerWinSvc.<StartAdminBroker>b__3...	Connection in progress -> Client DAVID version 4.4.0.0 ...
ⓘ	06:00:58	Event	AdminBrokerService.ValidateAdminAccess()	Administrator connection allowed : DCT1\david
⚠	06:00:58	Warning	AdminBrokerService.GetVuemSitesList()	Retrieving Sites List...
⚠	06:00:58	Warning	AdminBrokerService.GetVuemConfigurationSe...	Retrieving Configuration Settings List...
⚠	06:00:58	Warning	AdminBrokerService.GetVuemAgentConfigurat...	Retrieving Agent Configuration Settings List...
⚠	06:00:58	Warning	AdminBrokerService.GetVuemEnvironmentalSe...	Retrieving Environmental Settings List...

Username: N/A

The **WEM Agent Log Parser** allows you to open any Workspace Environment Management agent log file, making them searchable and filterable. The parser also summarizes the total number of events, warnings and exceptions (in the top right of the ribbon), as well as details about the log file (the name and port of the infrastructure service it first connected to, as well as the agent version and username).

XML printer list configuration

August 24, 2018

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>
```

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>
```

VUEMUserAssignedPrinter tag syntax

Each configured printer must be defined in a **<VUEMUserAssignedPrinter>** tag, using the following attributes:

<IdPrinter>. This is the Workspace Environment Management printer ID for the configured printer. Each printer must have a different ID. **Note** The XML Printer List action configured in the Workspace Environment Management Administration Console is also a printer action with its own ID which must be different from the ID of printers individually configured in the XML list.

<IdSite>. Contains the site ID for the relevant Workspace Environment Management site, which must match the ID of an existing site.

<State>. Specifies the state of the printer where 1 is active and 0 is disabled.

<ActionType>. Must always be 0.

<UseExtCredentials>. Must be 0. The use of specific Windows credentials is not currently supported.

<isDefault>. If 1, printer is the default Windows printer. If 0, it is not configured as default.

<IdFilterRule>. Must always be 1.

<RevisionId>. Must always be 1. If printer properties are subsequently modified, increment this value by 1 to notify the Agent Host and ensure 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 should be left blank.

<TargetPath>. This is the UNC path to the printer.

<ExtLogin>. Contains the name of the Windows account used when specifying Windows credentials for connection. [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.

```
&gt;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;SelfHealingEnabled&lt;/
    Name&gt;&lt;Value&gt;0&lt;/Value&gt;&lt;/VUEMActionAdvancedOption
```

To activate self-healing for a given printer object, simply copy and paste the above contents, changing the highlight **0** value to **1**.

Example printer object

The following example assigns two active printers on the client or computer **DEVICE1**:

- **HP LaserJet 2200 Series** on UNC path **\\server.example.net\HP LaserJet 2200 Series** (default printer)
- **Canon C5531i Series** printer on UNC path \\server.example.net\Canon C5531i Series

It also assigns one active printer on the client or computer DEVICE2:

- **HP LaserJet 2200 Series** on UNC path **\\server.example.net\HP LaserJet 2200 Series**

```
    <?xml version=”1.0” encoding=”utf-8”?>
      <
         ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
          xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance” xmlns:
         xsd=”http://www.w3.org/2001/XMLSchema”>
        <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
            <Key>DEVICE1</Key>
            <Value>
                <VUEMUserAssignedPrinter>
                    <IdPrinter>1</IdPrinter>
                    <IdSite>1</IdSite>
                    <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”?&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></SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

```
       <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
         <Key>DEVICE2</Key>
         <Value>
             <VUEMUserAssignedPrinter>
                 <IdPrinter>1</IdPrinter>
                 <IdSite>1</IdSite>
                 <State>1</State>
                 <ActionType>0</ActionType>
                 <UseExtCredentials>0</UseExtCredentials>
                 <isDefault>0</isDefault>
                 <IdFilterRule>1</IdFilterRule>
                 <RevisionId>1</RevisionId>
                 <Name>HP LaserJet 2200 Series</Name>
                 <Description />
                 <DisplayName />
                 <TargetPath>\\server.example.net\HP LaserJet 2200 Series</TargetPath>
                 <ExtLogin />
                 <ExtPassword />
                 <Reserved01>&lt;?xml version=”1.0” encoding=”utf-8”?&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance” xmlns:xsd=”http://www.w3.org/2001/XMLSchema”&gt;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;SelfHealingEnabled&lt;/Name&gt;&lt;Value&gt;0&lt;/Value&gt;&lt;/VUEMActionAdvancedOption&gt;&lt;/ArrayOfVUEMActionAdvancedOption&gt;</Reserved01>
             </VUEMUserAssignedPrinter>
         </Value></SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
    </ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

Filter conditions

January 18, 2019

Workspace Environment Management includes the following filter conditions that you use to configure the circumstances under which the agent assigns resources to users. For more information about using these conditions in the administration console, see Filters.

When using the filter conditions listed in the tables below, be aware of the following two scenarios:

- If the WEM agent is installed on a Windows client:
  - "Client" refers to RDS and VDI client machines that are connected to the machines on which the WEM agent is running (agent host).
  - "Computer" and "Client Remote" refer to the machines on which the WEM agent is running.
- If the WEM agent is installed on a physical Windows device, the conditions that contain "client" in the condition names are not applicable.

Condition Name	**Always True**
Expected value type	N/A
Expected result type	N/A
Expected syntax	N/A
Returns	True.

Condition Name	**ComputerName Match**
Expected value type	N/A
Expected result type	String.
Expected syntax	Single name test: Computername Multiple tests (OR): Computername1;Computername2 Wildcard (also works with multiples): ComputerName*
Returns	True if the current computer name matches the tested value, false otherwise.

Condition Name	**ClientName Match**
Expected value type	N/A
Expected value type	String.

Condition Name	**ClientName Match**
Expected syntax	Single name test: Clientname Multiple tests (OR): Clientname1;Clientname2 Wildcard (also works with multiples): ClientName*
Returns	True if the current client name matches the tested value, false otherwise.

Condition Name	**IP Address Match**
Expected value type	N/A
Expected result type	IP address.
Expected syntax	Single name test: IpAddress Multiple tests (OR): IpAddress1;IpAddress2 Wildcard (also works with multiples): IpAddress* Range (also works with multiples): IpAddress1-IpAddress2
Returns	True if the current computer IP address matches the tested value, false otherwise.

Condition Name	**Client IP Address Match**
Expected value type	N/A
Expected result type	IP address.
Expected syntax	Single name test: ClientIpAddress Multiple tests (OR): ClientIpAddress1;ClientIpAddress2 Wildcard (also works with multiples): ClientIpAddress* Range (also works with multiples): IpAddress1-IpAddress2
Returns	True if the current client IP address matches the tested value, false otherwise.

Condition Name	**Active Directory Site Match**
Expected value type	N/A
Expected result type	Exact name of the Active Directory site to test.

Condition Name	**Active Directory Site Match**
Expected syntax	Active directory site name.
Returns	True if the specified site matches the current site, false otherwise.

Condition Name	**Scheduling**
Expected value type	N/A
Expected result type	Day of week (example: Monday).
Expected syntax	Single name test: DayOfWeek Multiple tests (OR): DayOfWeek1; DayOfWeek2
Returns	True if today matches the tested value, false otherwise.

Condition Name	**Environment Variable Match**
Expected value type	String. Name of the tested variable.
Expected result type	String. Expected value of the tested variable.
Expected syntax	Single name test: value Not null test: ?
Returns	True if environment variable exists and value matches, false otherwise.

Condition Name	**Registry Value Match**
Expected value type	String. Full path and name of the registry value to test. Example: Registry Key **HKCU\Software\Citrix\TestValueName**
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. https://msdn.microsoft.com/en-us/library/aa392902(v=vs.85).aspx
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.
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

Condition Name	**User SBC Resource Type**
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 Virtual Apps Version Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Version. Example: 6.5
Expected syntax	N/A
Returns	True if version matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Apps Farm Name Match**
Expected value type	N/A

Condition Name	**Citrix Virtual Apps Farm Name Match**
Expected result type	String. Citrix Virtual Apps Farm Name (up to version 6.5). Example: Farm.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Apps Zone Name Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Zone Name (up to version 6.5). Example: Zone.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Desktops Farm Name Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Desktops Farm Name (up to version 5). Example: Farm.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Desktops Desktop Group Name Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Desktops Desktop Group Example: Group.
Expected syntax	N/A

Condition Name	**Citrix Virtual Desktops Desktop Group Name Match**
Returns	True if name matches the selected value, false otherwise.

Condition Name	**Citrix Provisioning Image Mode**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current Citrix Provisioning image mode matches the selected value, false otherwise.

Condition Name	**Client OS**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current client operating system matches the selected value, false otherwise.

Condition Name	**Active Directory Path Match**
Expected value type	N/A
Expected result type	String. Name of the tested Active Directory Path.
Expected syntax	Single name test: strict LDAP path matching Wildcard test: OU=Users* Multiple entries: separate entries with semicolon (;)
Returns	True if attribute exists and the value matches, false otherwise.

Condition Name	**Active Directory Attribute Match**
Expected value type	String. Name of the tested Active Directory attribute.
Expected result type	String. Expected value of the tested Active Directory attribute.
Expected syntax	Single value test: value Multiple value entries: separate entries with semicolon (;) Test for not null: ?
Returns	True if attribute exists and the value matches, false otherwise.

Condition Name	**Name or Value is in List**
Expected value type	String. Full file path of the XML list generated by the Integrity List manager utility.
Expected result type	String. Expected value of the name/value to look for in the list.
Expected syntax	String
Returns	True if the value is found in the name/value pairs in the specified list, false otherwise.

Condition Name	**No ComputerName Match**
Negative condition behavior	Executes **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	Executes 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	Executes 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	Executes Client IP Address Match and returns the opposite result (true if false, false if true). See condition **Client IP Address Match** for more information.

Condition Name	**No Active Directory Site Match**
Negative condition behavior	Executes 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	Executes 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	Executes 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	Executes 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	Executes User Country Match and returns the opposite result (true if false, false if true). See condition **User Country Match **for more information.

Condition Name	**No User UI Language Match**
Negative condition behavior	Executes 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 Citrix Virtual Apps Version Match**
Negative condition behavior	Executes 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	Executes 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	Executes 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	Executes 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 Desktop Group Name Match**
Negative condition behavior	Executes Citrix Virtual Desktops Desktop Group Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Desktops Desktop Group Name Match** for more information.

Condition Name	**No Active Directory Path Match**
Negative condition behavior	Executes 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	Executes 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	Executes Name or Value is in List and returns the opposite result (true if false, false if true). See condition **Name or Value is in List** for more information.

Condition Name	**Client Remote OS Match**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current remote client operating system matches selected value, false otherwise.

Condition Name	**No Client Remote OS Match**
Negative condition behavior	Executes 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: ?

Condition Name	**Dynamic Value Match**
Returns	True if dynamic expression result value exists and value matches, false otherwise.

Condition Name	**No Dynamic Value Match**
Negative condition behavior	Executes Dynamic Value Match and returns the opposite result (true if false, false if true). See condition **Dynamic Value Match** for more information.

Condition Name	**Transformer Mode State**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current Transformer state matches selected value, false otherwise.

Condition Name	**No Client OS Match**
Negative condition behavior	Executes 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

Condition Name	**Active Directory Group Match**
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	Executes Active Directory Group Match and returns the opposite result (true if false, false if true). See condition **Active Directory Group Match** for more information.

Condition Name	**File Version Match**
Expected value type	String. Full path and name of the file to test.
	Example: **C:\Test\TestFile.dll**
Expected result type	String. Expected file version value of the tested file.
Expected syntax	Single name test: value Not null test: ?
Returns	True if registry value exists and value matches, false otherwise.

Condition Name	**No File Version Match**
Negative condition behavior	Executes 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

Condition Name	**Network Connection State**
Returns	True if current network connection state matches selected value, false otherwise.

Condition Name	**Published Resource Name**
Expected value type	N/A
Expected result type	String. Name of the published resource (Citrix Virtual Apps/Citrix Virtual Desktops/RDS).
Expected syntax	Single name test: published resource name Multiple tests (OR): Name1;Name2 Wildcard test: Name*
Returns	True if the current published resource name matches the tested value, false otherwise.

Condition Name	**Name is in List**
Expected value type	String. Full file path of the XML list generated by the Integrity List manager utility.
Expected result type	String. Expected value of the name to look for in the list.
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	Executes Name is in List and returns the opposite result (true if false, false if true). See condition **Name is in List** for more information.

Condition Name	**File/Folder exists**
Expected value type	N/A
Expected result type	String.
Expected syntax	Full path of the file system entry (file or folder) to test.
Returns	True if the specified file system entry exists, false otherwise.

Condition Name	**File/Folder does not exist**
Negative condition behavior	Executes File/Folder exists and returns the opposite result (true if false, false if true). See condition **File/Folder exists** for more information.

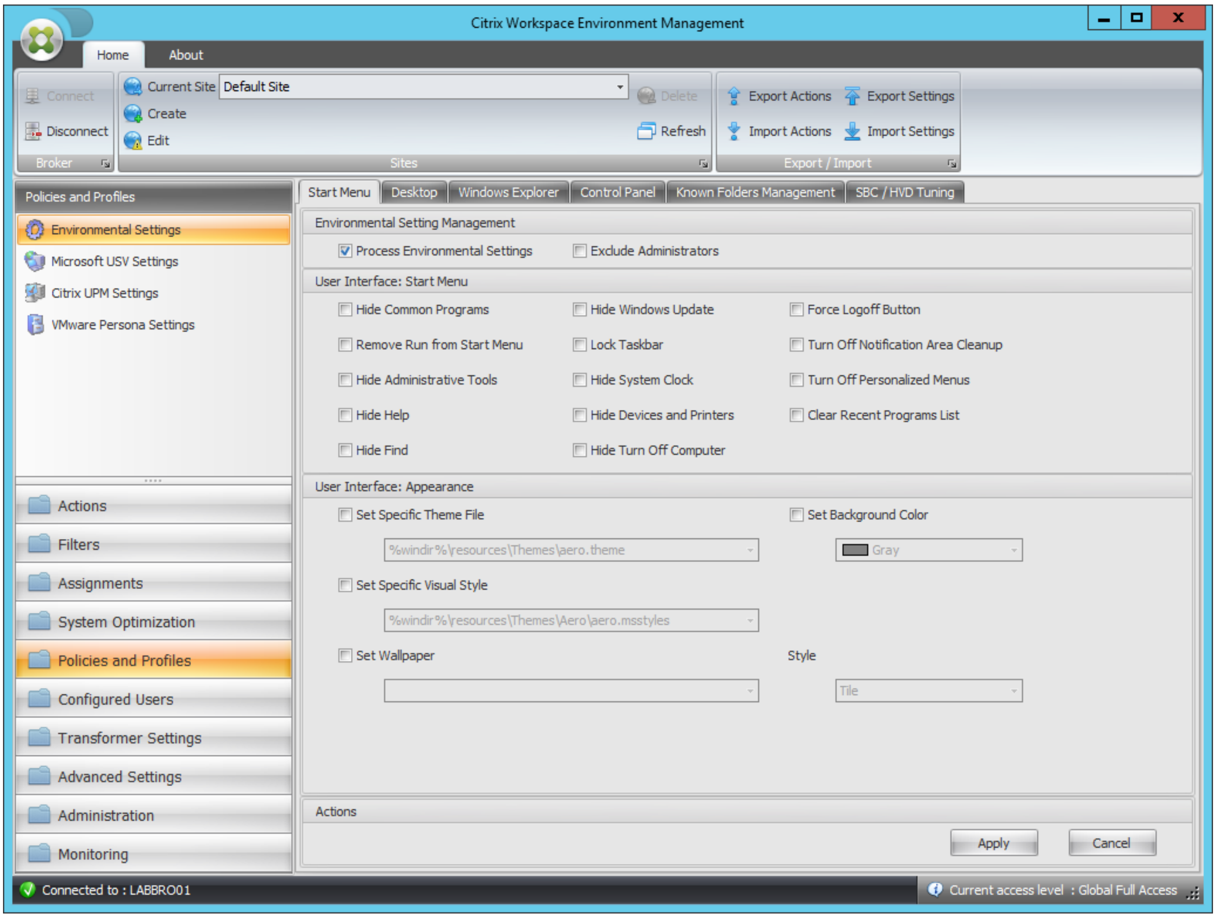
Condition Name	**DateTime Match**
Expected value type	N/A
Expected result type	DateTime as String. Date/time to test.
Expected syntax	Single Date: 06/01/2016 Date Range: 06/01/2016-08/01/2016 Multiple entries: entry1;entry2 Ranges and single dates can be mixed
Returns	True if execution date/time matches any of the specified entry, false otherwise.

Condition Name	**No DateTime Match**
Negative condition behavior	Executes DateTime Match and returns the opposite result (true if false, false if true). See condition **DateTime Match** for more information.

Environmental Settings registry values

September 18, 2018

This article describes the registry values associated with Environmental Settings in Workspace Environment Management.



Environmental Setting Management

☑ Process Environmental Settings ☐ Exclude Administrators

User Interface: Start Menu

☐ Hide Common Programs ☐ Hide Windows Update ☐ Force Logoff Button
☐ Remove Run from Start Menu ☐ Lock Taskbar ☐ Turn Off Notification Area Cleanup
☐ Hide Administrative Tools ☐ Hide System Clock ☐ Turn Off Personalized Menus
☐ Hide Help ☐ Hide Devices and Printers ☐ Clear Recent Programs List
☐ Hide Find ☐ Hide Turn Off Computer

User Interface: Appearance

☐ Set Specific Theme File: %windir%\resources\Themes\aero.theme
☐ Set Background Color: Gray
☐ Set Specific Visual Style: %windir%\resources\Themes\Aero\aero.msstyles
☐ Set Wallpaper
Style: Tile

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
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\
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\
Value Name	NoFind
Value Type	DWORD

Hide Find	
Enabled Value	1
Disabled Value	0
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

Hide System Clock	
Processing	Service called by agent

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
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

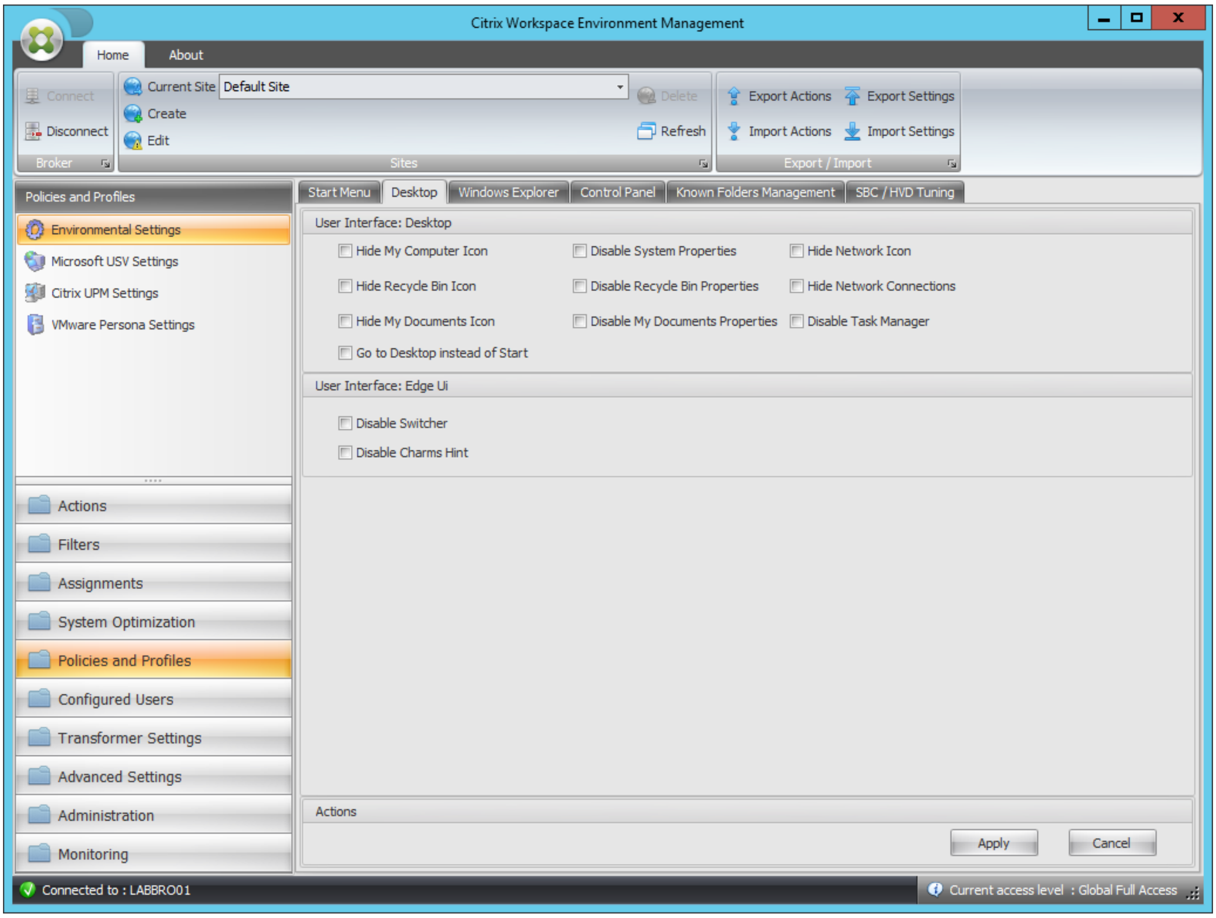
Set Specific Theme File	
Enabled Value	Path specified in console
Disabled Value	Value is absent
Processing	Service at logon

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

Set Wallpaper	
Processing	Service at logon
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



User Interface: Desktop

☐ Hide My Computer Icon ☐ Disable System Properties ☐ Hide Network Icon

☐ Hide Recycle Bin Icon ☐ Disable Recycle Bin Properties ☐ Hide Network Connections

☐ Hide My Documents Icon ☐ Disable My Documents Properties ☐ Disable Task Manager

☐ Go to Desktop instead of Start

User Interface: Edge Ui

☐ Disable Switcher

☐ Disable Charms Hint

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

Hide Recycle Bin Icon	
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
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
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

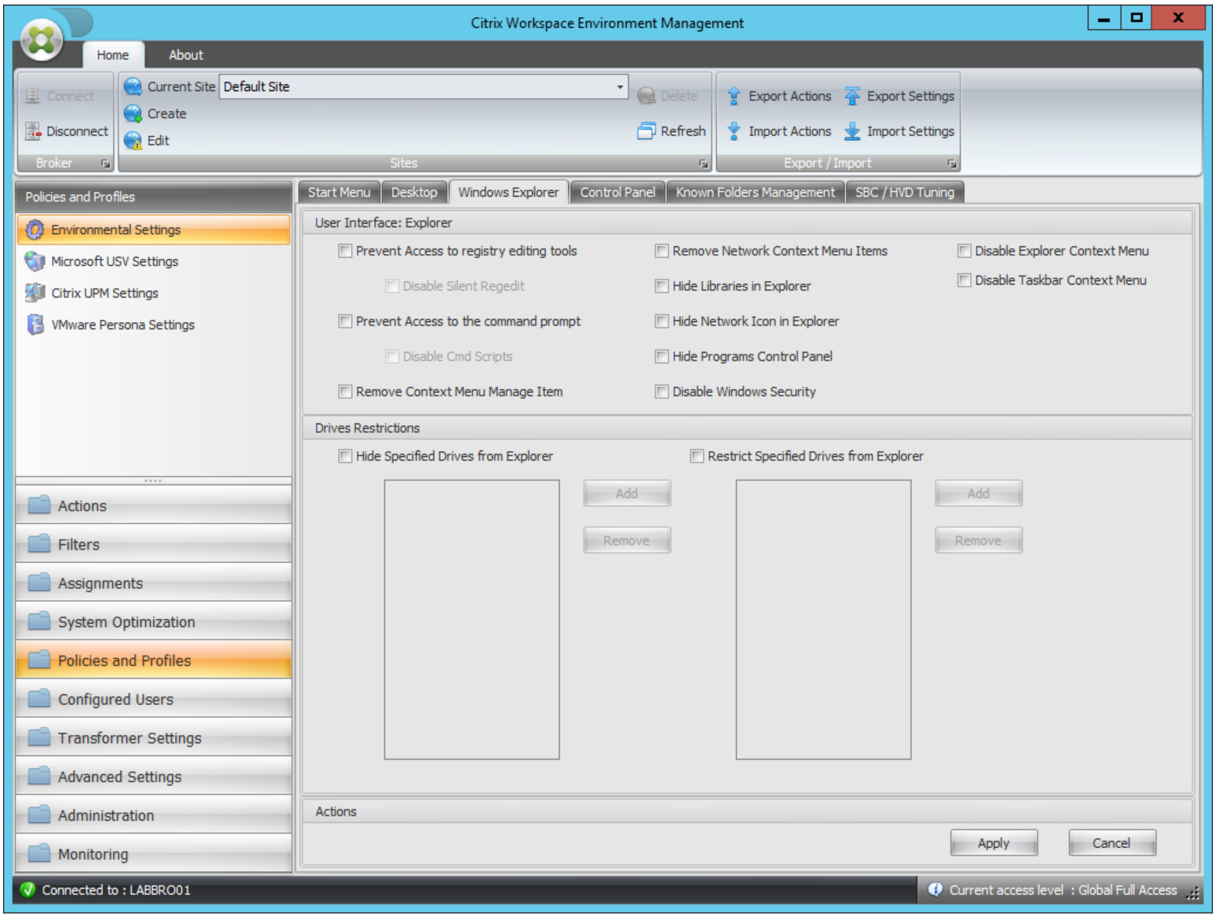
Hide Network Connections	
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

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

Disable Charm Hints	
Processing	Service at logon



User Interface: Explorer

☐ Prevent Access to registry editing tools
☐ Disable Silent Regedit
☐ Prevent Access to the command prompt
☐ Disable Cmd Scripts
☐ Remove Context Menu Manage Item
☐ Remove Network Context Menu Items
☐ Hide Libraries in Explorer
☐ Hide Network Icon in Explorer
☐ Hide Programs Control Panel
☐ Disable Windows Security
☐ Disable Explorer Context Menu
☐ Disable Taskbar Context Menu

Drives Restrictions

☐ Hide Specified Drives from Explorer
☐ Restrict Specified Drives from Explorer

Actions

Connected to : LABBRO01

Current access level : Global Full Access

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
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

Hide Libraries in Explorer	
Enabled Value	1
Disabled Value	0
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

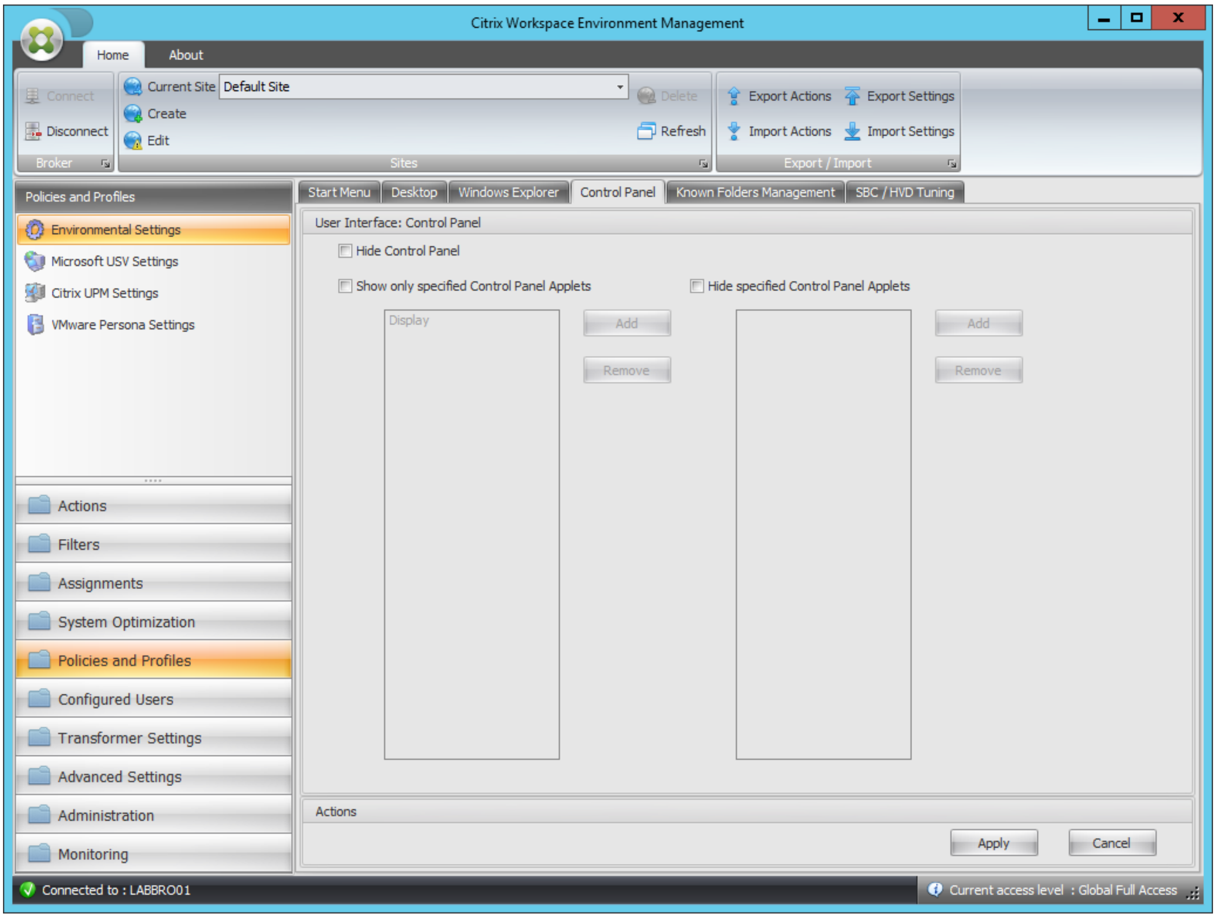
Disable Windows Security	
Processing	Service called by agent

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
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon



Current Site: Default Site

User Interface: Control Panel

□ Hide Control Panel

□ Show only specified Control Panel Applets

□ Hide specified Control Panel Applets

Display

Actions

Connected to : LABBRO01

Current access level : Global Full Access

Hide Control Panel	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoControlPanel
Value Type	DWORD
Enabled Value	1

Hide Control Panel	
Disabled Value	0
Processing	Service called by agent

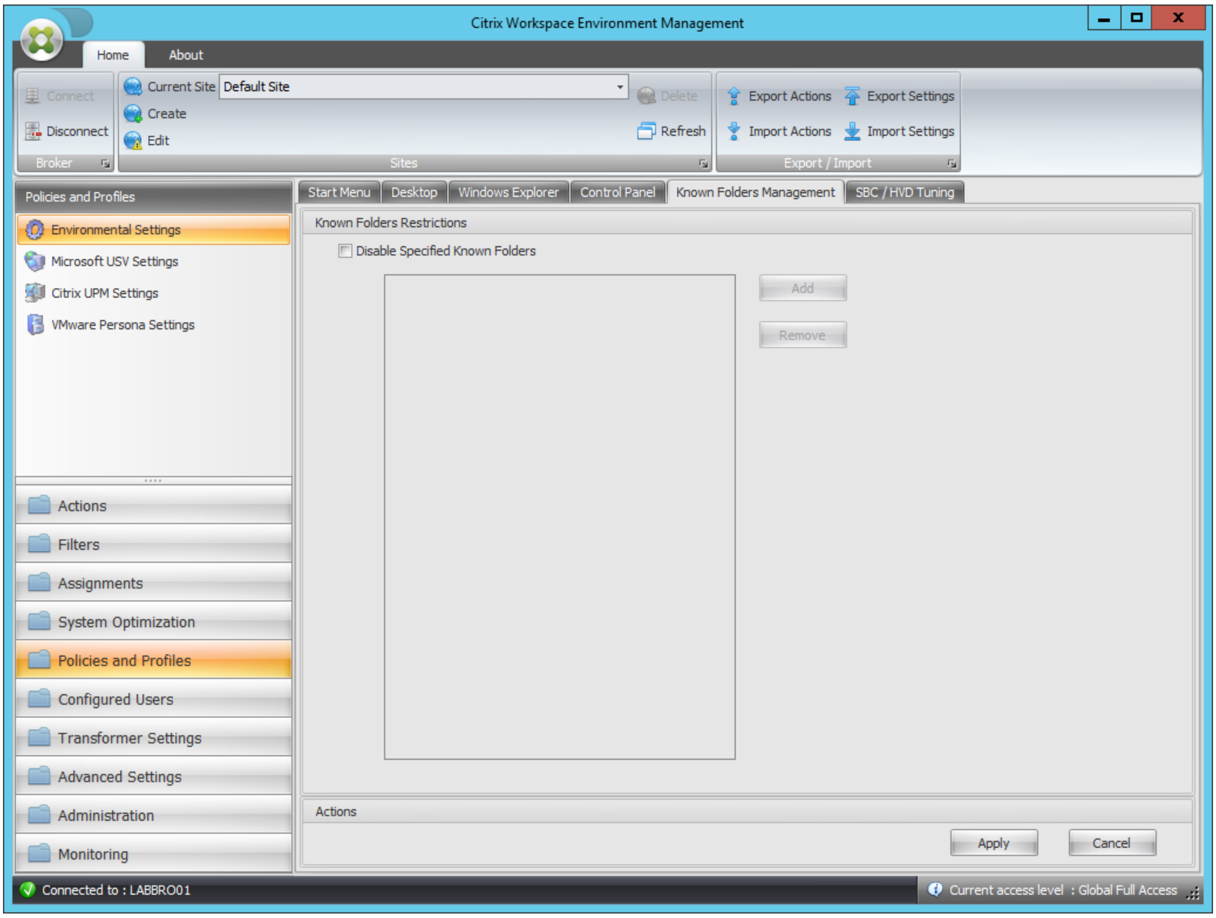
Show only specified Control Panel Applets	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	RestrictCpl
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

Hide specified Control Panel Applets	
Processing	Service called by agent

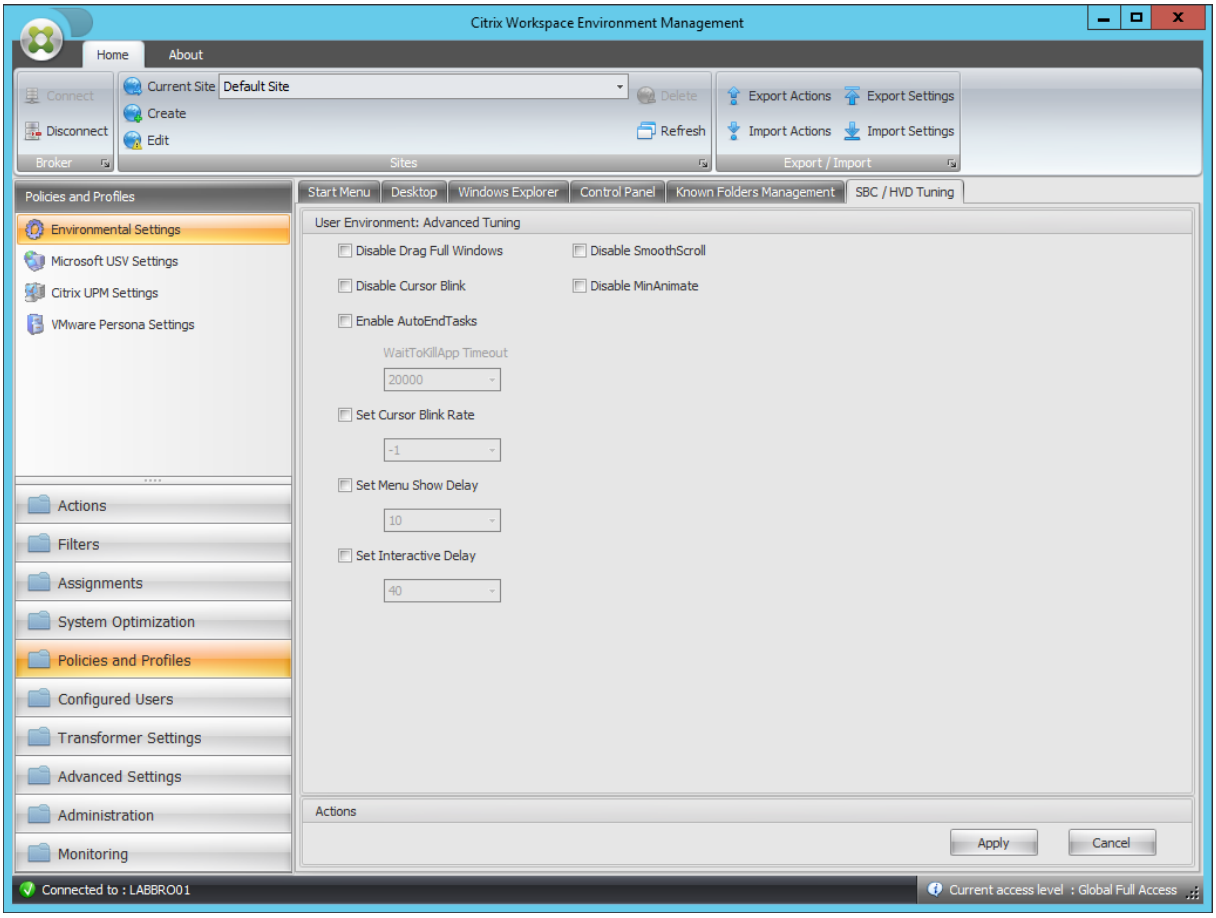
For each disallowed applet	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ DisallowCpl
Value Name	Applet index (starting at 1 and automatically incremented)
Value Type	REG_SZ
Enabled Value	AppletName
Disabled Value	Null / Removed
Processing	Service called by agent



☐ Disable Specified Known Folders

Disable Specified Known Folders	
Parent Key	HKCU\Software\Policies\Microsoft\Windows\Explorer
Value Name	DisableKnownFolders
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon

For each disabled folder	
Parent Key	HKCU\Software\Policies\Microsoft\Windows\Explorer\DisableKnownFolders
Value Name	Disabled folder name
Value Type	REG_SZ
Enabled Value	Disabled folder name
Disabled Value	Null / Removed
Processing	Service at logon



User Environment: Advanced Tuning

□ Disable Drag Full Windows
□ Disable SmoothScroll
□ Disable Cursor Blink
□ Disable MinAnimate
□ Enable AutoEndTasks
WaitToKillApp Timeout: 20000
□ Set Cursor Blink Rate: -1
□ Set Menu Show Delay: 10
□ Set Interactive Delay: 40

Disable Drag Full Windows	
Parent Key	HKCU\Control Panel\Desktop
Value Name	DragFullWindows
Value Type	DWORD
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
Enabled Value	1

Disable Cursor Blink	
Disabled Value	0
Processing	Service at logon

Enable AutoEndTasks	
Parent Key	HKCU\Control Panel\Desktop
Value Name	EnableAutoEndTasks
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)
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

Disable MinAnimate	
Parent Key	HKCU\Control Panel\Desktop
Value Name	MinAnimate
Value Type	DWORD

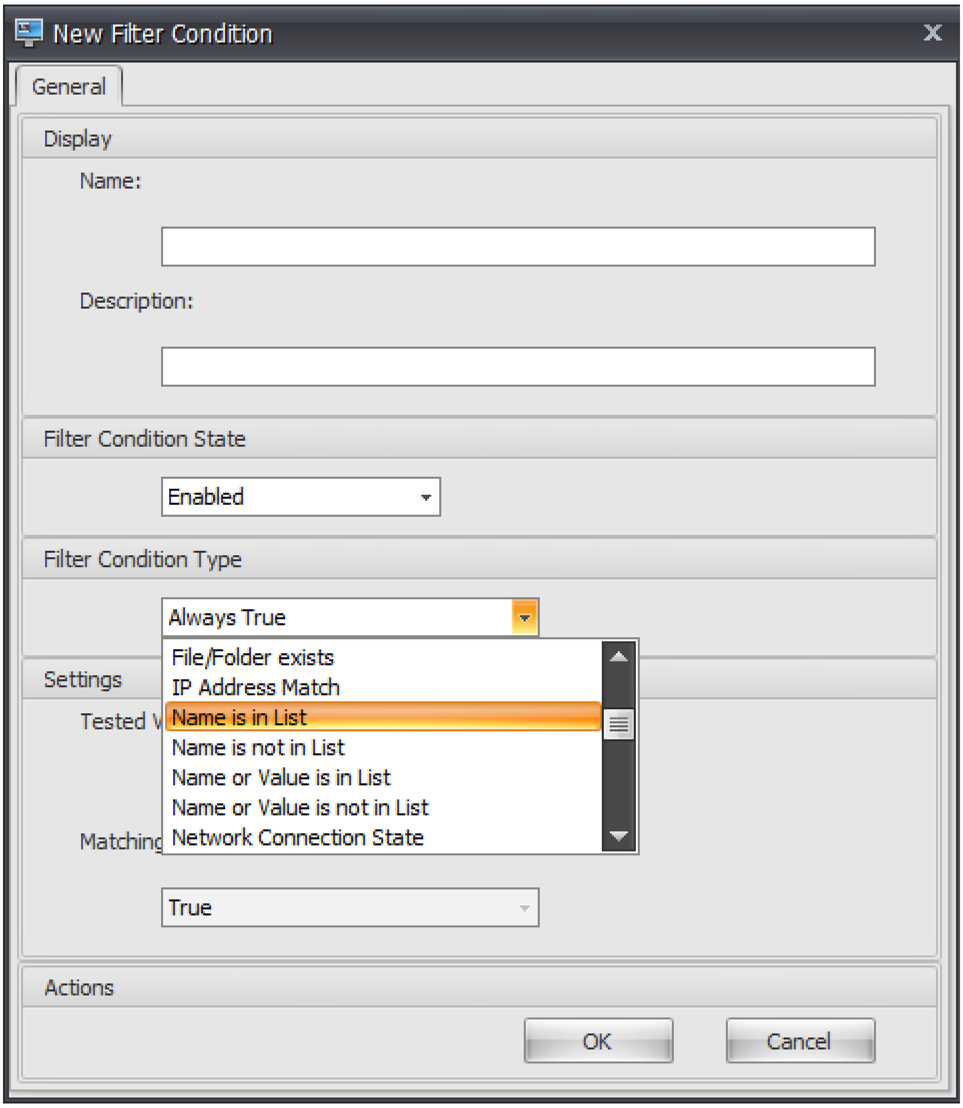
Disable MinAnimate	
Enabled Value	0
Disabled Value	1
Processing	Service at logon

WEM Integrity Condition List Manager

January 3, 2019

WEM Integrity Condition List Manager is a powerful tool that helps you create the XML file for filtering purposes. The tool is used with the following filter condition types: **Name is in List**, **Name is not in List**, **Name or Value is in List**, and **Name or Value is not in List**. For more information about using these conditions in the administration console, see Filters.

This article describes how to use the WEM Integrity Condition List Manager to create the XML file for filtering purposes. For example, suppose you want to filter the actions by using the WEM Integrity Condition List Manager in conjunction with **Name is in List**.



Name:

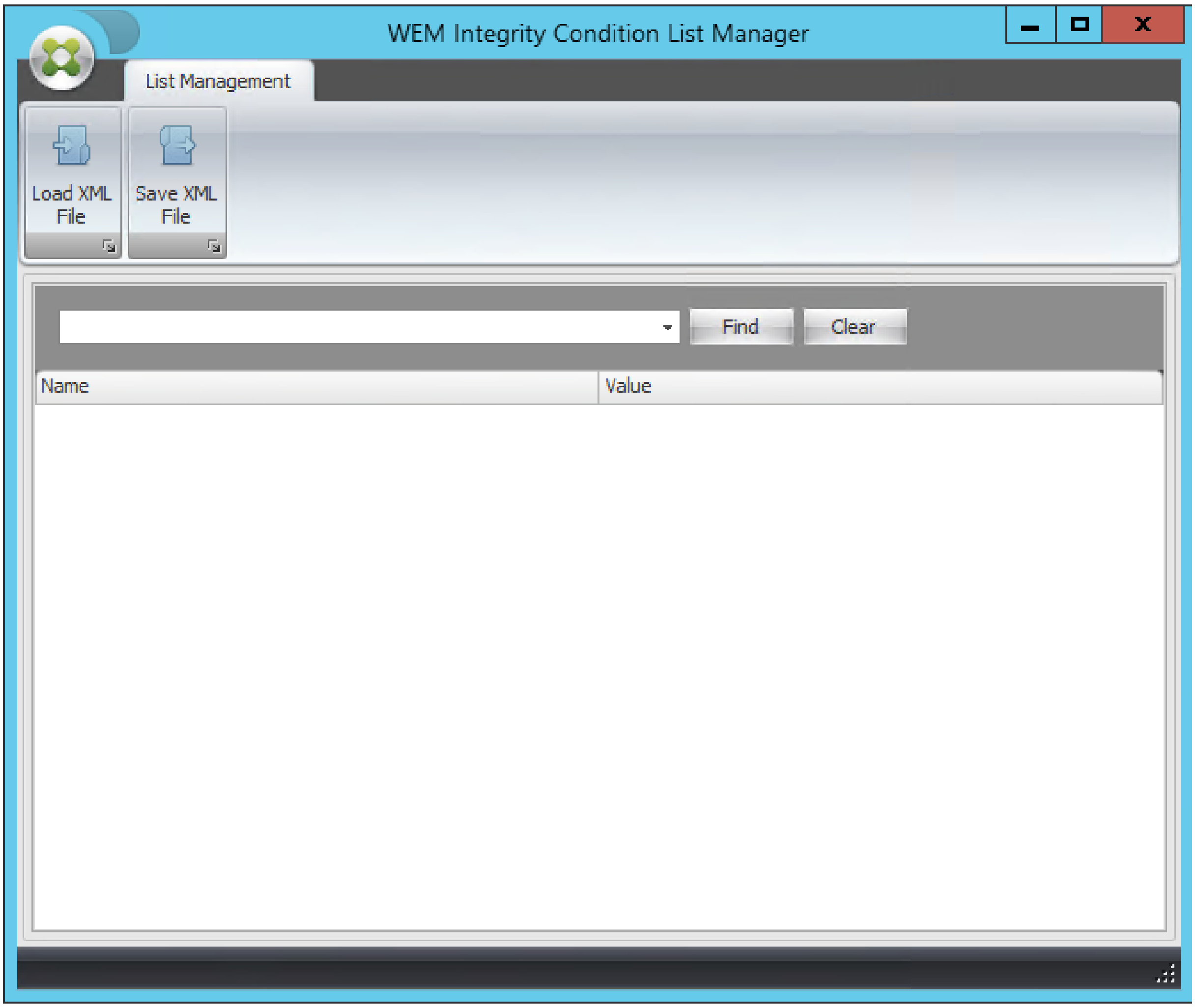
Description:

Filter Condition State: Enabled

Filter Condition Type: Always True

True

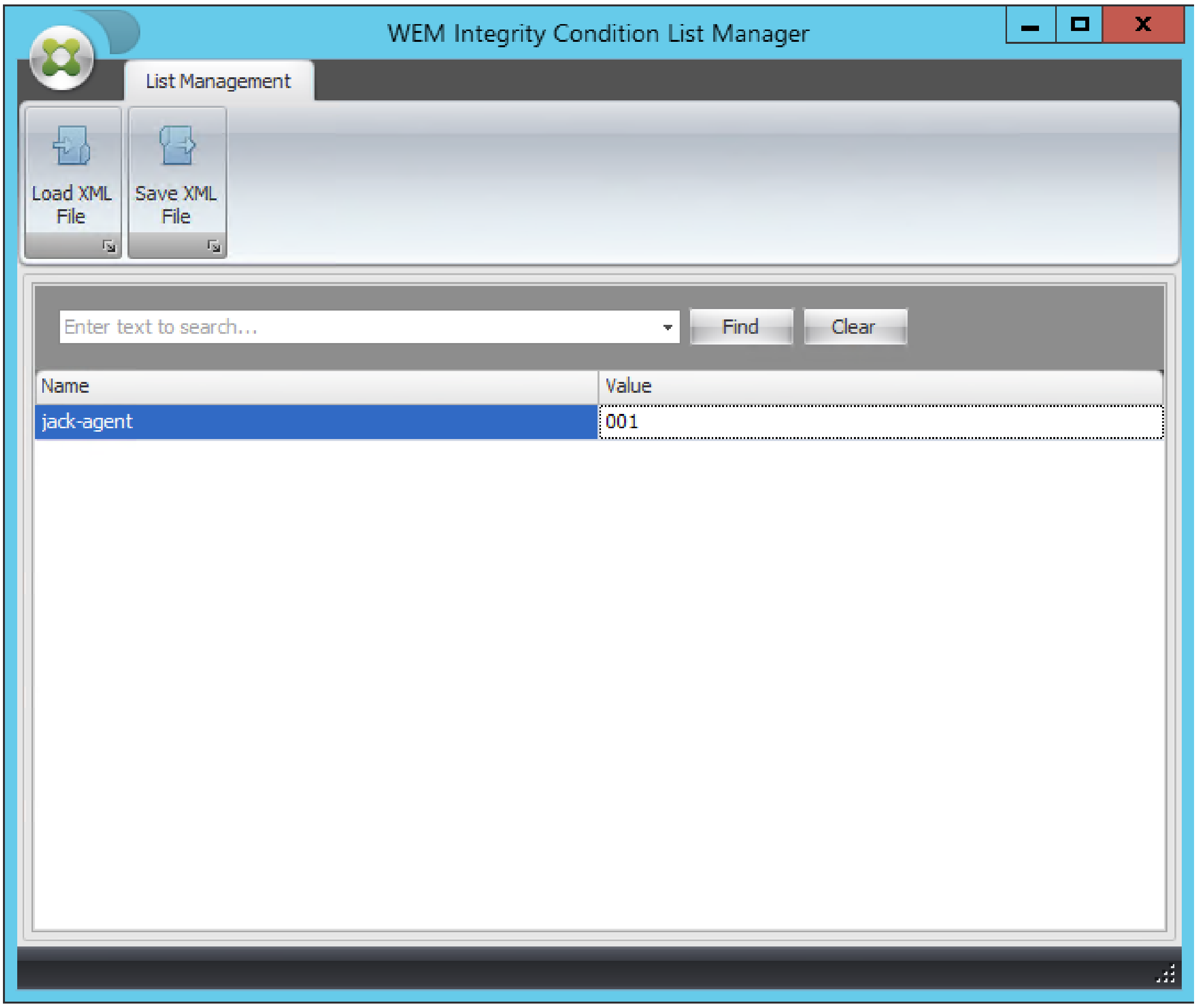
Step 1. Open WEM Integrity Condition List Manager.



Step 2. Right-click the blank area and then select **Add** in the context menu.

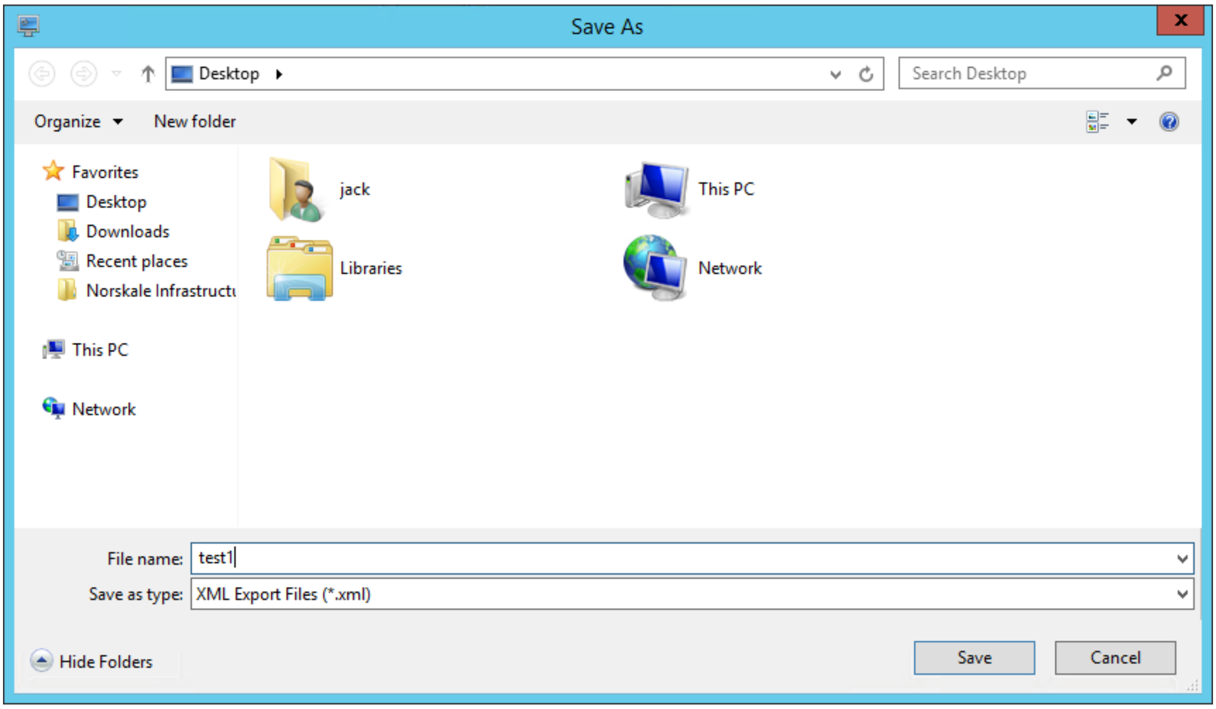
Step 3. Type the name in the **Name** field.

> **Note:**
>
> Type the name of the machine on which the WEM agent is running (agent host).



Name	Value
jack-agent	001

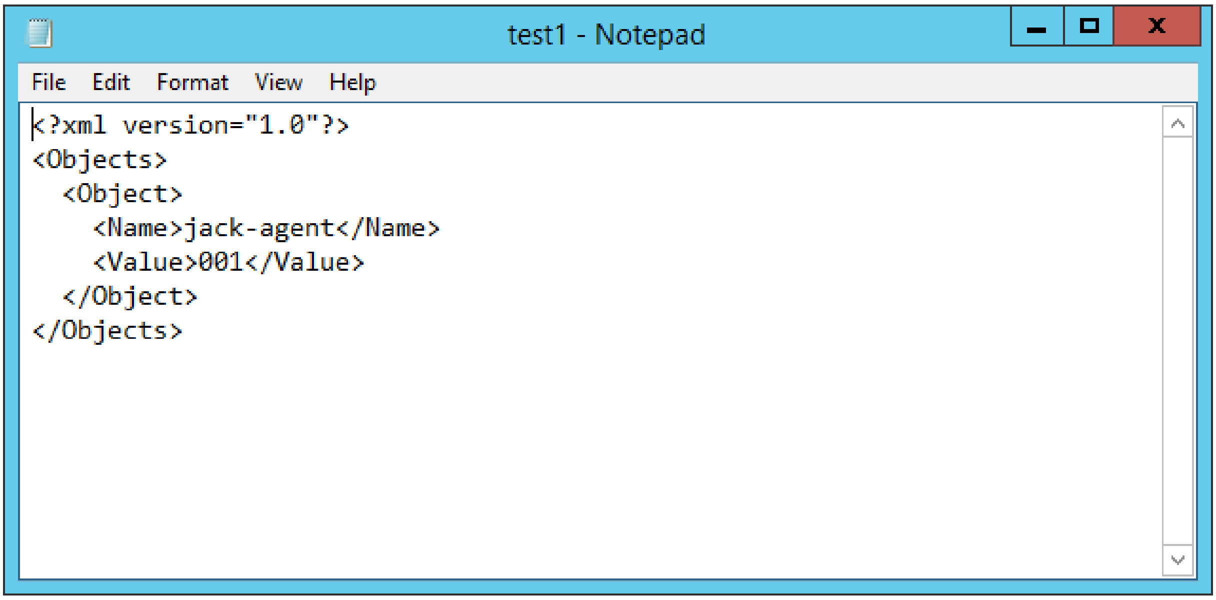
Step 4. Click **Save XML File**, browse to the desired folder, and then click **Save**.



File name: test1

Save as type: XML Export Files (*.xml)

Step 5. Open the saved XML file to verify that the information you provided was saved correctly.

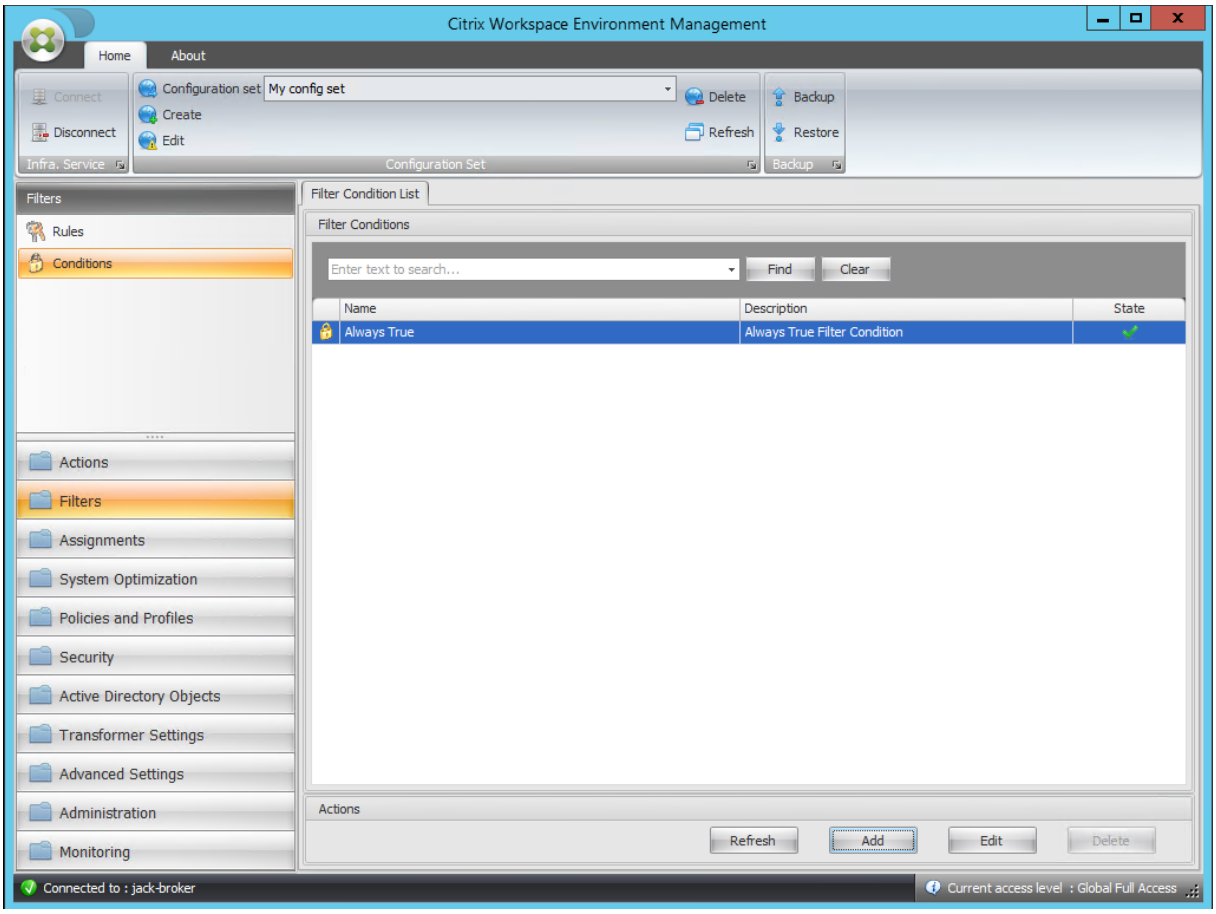


```
<?xml version="1.0"?>
<Objects>
  <Object>
    <Name>jack-agent</Name>
    <Value>001</Value>
  </Object>
</Objects>
```

Step 6. Copy the saved XML file to a folder on the agent host.

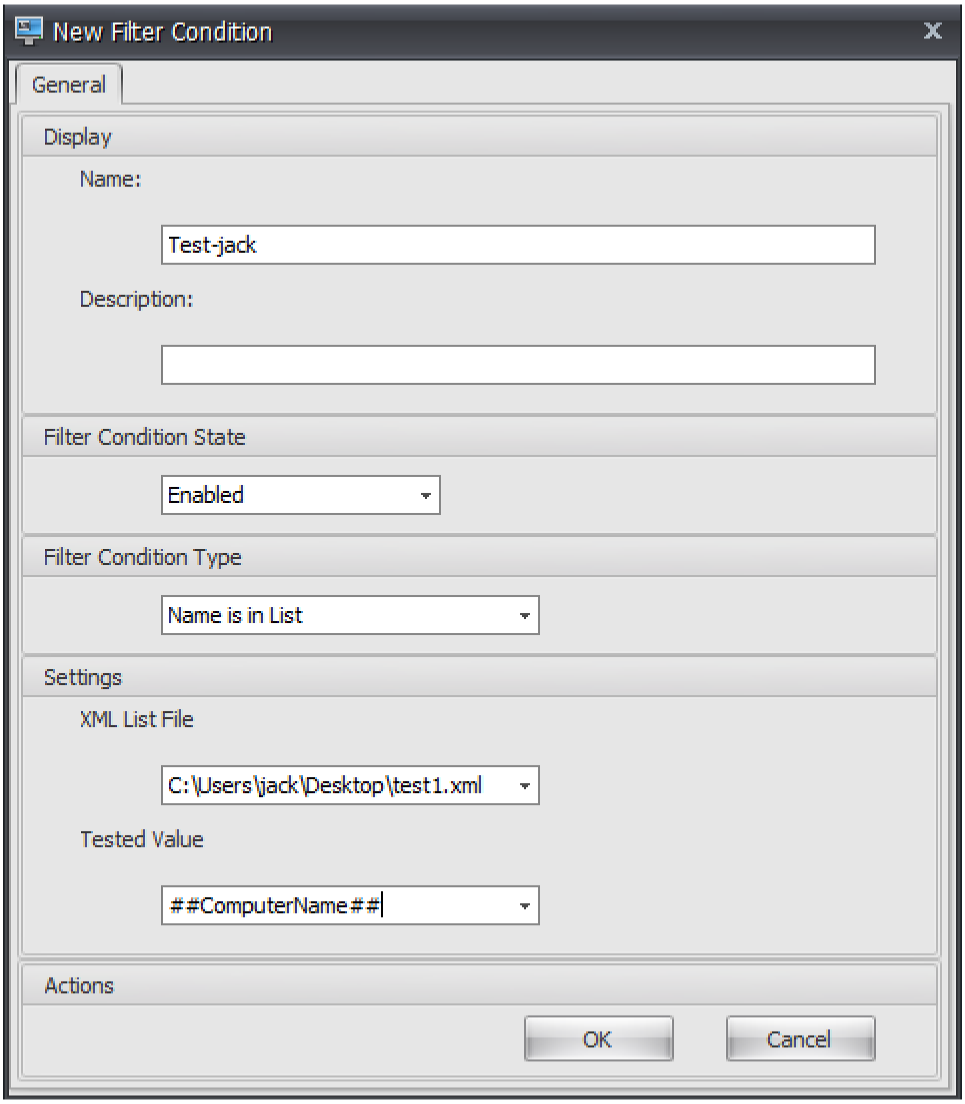
> **Note:**
>
> This feature does not work if you save the XML file on an administration console machine.

Step 7. Go to the **Administration Console > Filters > Conditions > Filter Condition List** tab and then click **Add**.



Name	Description	State
Always True	Always True Filter Condition	✓

Step 8. Type the information and then click **OK**.



New Filter Condition

General

Display

Name: Test-jack

Description:

Filter Condition State

Enabled

Filter Condition Type

Name is in List

Settings

XML List File

C:\Users\jack\Desktop\test1.xml

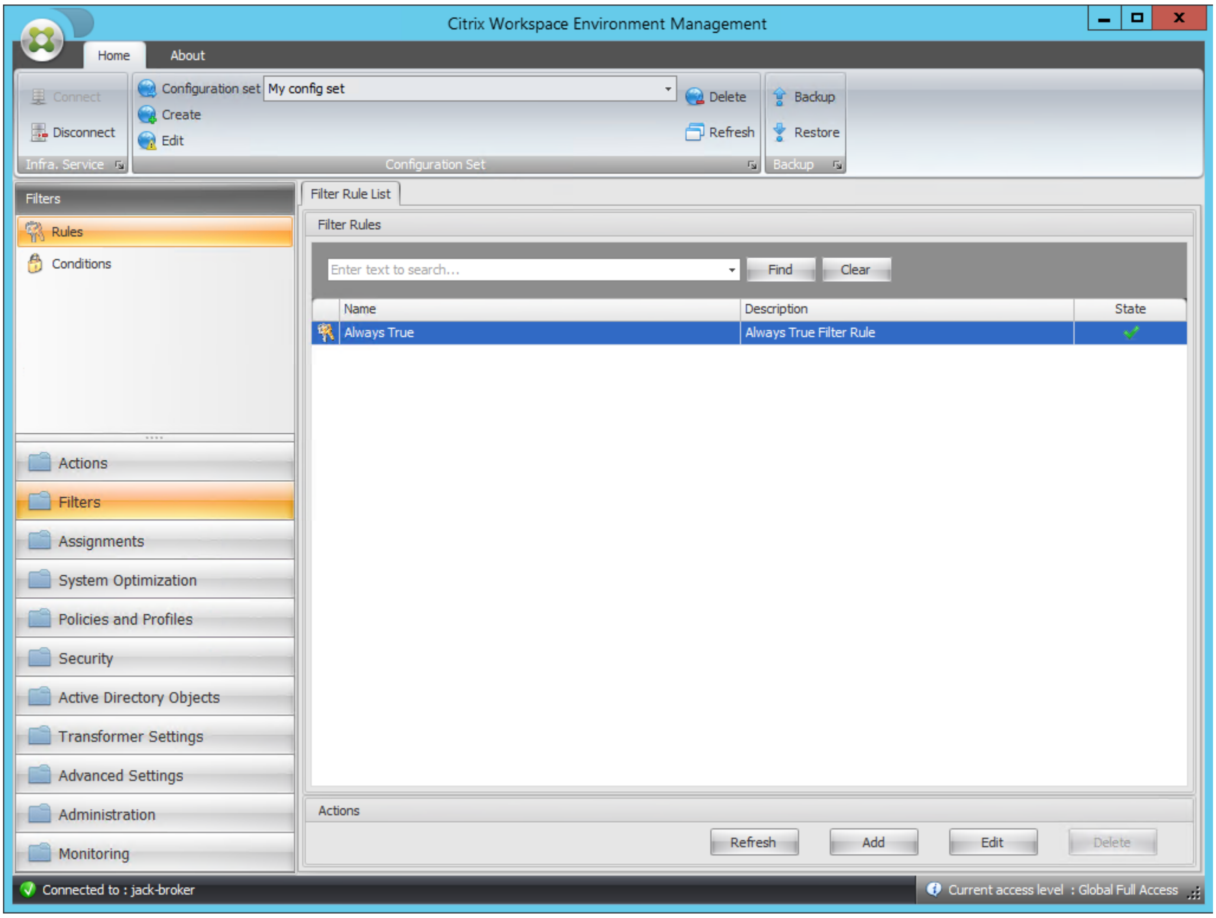
Tested Value

##ComputerName##

Actions

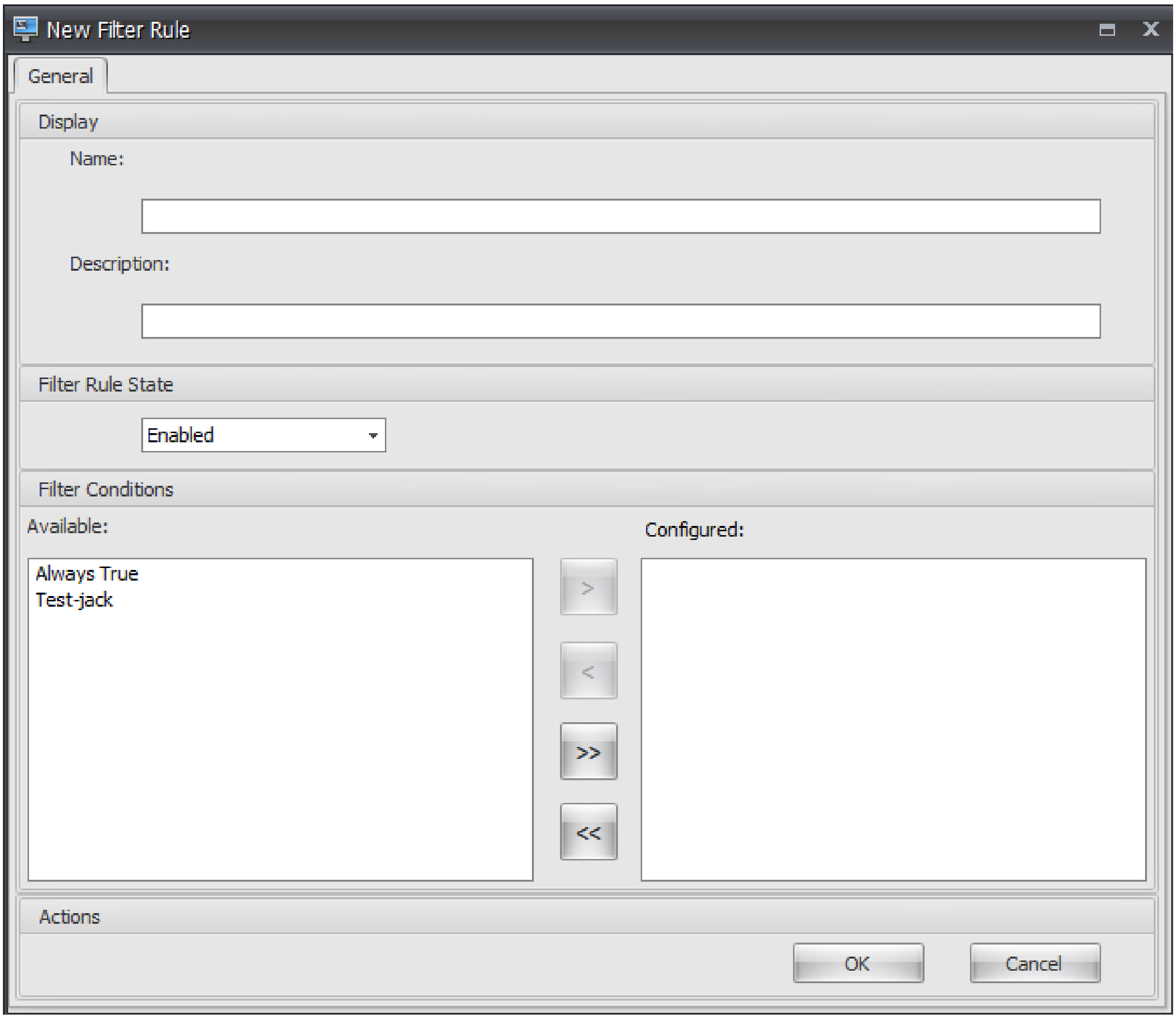
> **Note:**
>
> - **Filter Condition Type**. Select **Name is in List**.
> - **XML List File**: C:\Users\<user1>\Desktop\test1.xml (file address on the agent host)
> - **Tested Value**. Type the dynamic token that corresponds to the name you typed in the **Name** field in the WEM Integrity Condition List Manager. In this example, you typed the name of the machine on which the agent is running (agent host). Therefore, you must use the dynamic token "##ComputerName##." For more information about using dynamic tokens, see Dynamic tokens.

Step 9. Go to the **Administration Console > Filters > Rules > Filter Rule List** tab and then click **Add**.

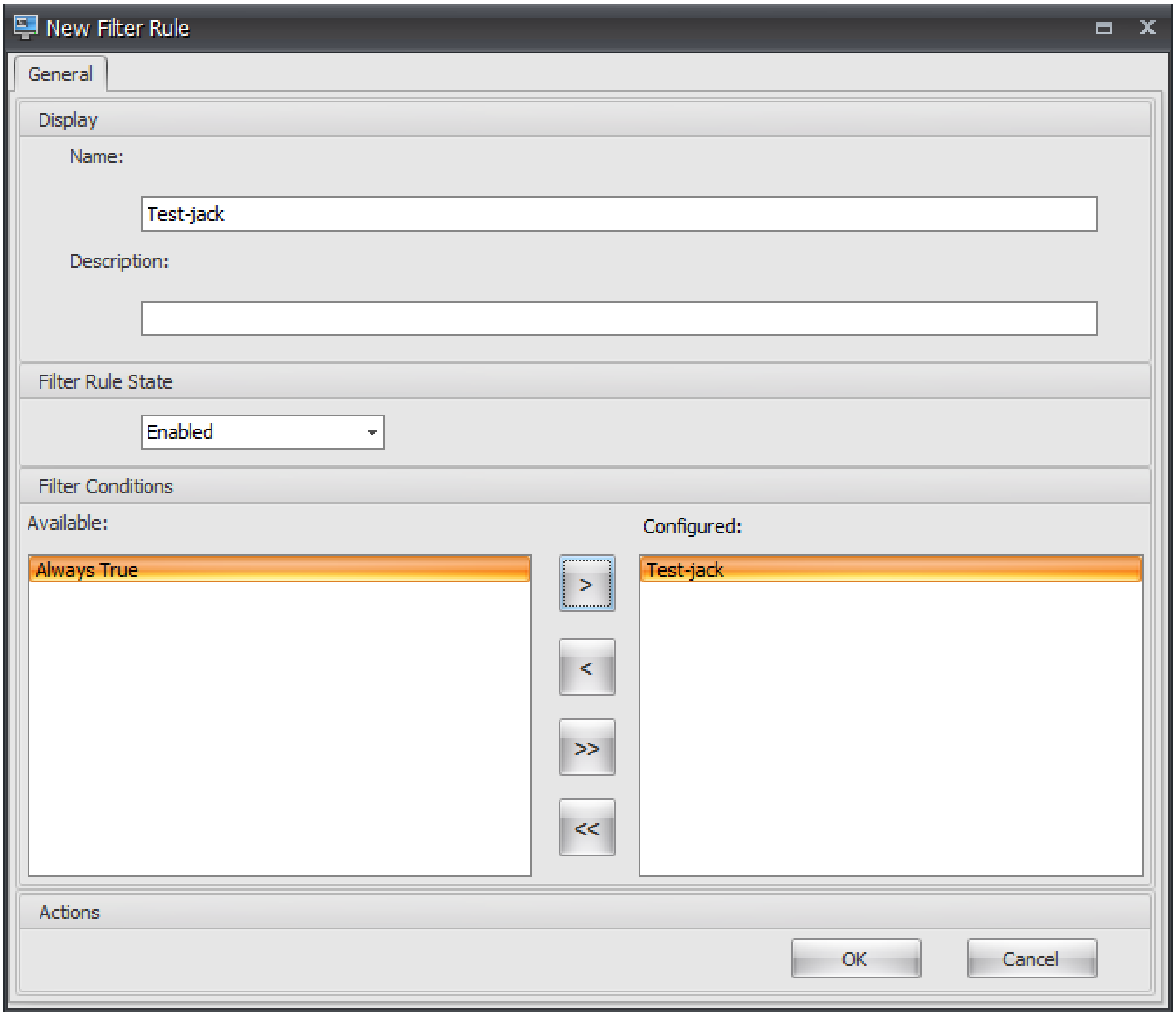


Name	Description	State
Always True	Always True Filter Rule	✓

Step 10. Type the filter name in the **Name** field.



Step 11. Move the configured condition from the **Available** pane to the **Configured** pane and then click **OK**.



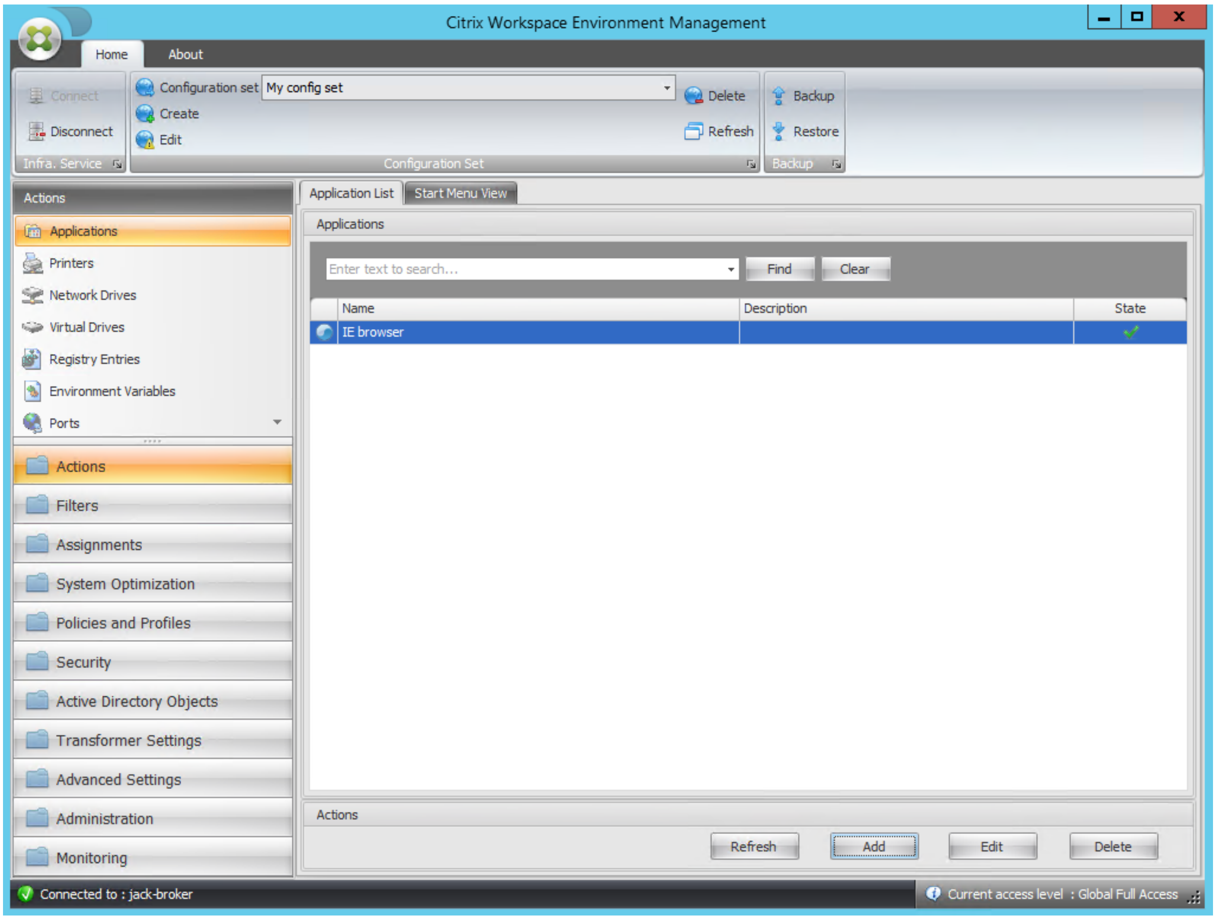
Test-jack

Enabled

Always True

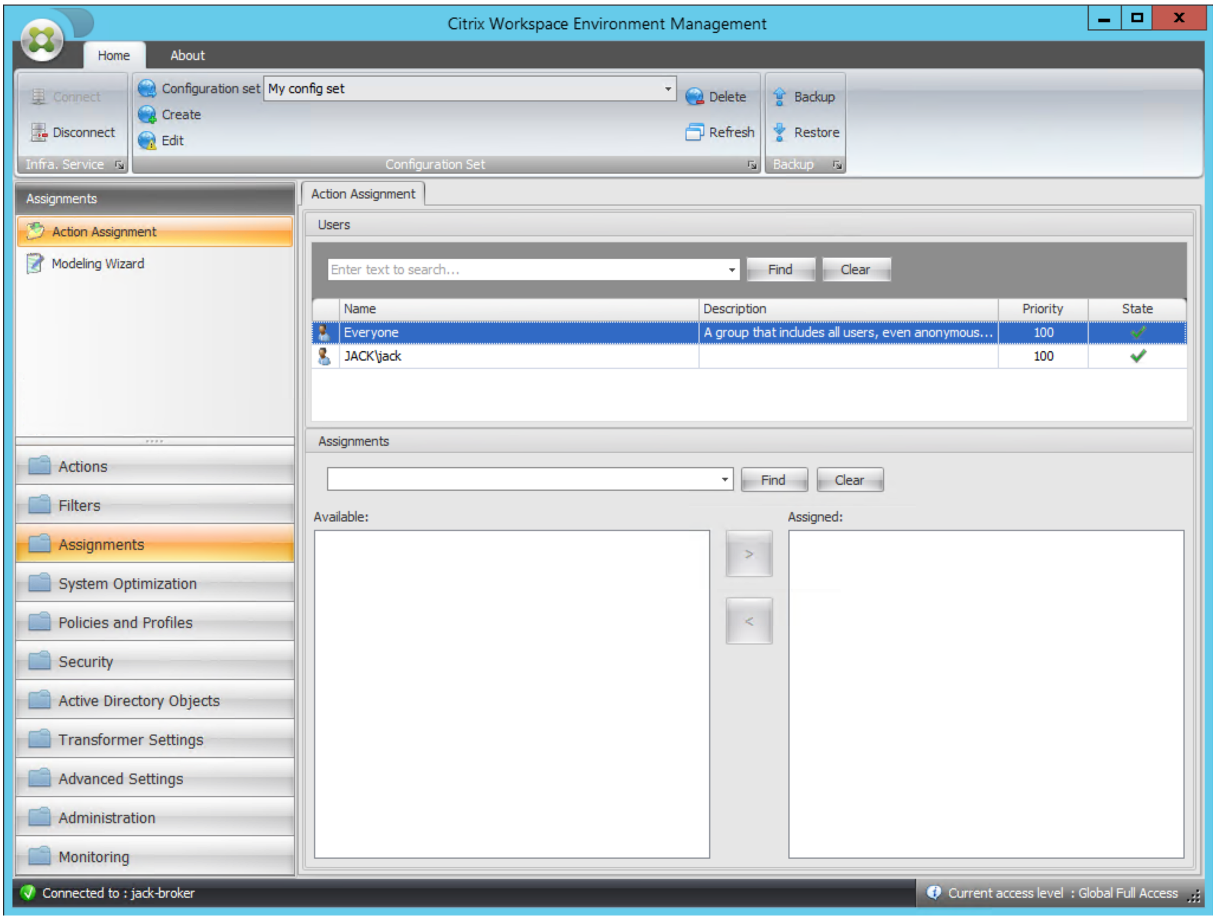
Test-jack

Step 12. Go to the **Administration Console > Actions > Applications > Application List** tab and then add an application.



Name	Description	State
IE browser		✓

Step 13. Go to the **Administration Console > Assignments > Action Assignment** tab.



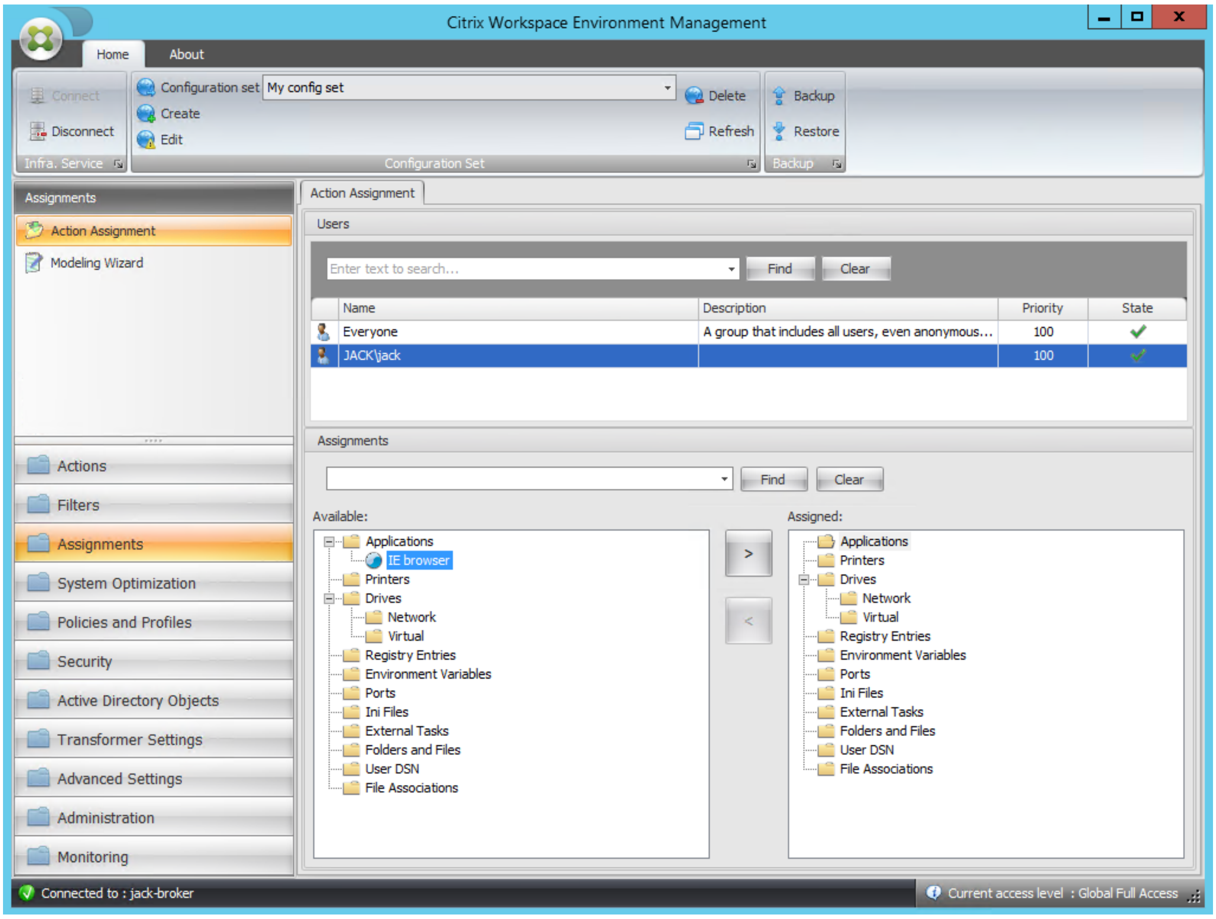
Configuration set: My config set

Name	Description	Priority	State
Everyone	A group that includes all users, even anonymous…	100	✓
JACK\jack		100	✓

Connected to : jack-broker

Current access level : Global Full Access

Step 14. Double-click the desired user or user group (in this example, select the agent host).



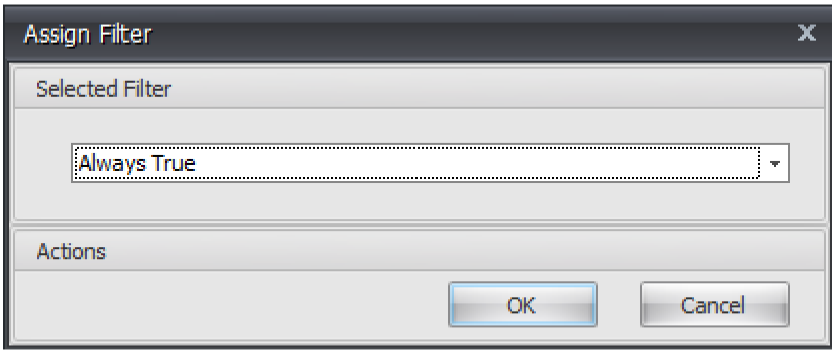
Configuration set: My config set

Name	Description	Priority	State
Everyone	A group that includes all users, even anonymous...	100	✓
JACK\jack		100	✓

Connected to : jack-broker

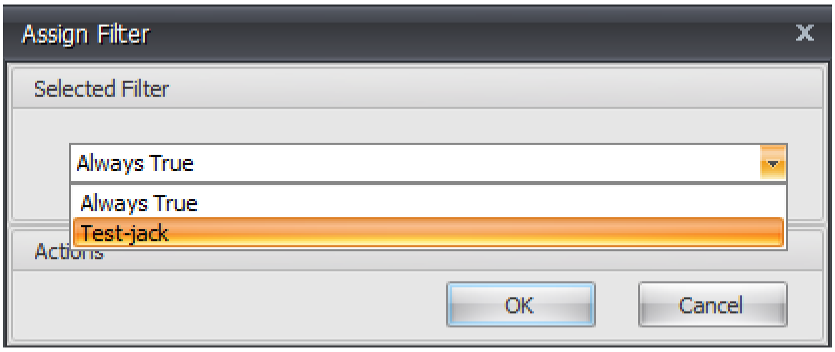
Current access level : Global Full Access

Step 15. Move the application from the **Available** pane to the **Assigned** pane.

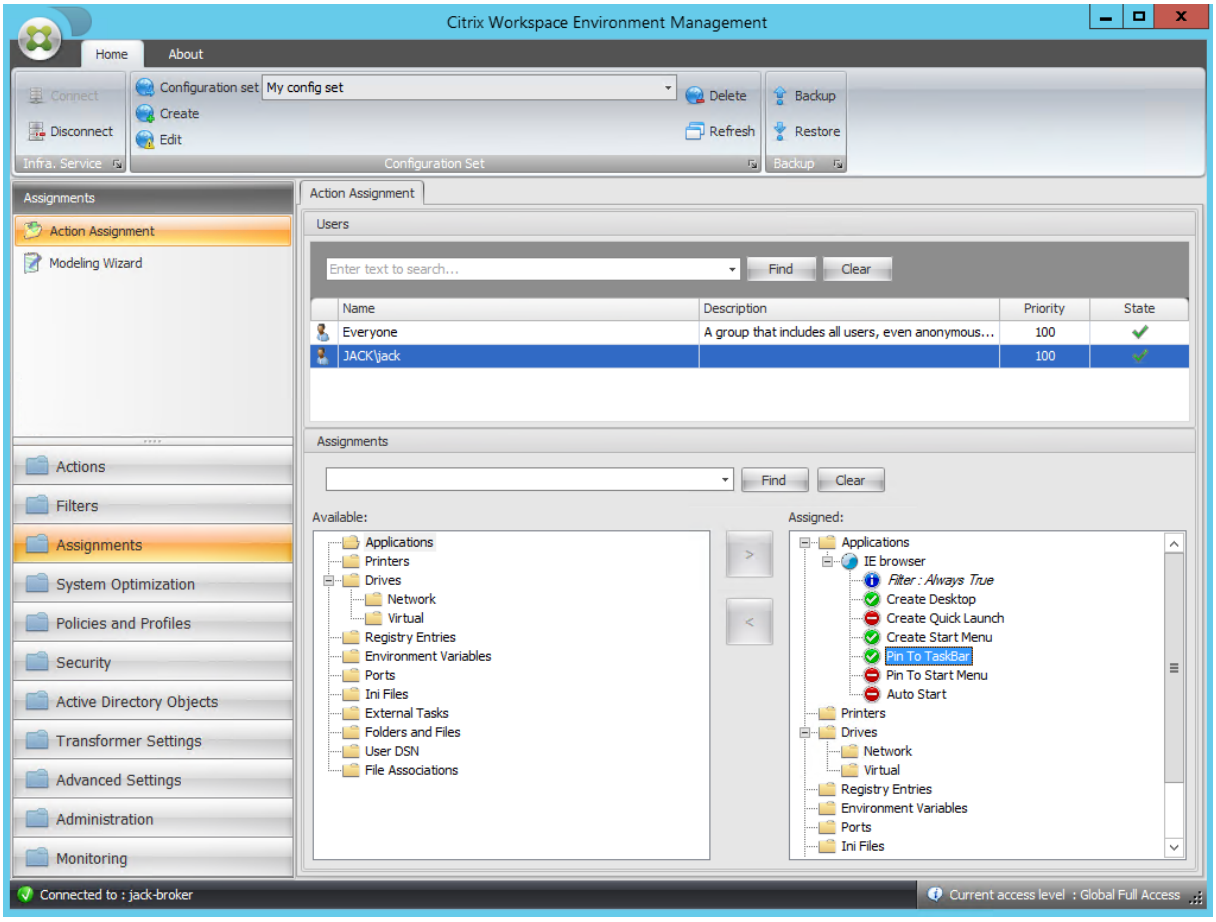


Always True

Step 16. Select the filter and then click **OK**.

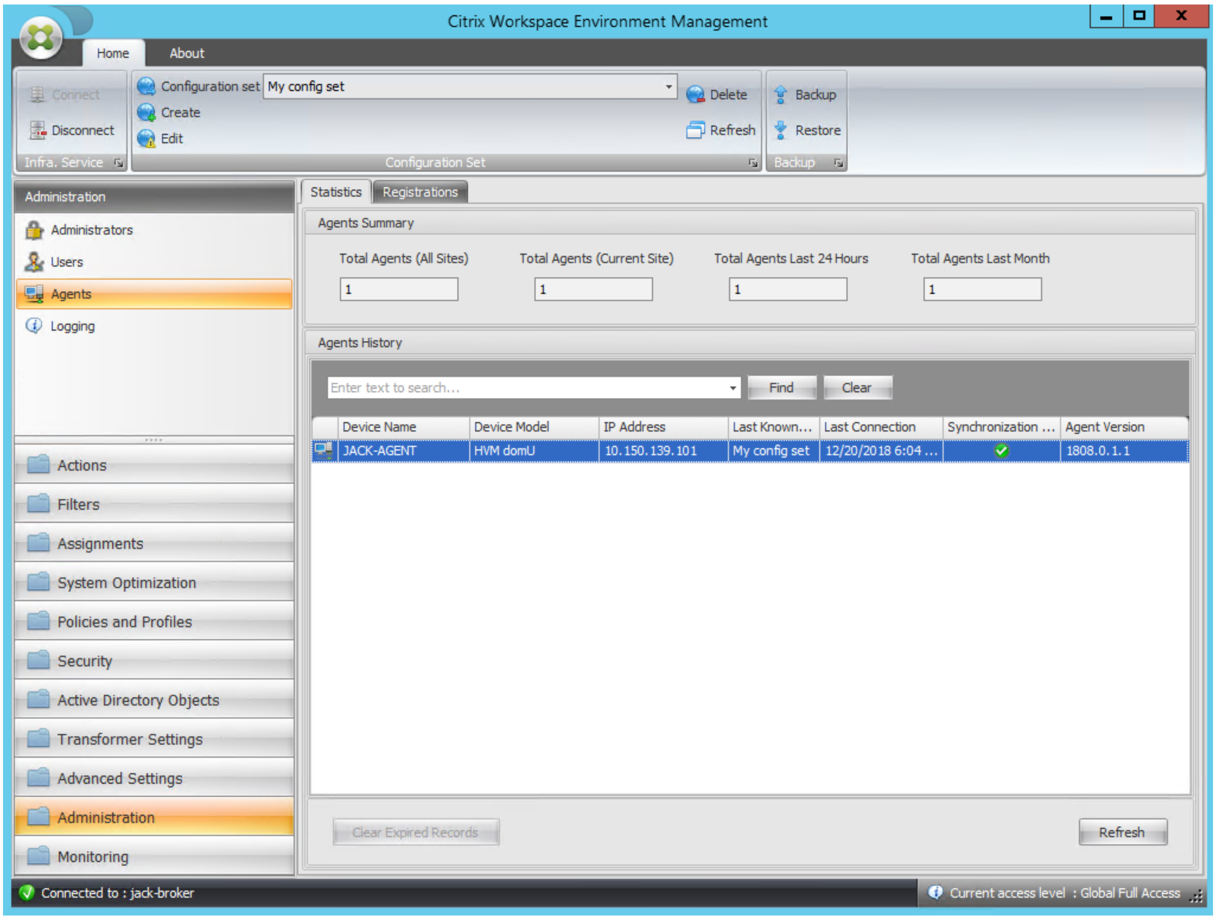


Step 17. Enable the options for the assigned application (in this example, enable **Create Desktop** and **Pin To TaskBar**).



Name	Description	Priority	State
Everyone	A group that includes all users, even anonymous...	100	✓
JACK\jack		100	✓

Step 18. Go to the **Administration Console > Administration > Agents > Statistics** tab and then click **Refresh**.



Configuration set: My config set

Total Agents (All Sites)	Total Agents (Current Site)	Total Agents Last 24 Hours	Total Agents Last Month
1	1	1	1

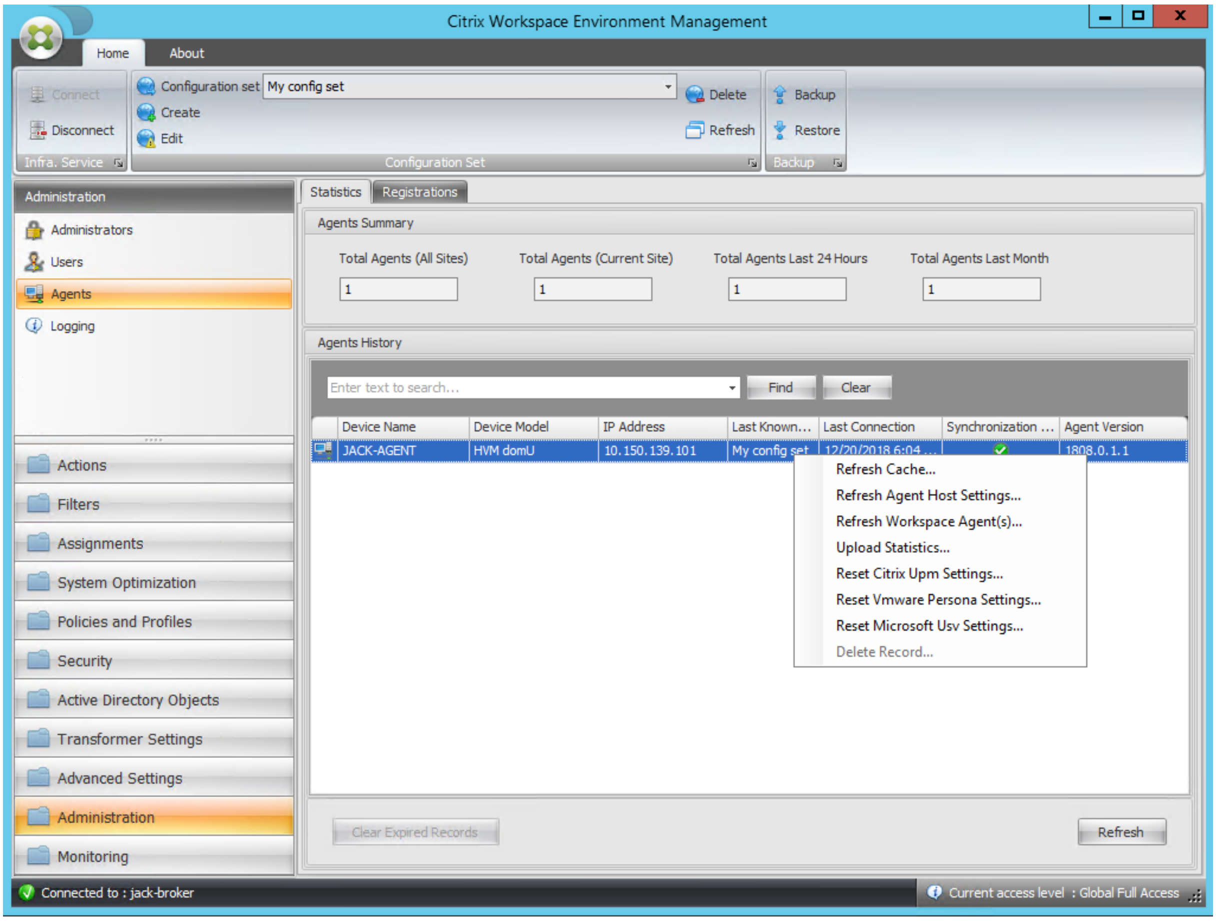
Device Name	Device Model	IP Address	Last Known...	Last Connection	Synchronization ...	Agent Version
JACK-AGENT	HVM domU	10.150.139.101	My config set	12/20/2018 6:04 ...	✓	1808.0.1.1

Connected to : jack-broker

Current access level : Global Full Access

Step 19. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.

> **Note:**
>
> For the settings to take effect, you can also go to the machine on which the agent is running and then refresh Citrix WEM Agent.



Configuration set: My config set

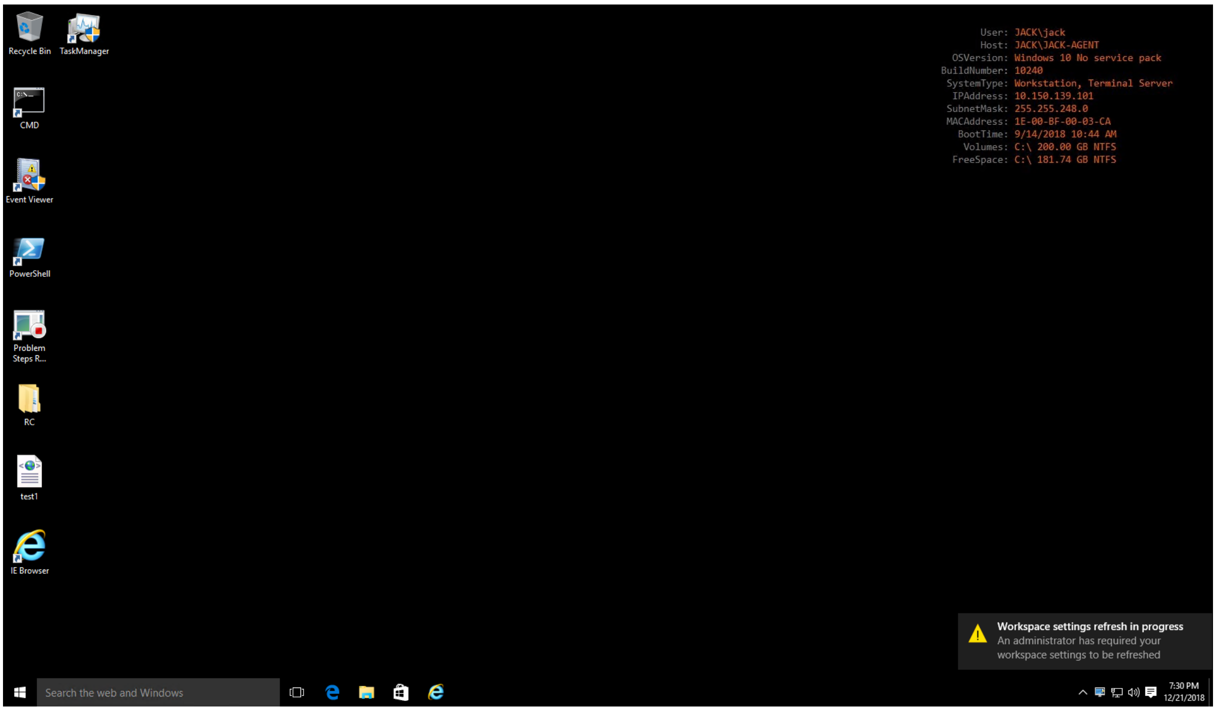
Total Agents (All Sites)	Total Agents (Current Site)	Total Agents Last 24 Hours	Total Agents Last Month
1	1	1	1

Device Name	Device Model	IP Address	Last Known…	Last Connection	Synchronization …	Agent Version
JACK-AGENT	HVM domU	10.150.139.101	My config set	12/20/2018 6:04 …	✓	1808.0.1.1

Connected to : jack-broker

Current access level : Global Full Access

Step 20. Go to the machine on which the agent is running (agent host) to verify that the configured condition works.



```
       User: JACK\jack
       Host: JACK\JACK-AGENT
  OSVersion: Windows 10 No service pack
BuildNumber: 10240
 SystemType: Workstation, Terminal Server
  IPAddress: 10.150.139.101
 SubnetMask: 255.255.248.0
 MACAddress: 1E-00-BF-00-03-CA
   BootTime: 9/14/2018 10:44 AM
    Volumes: C:\ 200.00 GB NTFS
  FreeSpace: C:\ 181.74 GB NTFS
```

Workspace settings refresh in progress
An administrator has required your workspace settings to be refreshed

7:30 PM
12/21/2018

In this example, the application is successfully assigned to the agent host, which is created on the desktop and pinned to the taskbar.

Glossary

September 4, 2018

> **Note:**
>
> Learn about product name changes here.

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.

On 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.

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).

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).

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.

Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States