Workspace Environment Management 2009

Contents

Workspace Environment Management 2009

August 11, 2020

Workspace Environment Management 2009 is the current release. For documentation of earlier releases and the Citrix Cloud Workspace Environment Management service, see the following sections:

- Workspace Environment Management 2006
- Workspace Environment Management 2003
- Workspace Environment Management 1912
- Workspace Environment Management 1909
- Workspace Environment Management 1906
- 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.

Introduction

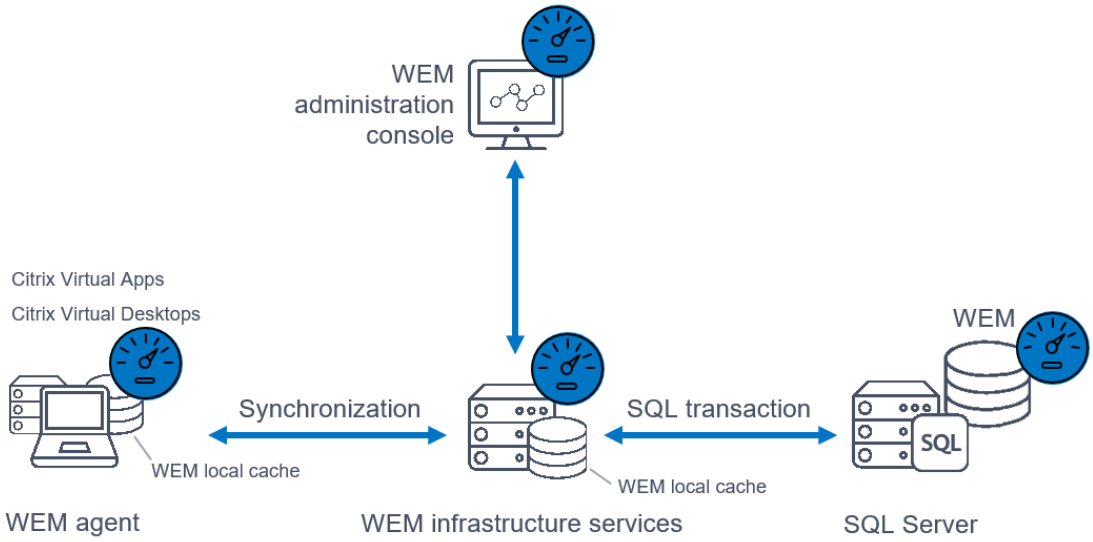
Workspace Environment Management uses intelligent resource management and Profile Management technologies to deliver the best possible performance, desktop logon, and application response times for Citrix Virtual Apps and Desktops deployments. It is a software-only, driver-free solution.

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 fast as possible.

Technical overview

Workspace Environment Management (WEM) has the following architecture:



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

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

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

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

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

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

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

What's new

August 12, 2020

What's new in 2009

Workspace Environment Management 2009 includes the following new features. For information about bug fixes, see Fixed issues.

Support for the Windows 10 1909 template

WEM adds support for the Windows 10 1909 template introduced in Citrix optimizer. You can now use WEM to perform template-based system optimizations for Windows 10 1909 machines. For information about using Citrix optimizer, see Citrix optimizer.

Profile Management

Workspace Environment Management now supports all versions of Profile Management through 2009. The following new options are now available on the **Administration Console > Policies and Profiles > Citrix Profile Management Settings > Profile Container Settings** tab:

- **Enable Folder Exclusions for Profile Container** (option for excluding the listed folders from the profile container)
- **Enable Folder Inclusions for Profile Container** (option for keeping the listed folders in the profile container when their parent folders are excluded)

For more information, see Profile Container Settings.

Administration console

The administration console user interface has changed:

- In **Administration Console > Policies and Profiles > Citrix Profile Management Settings**, there is a new **Profile Container Settings** tab for you to configure Profile Management profile container settings.
- The **Enable Profile Container** option now moves to the **Profile Container Settings** tab. Previously, the option was present on the **Synchronization** tab.

Fixed issues

October 26, 2020

Workspace Environment Management 2009 contains the following fixed issues compared to Workspace Environment Management 2006:

- After you upgrade the WEM agent to version 1912, it might take a long time for the agent to process policy-related registry entries. [WEM-7720, CVADHELP-14224]
- The following error message might appear in the WEM agent log file on a regular basis:

  ```
  Exception -> ConfigurationDataSourcesHelper.CheckAgentBrokerServiceClient
  (): System.ServiceModel.FaultException: There are too many active
  security negotiations or secure conversations at the service. Please
  retry later.
  ```

  The issue is caused by an incorrect Windows Communication Foundation (WCF) authentication pool size. [WEM-8281, CVADHELP-14467]
- When you finish importing your Group Policy settings into WEM, the following message might appear even if you are the only administrator that is using the administration console:
  - Configuration Change Update: An administrator has made configuration-related changes. Click OK to reflect the changes in the current administration console. [WEM-9234]
- Some of the action items you selected in the **Restore** wizard might be cleared if you click the **Previous** button to return to the previous pages. The issue occurs when you use the **Restore** wizard to restore a zip backup of your GPOs converted using the **Migrate** wizard. [WEM-9281]

Known issues

September 28, 2020

- After you upgrade the WEM agent to version 1912, the memory consumption of **Citrix WEM Agent Host Service** might exceed 2G. If debug mode is enabled, you can see that the following messages appear many times in the **Citrix WEM Agent Host Service Debug.log** file:
  - **Adding history entry to the DB writer queue**
  - **Initializing process limitation thread for process** [WEM-9432, CVADHELP-15147]
- When editing a default packaged rule, you are prompted to provide valid values on the **Publisher** tab of the **Edit Rule** window, with the **OK** button grayed out. However, the **OK** button remains grayed out even if you provide valid values on the **Publisher** tab later. [WEM-9498]

- After you upgrade the WEM agent to version 2005, **Citrix WEM Agent Host Service** might consume between 10% and 30% of the total CPU resources, affecting the user experience. [WEM-9902, WEMHELP-47]
- The WEM administration console might fail to display the changes you made to the working directory for an installed application the next time you edit the application. [WEM-10007, CVADHELP-15695]
- When using the application security feature, you see a green checkmark next to a user or user group in the **Assigned** column of the **Assignments** section in the **Edit Rule** or **Add Rule** window. The green checkmark icon does not necessarily indicate that the rule is assigned to that user or user group. Only a user or user group that has a blue highlight in the background is the one to which the rule is assigned. [WEM-10047]
- In non-persistent environments, changes you make through the administration console might fail to take effect on the agent hosts. The issue occurs because the agent cache file in the base image might cause cache synchronization problems. As a workaround, users need to first delete the cache on their agent hosts and then refresh the cache manually to synchronize the cache with the infrastructure services.

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

  1. Stop **Citrix WEM Agent Host Service**.
  2. Delete these agent local database files: **LocalAgentDatabase.db** and **LocalAgentDatabase.db**. [WEM-10082]
- The following options are not mutually exclusive. However, the administration console does not allow you to configure them at the same time.
  - **Hide Specified Drives from Explorer** and **Restrict Specified Drives from Explorer** (on the **Policies and Profiles > Environmental Settings > Windows Explorer** tab) [WEM-10172, WEMHELP-52]

Third party notices

March 26, 2020

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

March 26, 2020

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 that are deprecated or removed.

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

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

Item	Announced in	Removed in	Alternative
Support for VMware Persona settings.	1906	**1909**	
Support for WEM infrastructure services on the following OS platforms: Windows Server 2008 R2 SP1, and Windows Server 2012.	4.7	**1808**	

Item	Announced in	Removed in	Alternative
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

June 5, 2020

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

Overview

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

Prerequisites

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

Installation and configuration

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

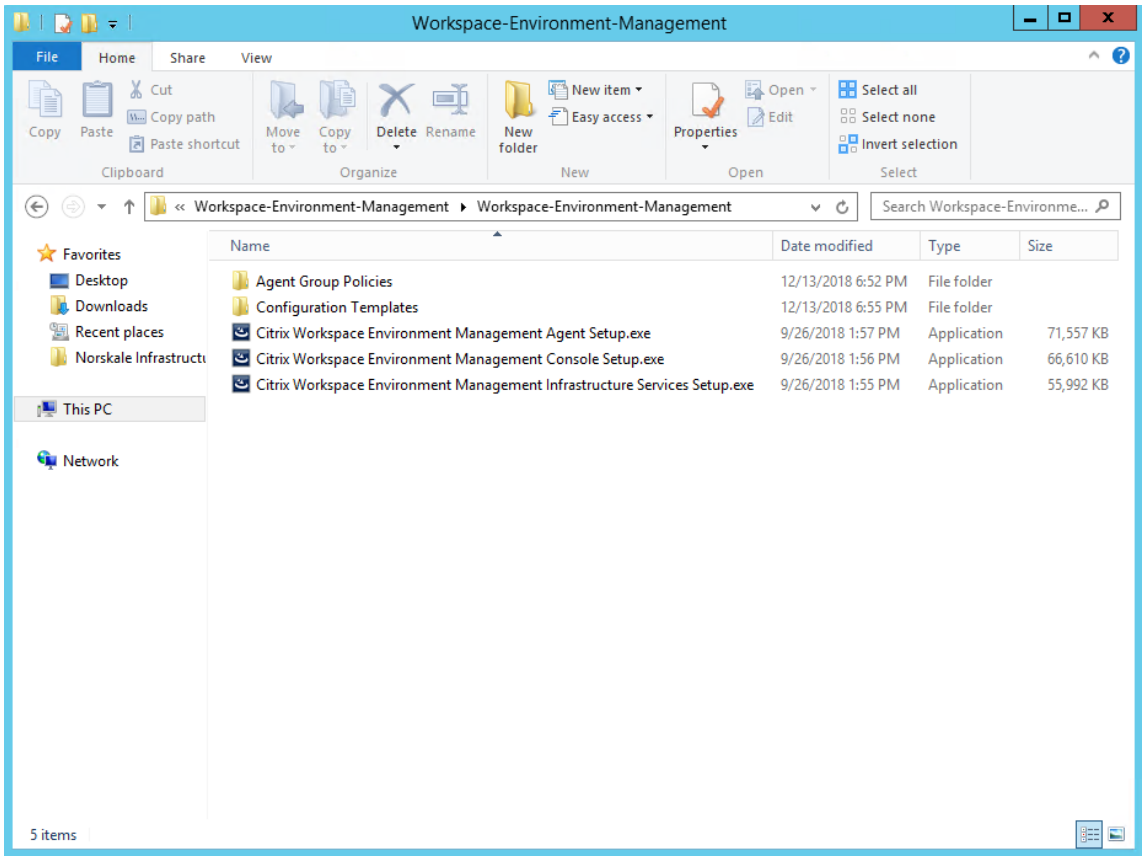
- Infrastructure services
- Administration console
- Agent

> **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 in-

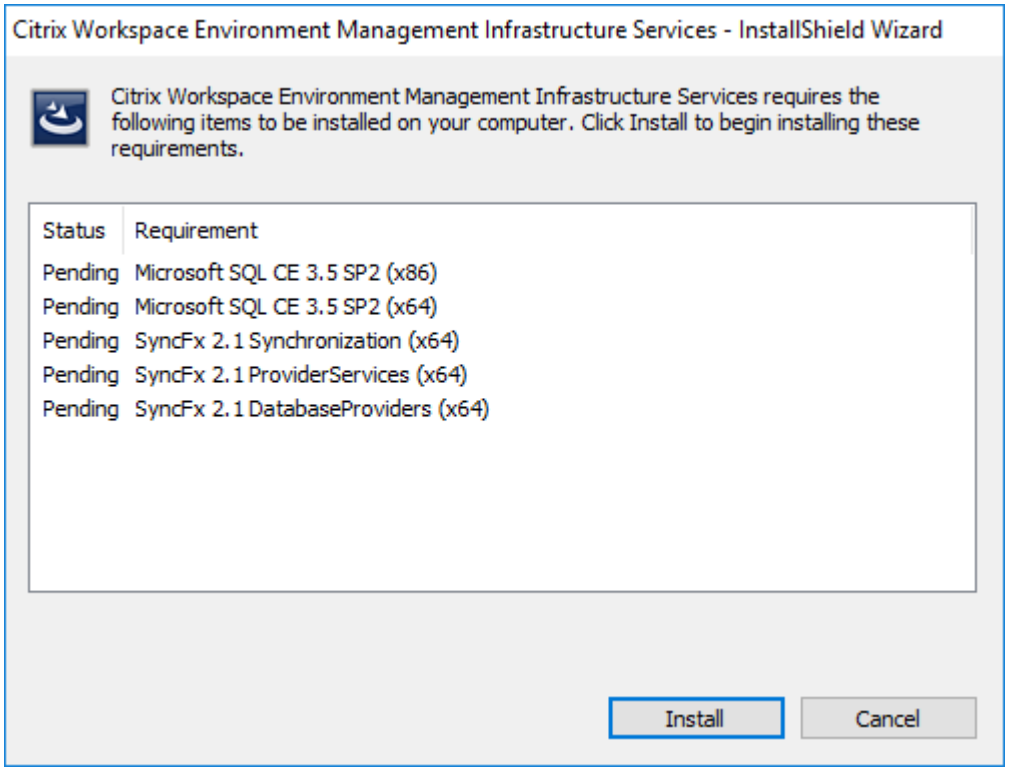
> stalled.

Step 1: Install the infrastructure services

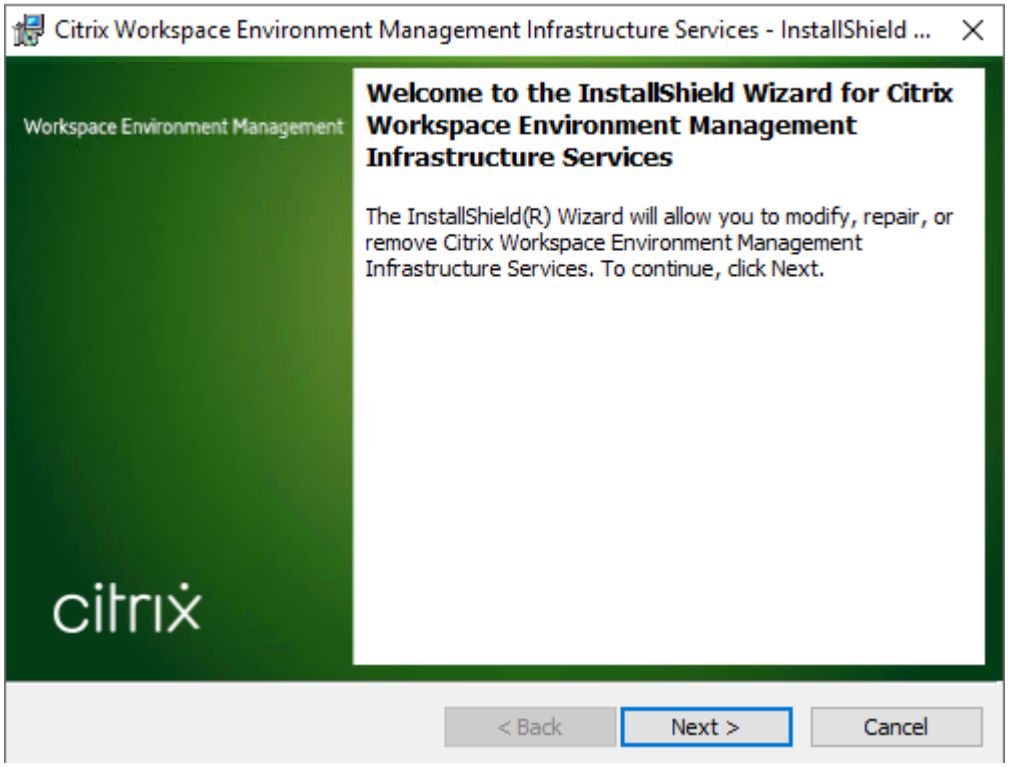
1. Download the latest WEM installer from the Citrix Virtual Apps and Desktops Premium Edition Components downloads page https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/. Extract the zip file to a convenient folder.



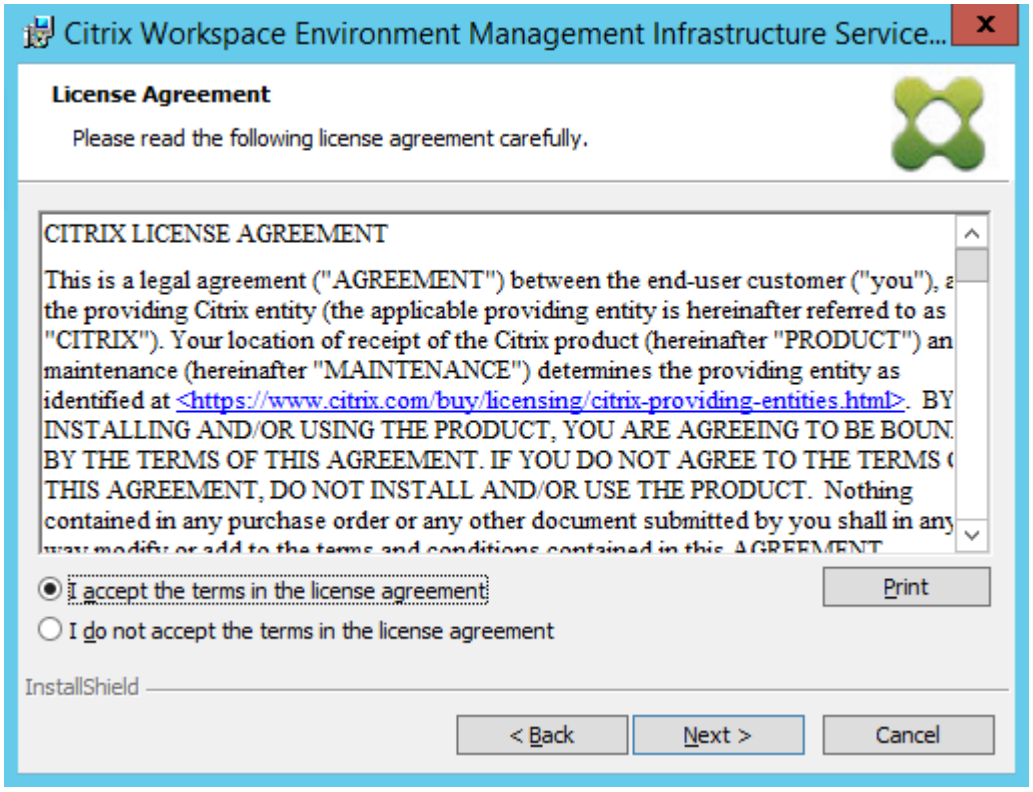
2. Run **Citrix Workspace Environment Management Infrastructure Services Setup.exe** on your infrastructure server.
3. Click **Install**.



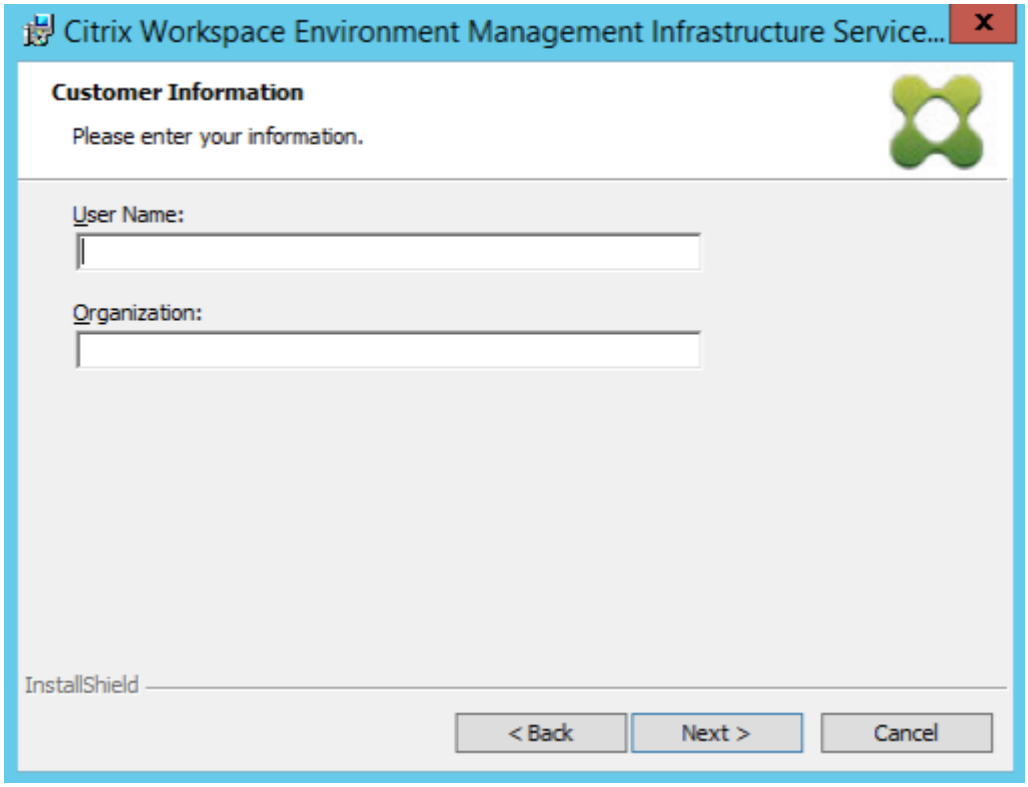
4. Click **Next**.



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

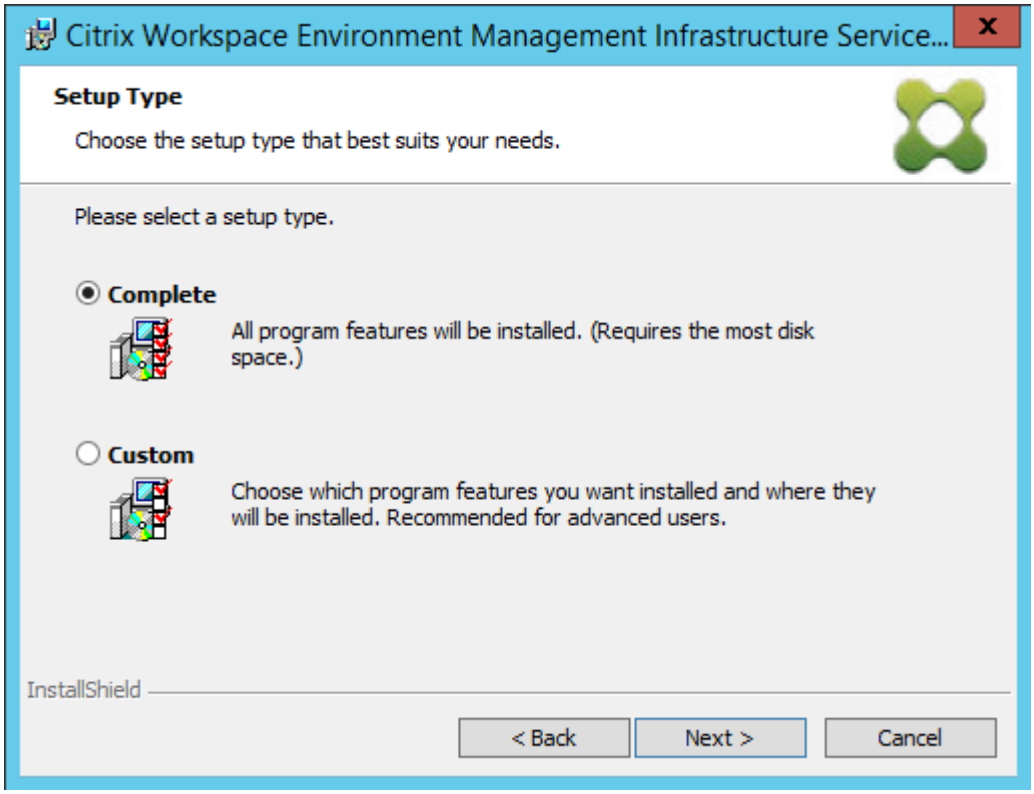


6. Type your user name and organization and then click **Next**.

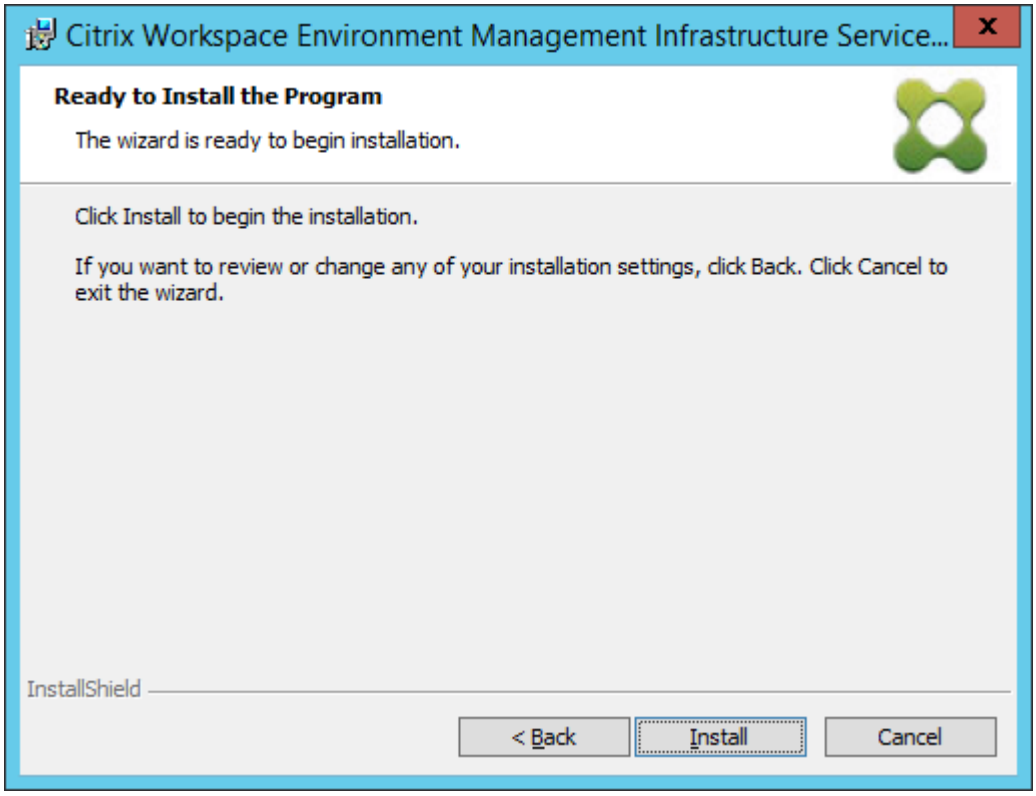


7. Select **Complete** and then click **Next**.

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

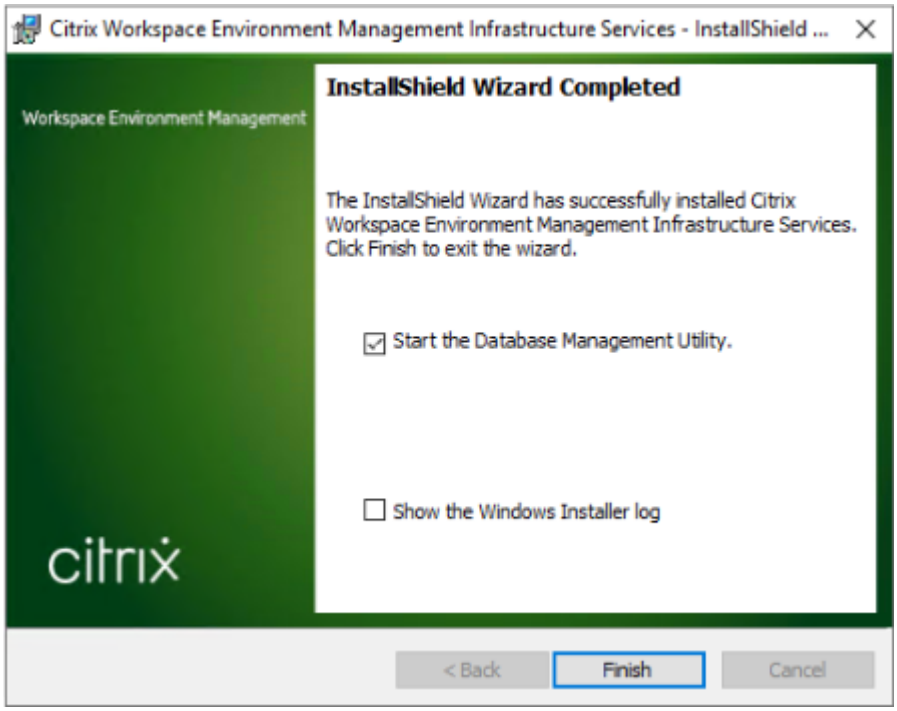


8. On the Ready to Install the Program page, click **Install**.



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

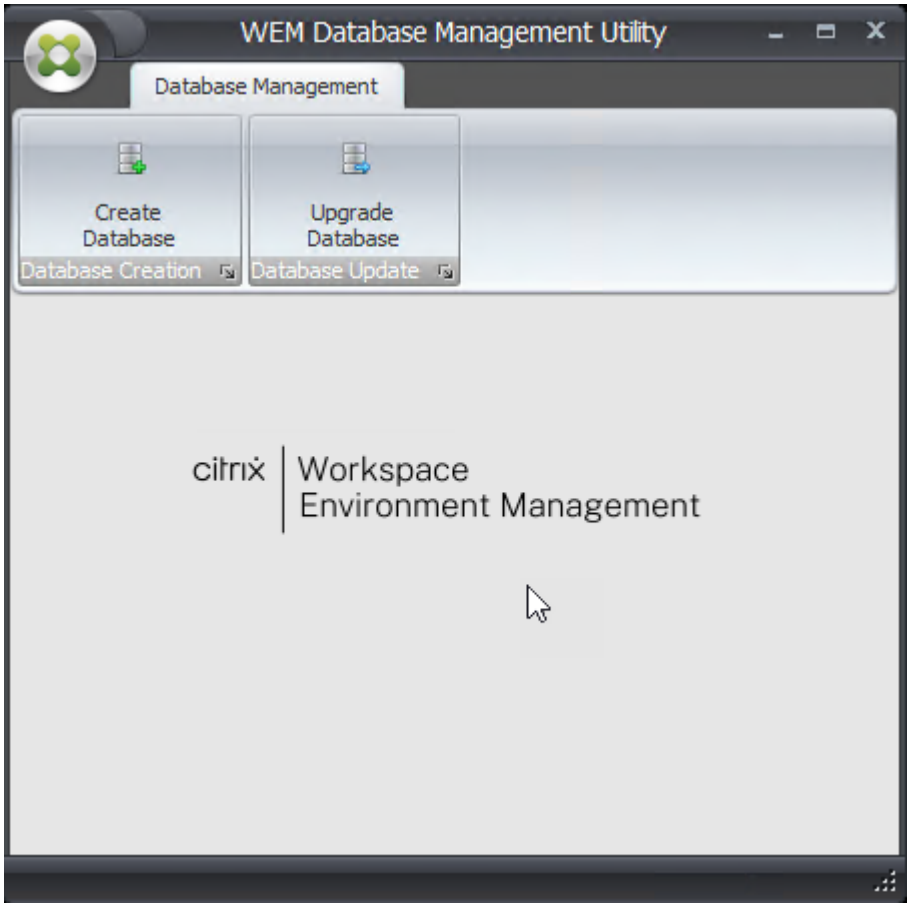
> **Note:**
>
> By default, the **Start the Database Management Utility** option is selected, and the utility starts automatically. You can also start the utility from the **Start** menu at **Citrix** > **Workspace Environment Management** > **WEM Database Management Utility**.



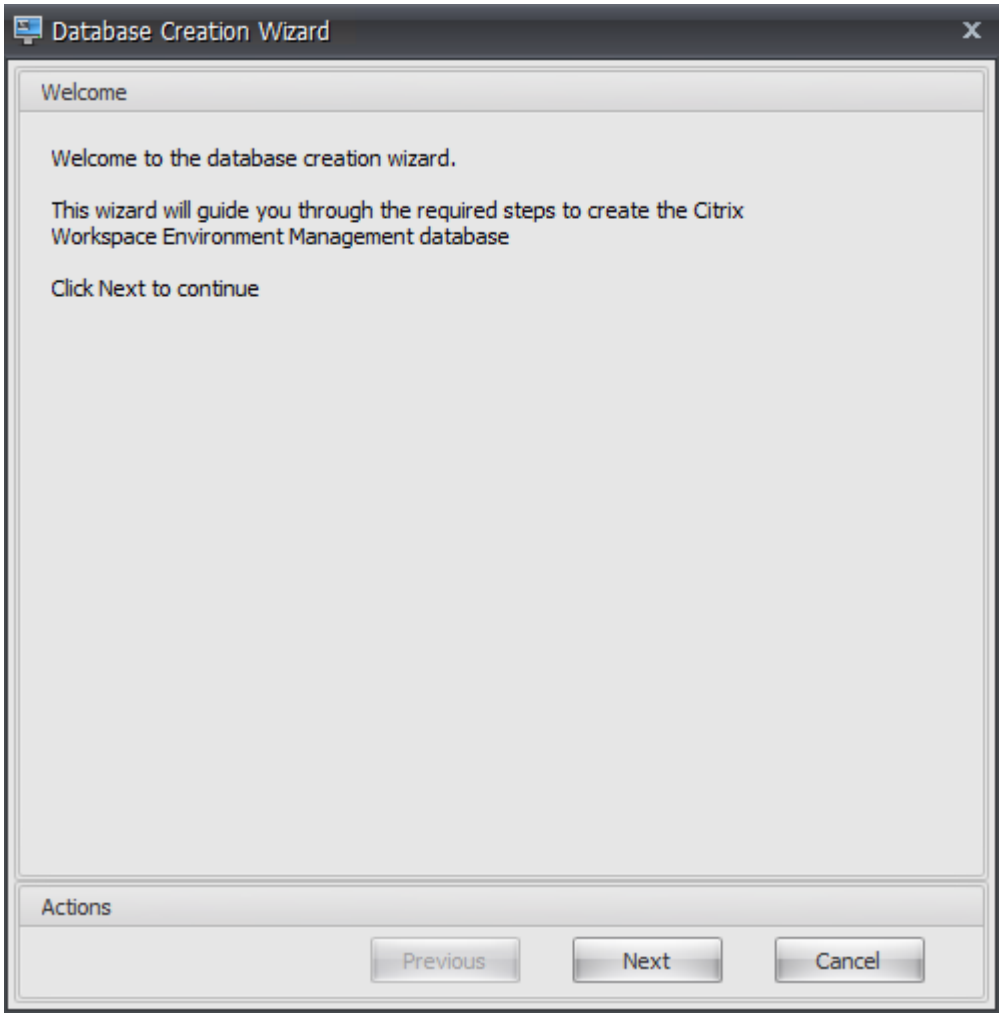
Step 2: Create a WEM database

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.

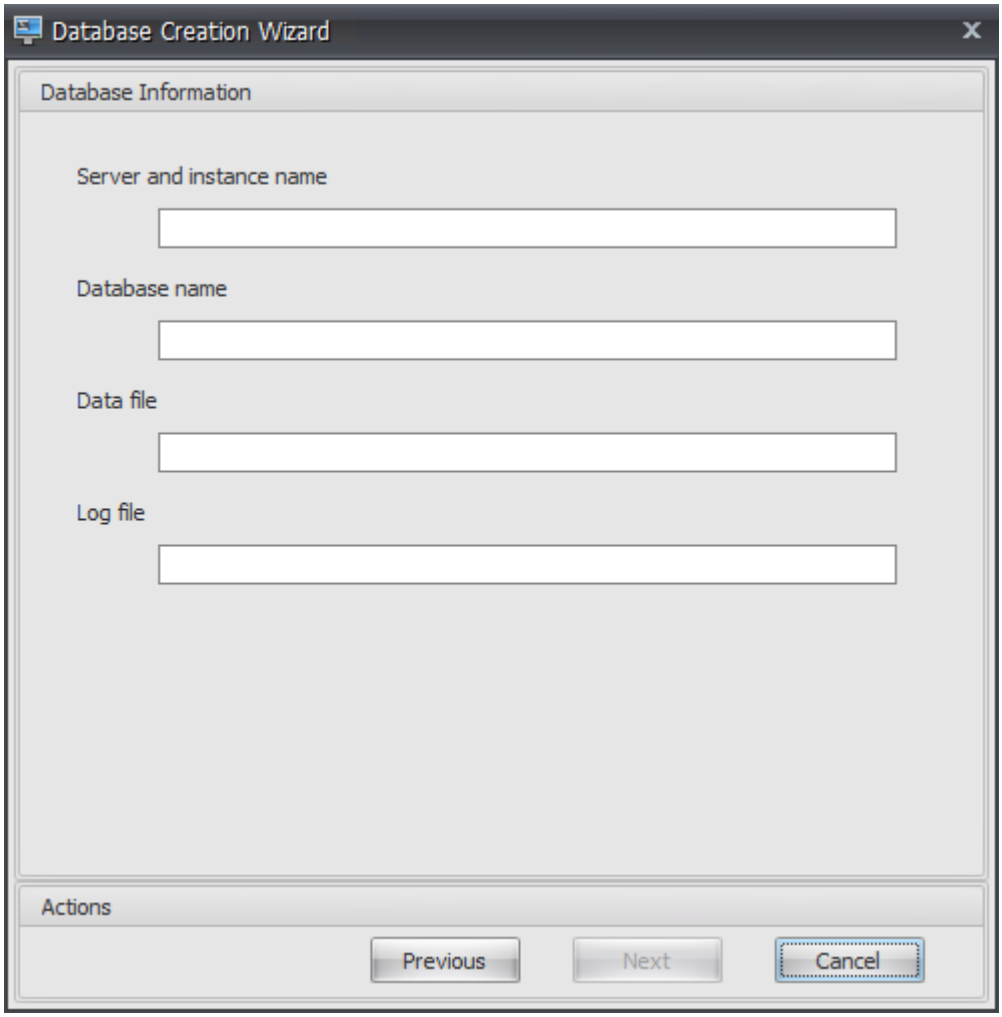


2. On the Welcome page, click **Next**.

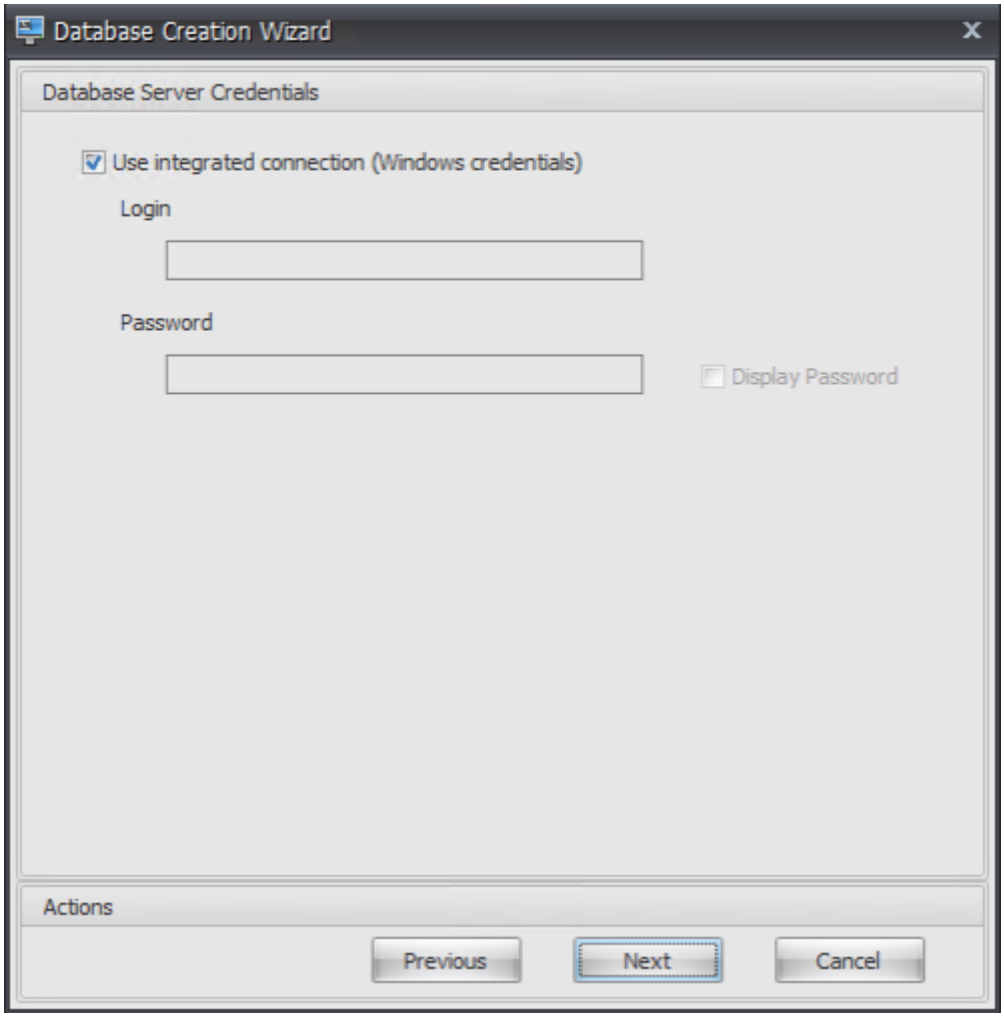


3. On the Database Information page, type the required information and then click **Next**.

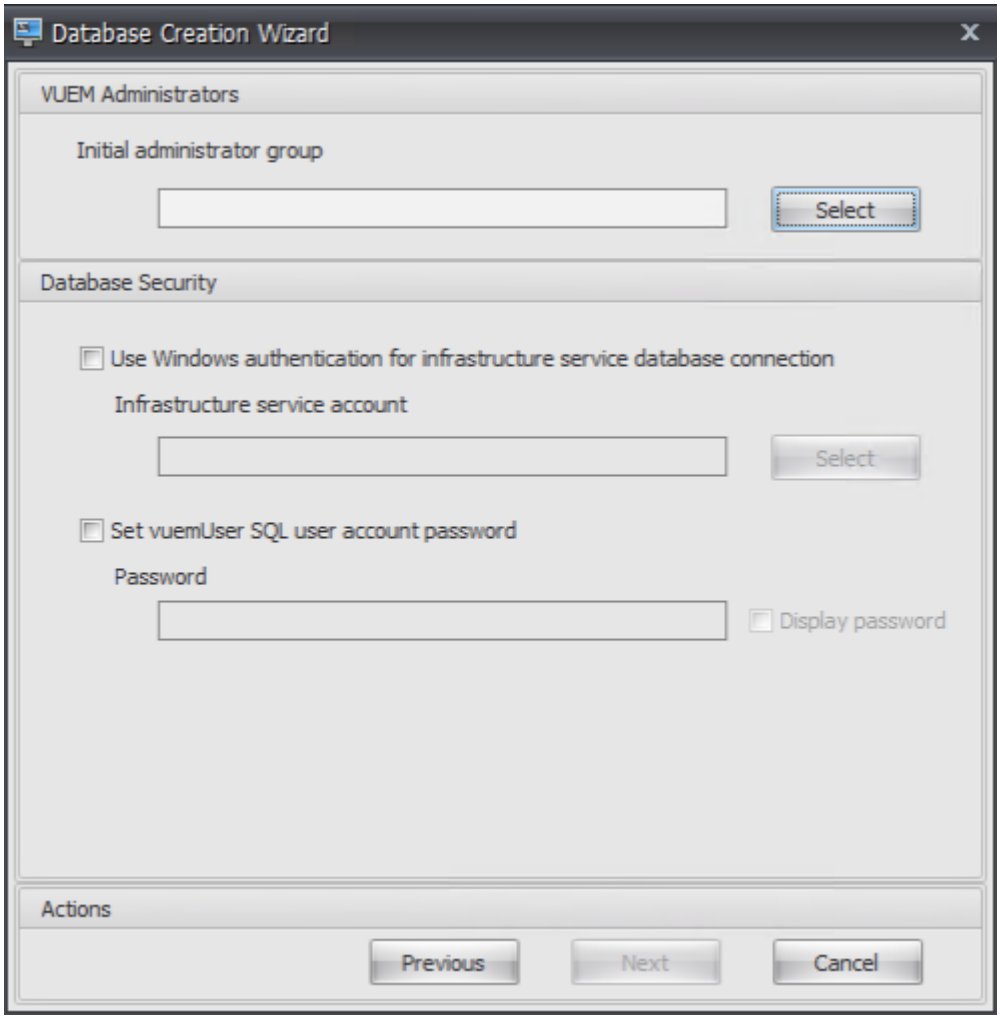
> **Note:**
>
> - For the server and instance name, type the machine name, fully qualified domain name, or IP address.
> - For the file paths, type the exact paths specified by your database administrator. Make sure that any auto-completed file paths are correct.



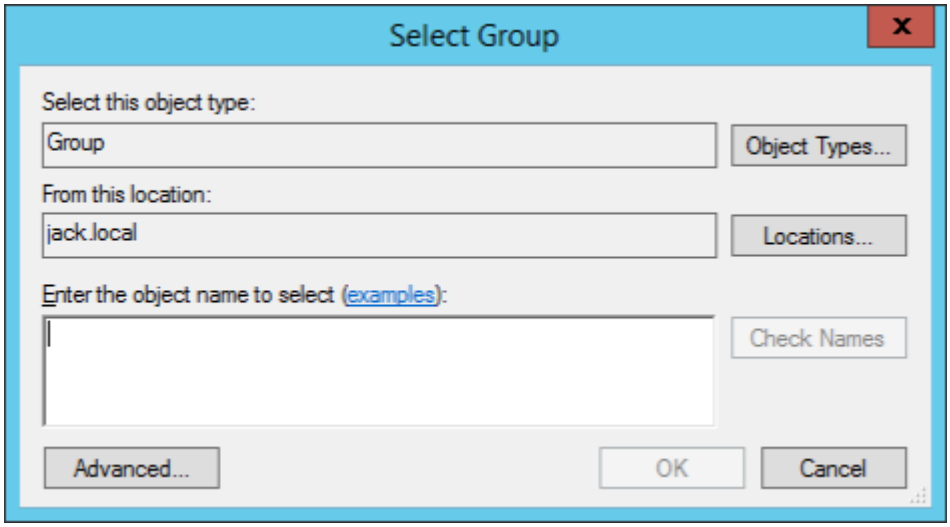
4. On the Database Server Credentials page, type the required information and then click **Next**.



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



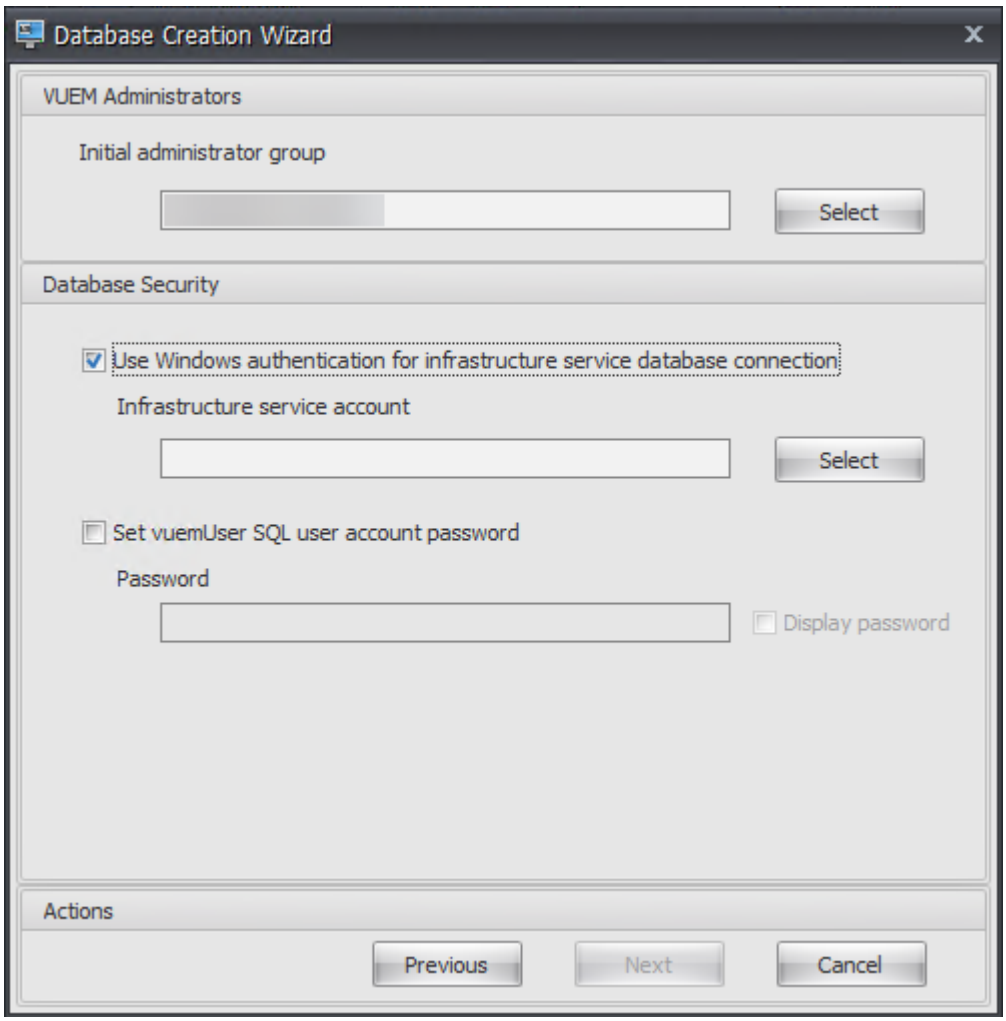
6. In the Select Group window, type a user group with administration permissions to the administration console, click **Check Names**, and then click **OK**.



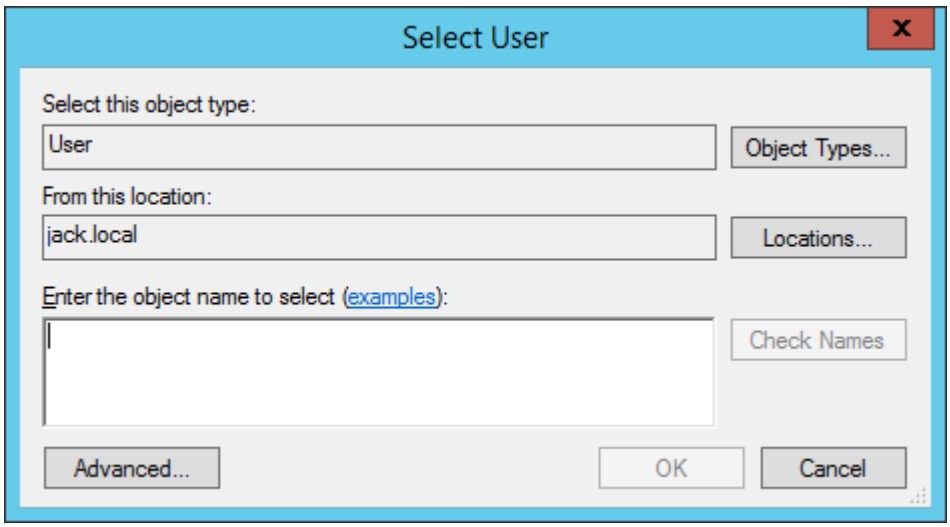
7. Under Database Security, select **Use Windows authentication for infrastructure service**

database connection and then click **Select**.

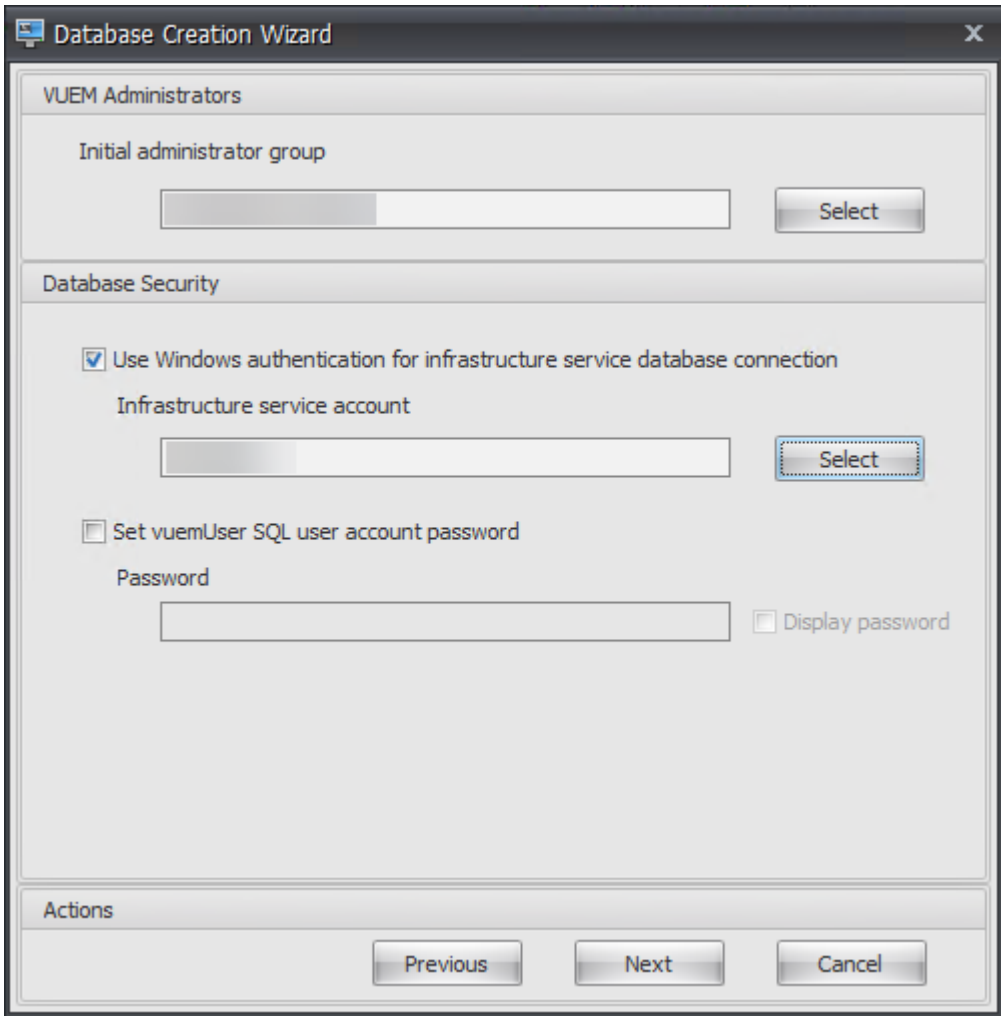
> **Note:**
>
> - If you select neither **Use Windows authentication for infrastructure service database connection** nor **Set vuemUser SQL user account password**, the SQL user account is used by default.
> - To use your own vuemUser SQL account password (for example, if your SQL policy requires a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



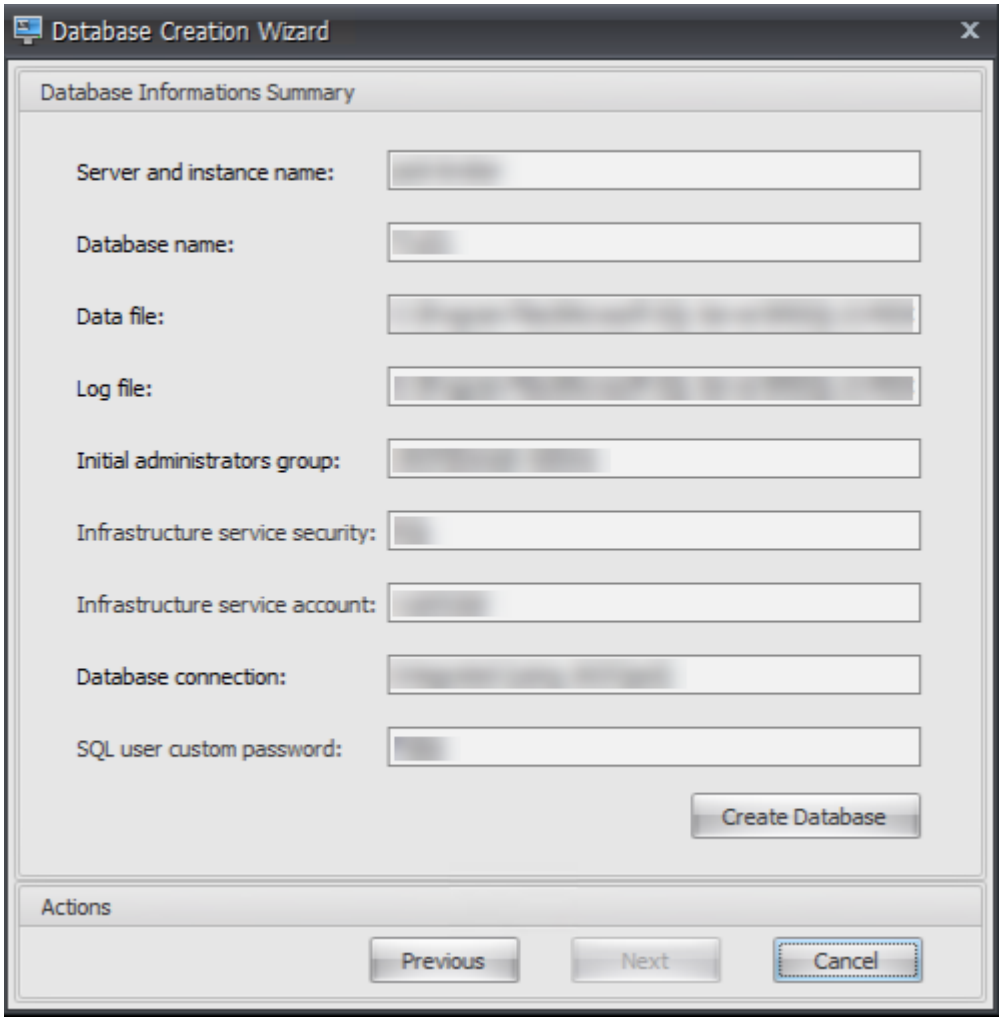
8. In the Select User window, type the name of the infrastructure service account, click **Check Names**, and then click **OK**.



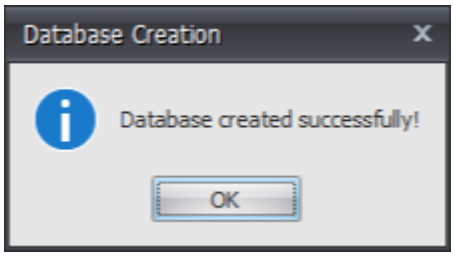
9. Click **Next**.



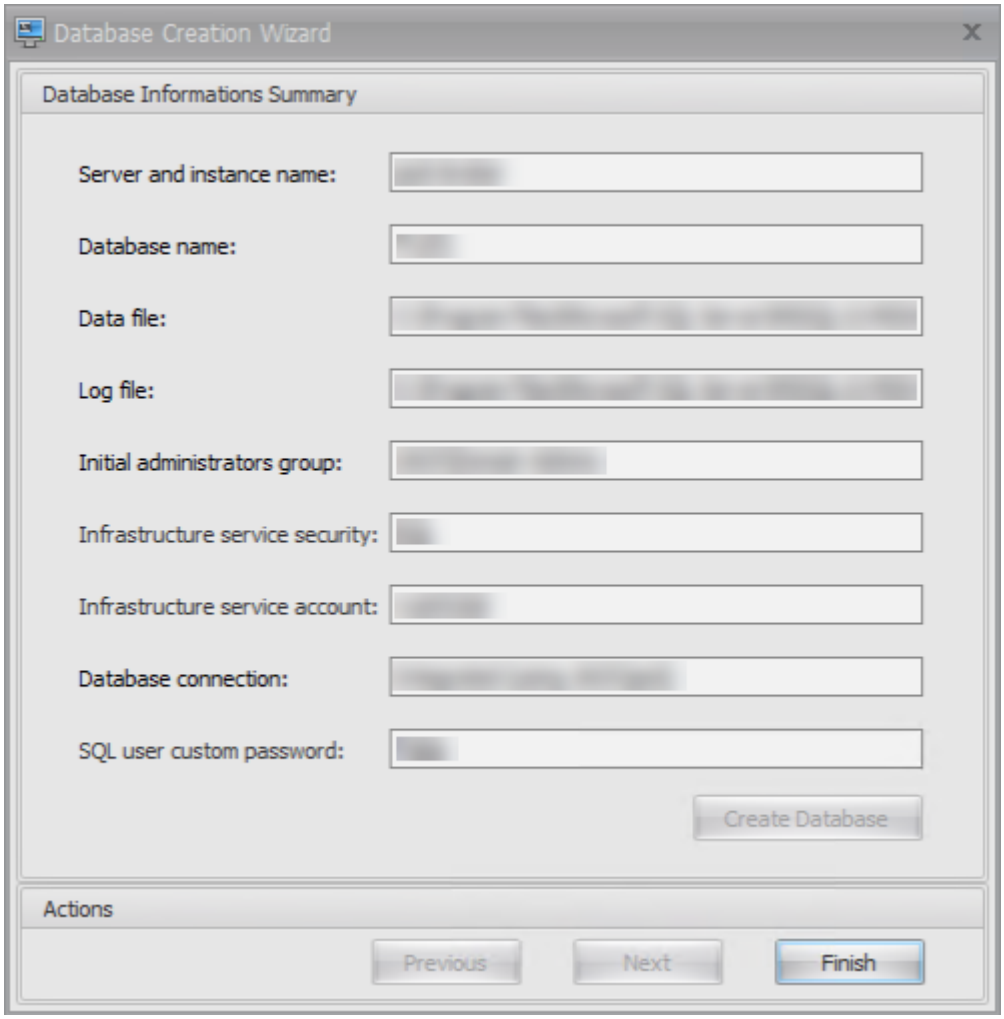
10. On the Database Information Summary page, click **Create Database**.



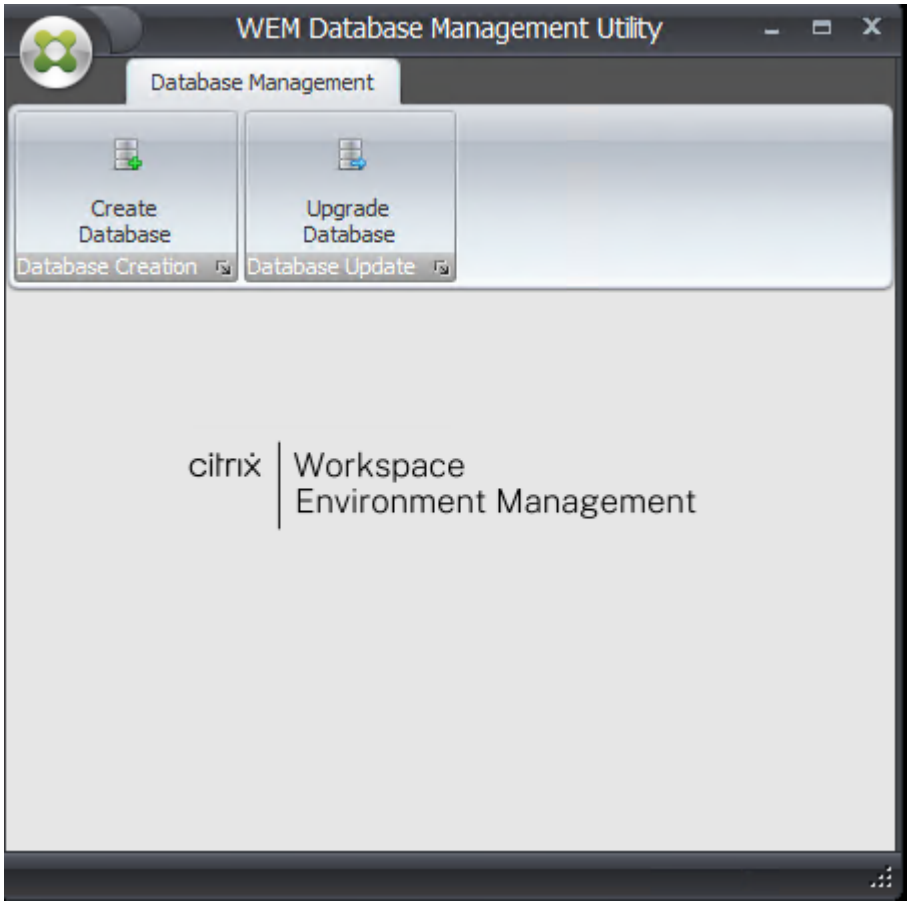
11. Click **OK**.



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

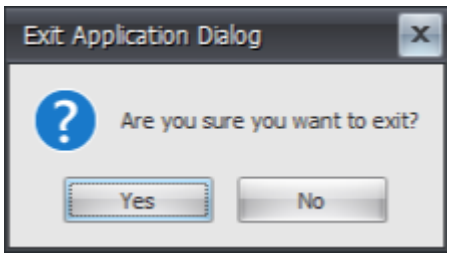


13. Close the **WEM Database Management Utility**.



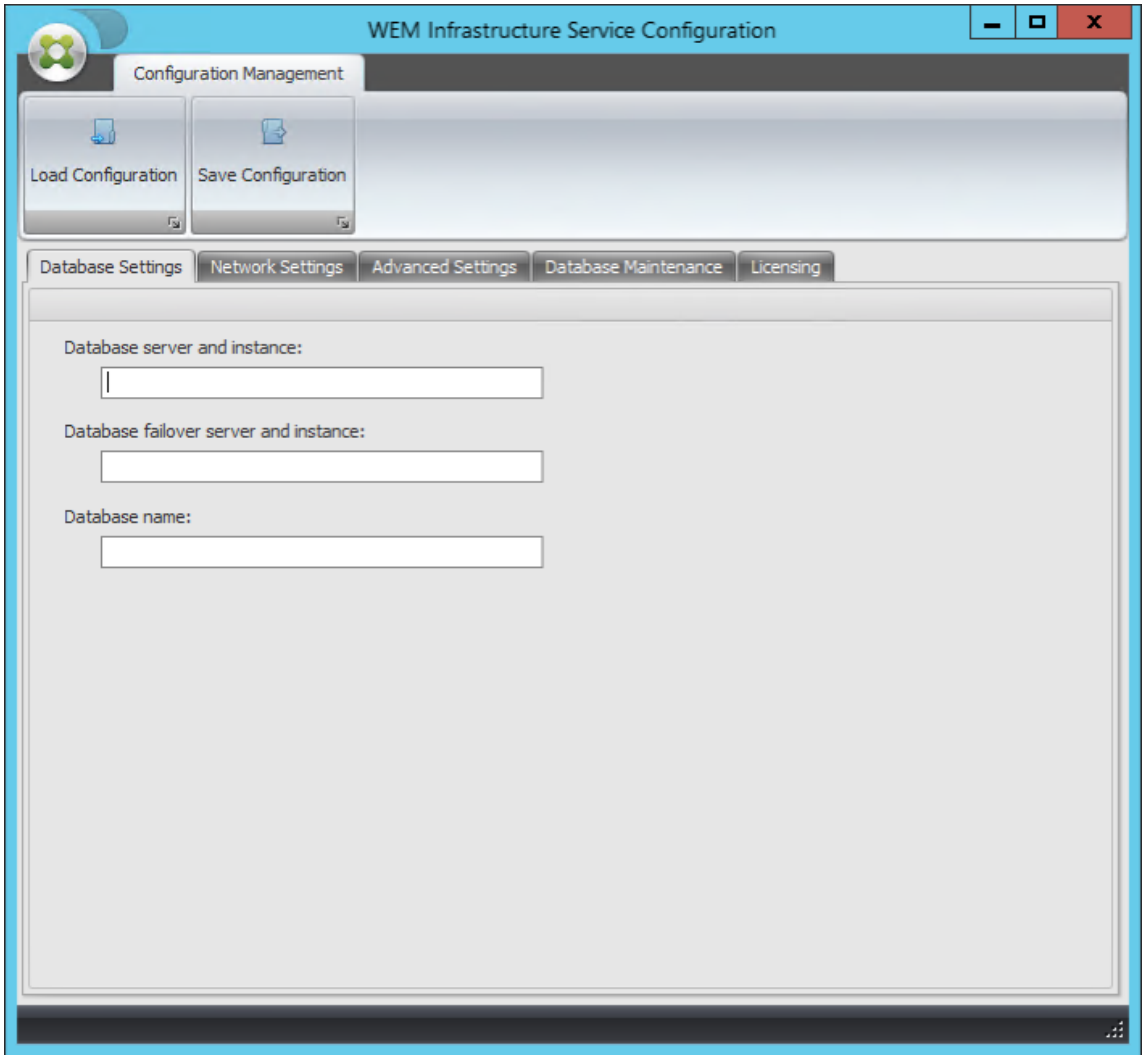
14. In the Exit Application Dialog, click **Yes**.

> **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.



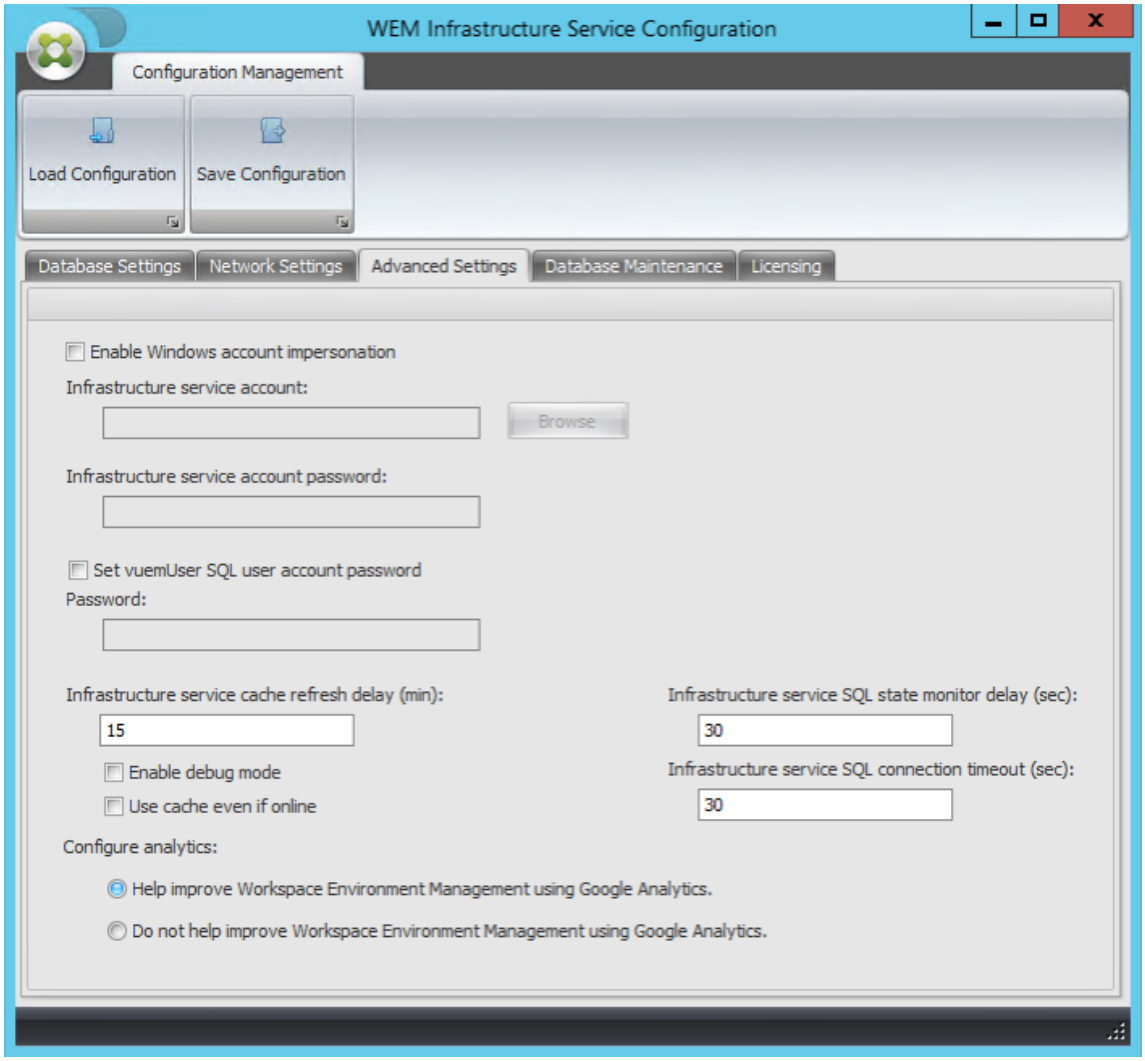
Step 3: Configure infrastructure services

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

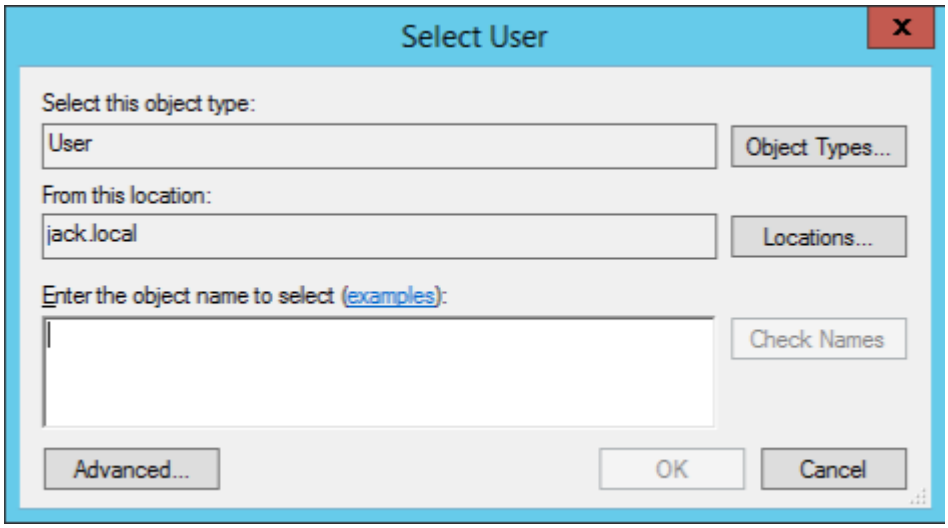


3. On the **Advanced Settings** tab, select **Enable Windows account impersonation** and then click **Browse**.

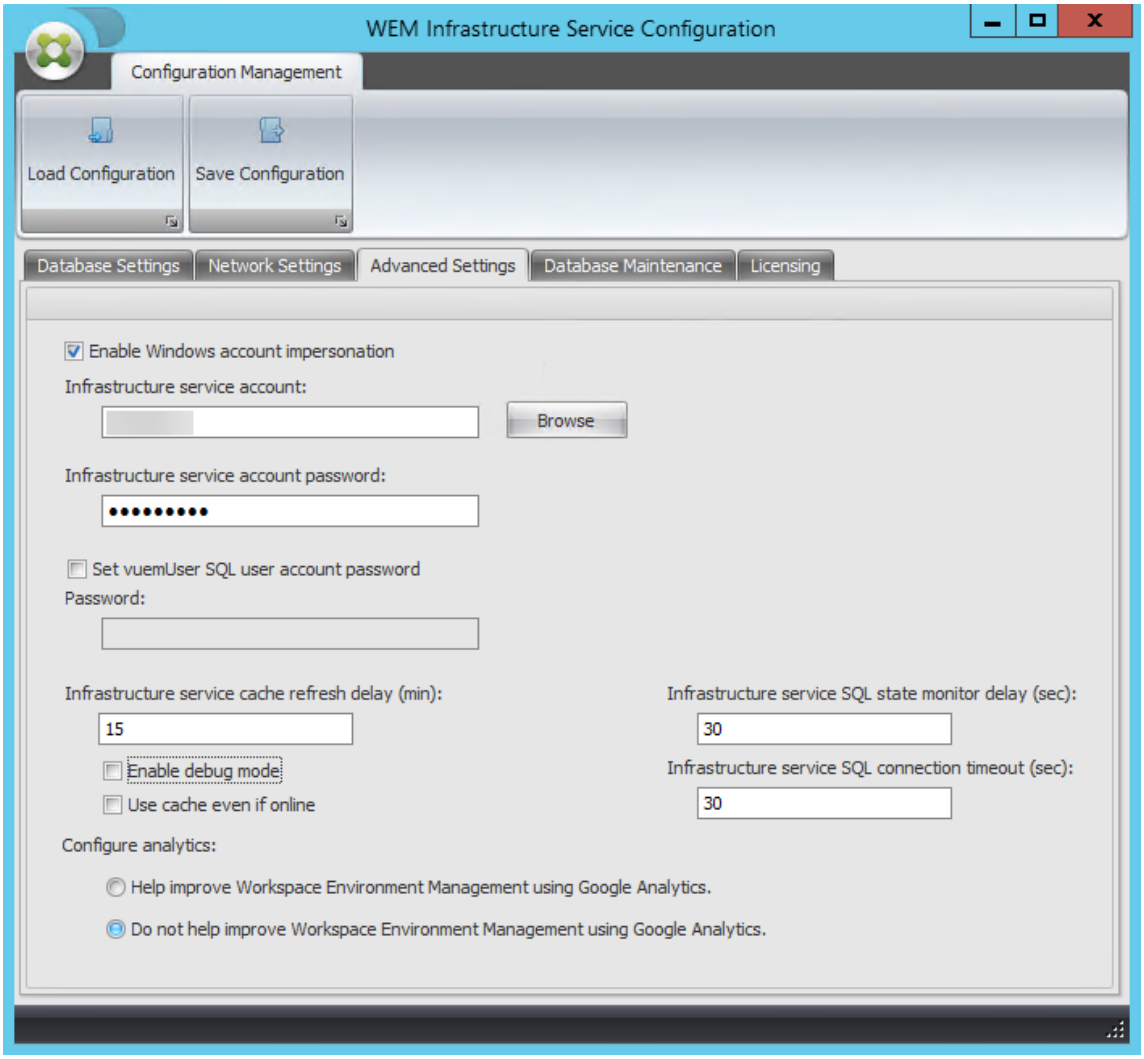
> **Note:**
>
> Depending on the choices you made during WEM database creation in Step 2, select **Enable Windows account impersonation** or **Set vuemUser SQL user account password**.



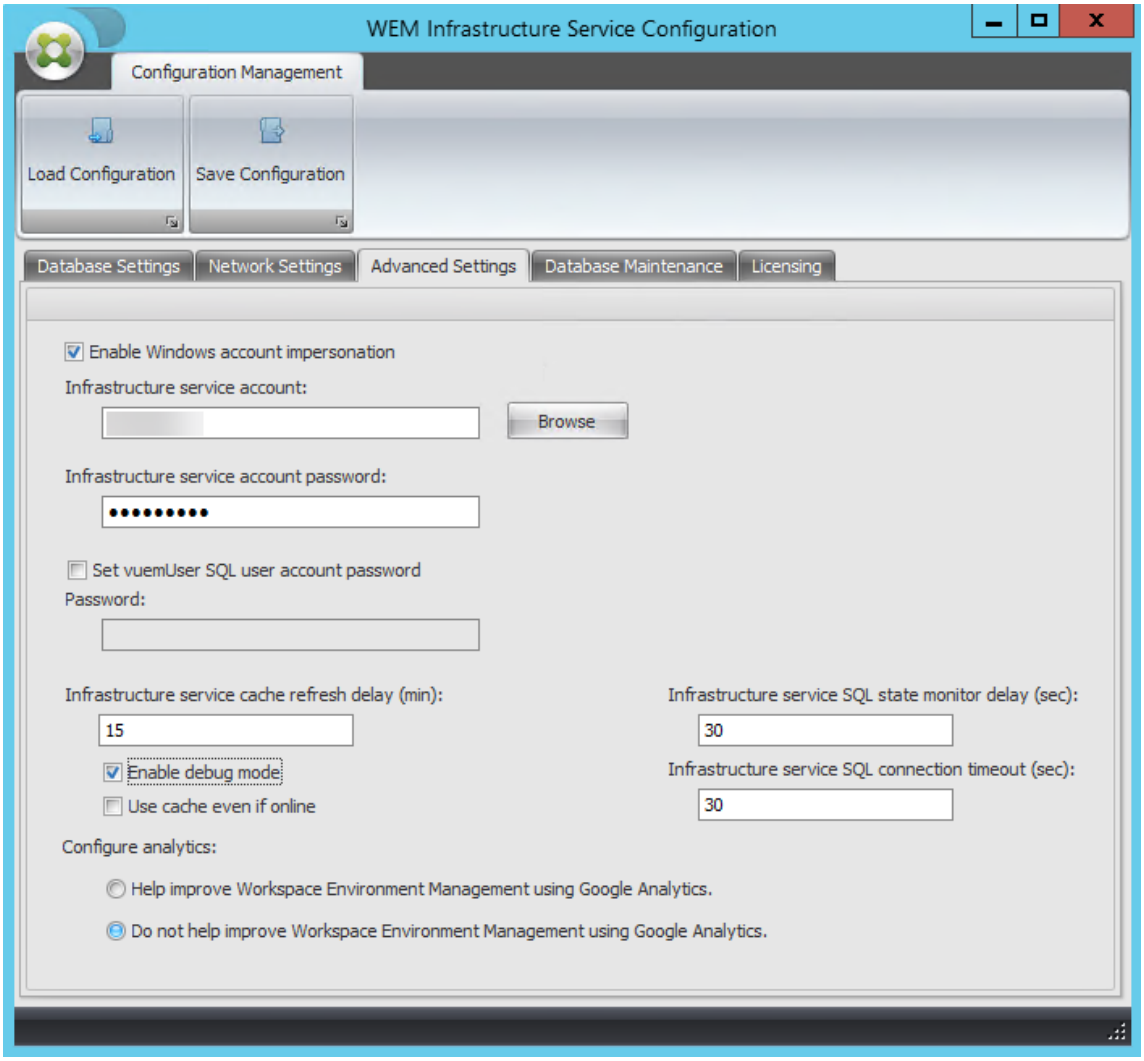
4. Type a user name, click **Check Names**, and then click **OK**.



5. Type the infrastructure service account password.

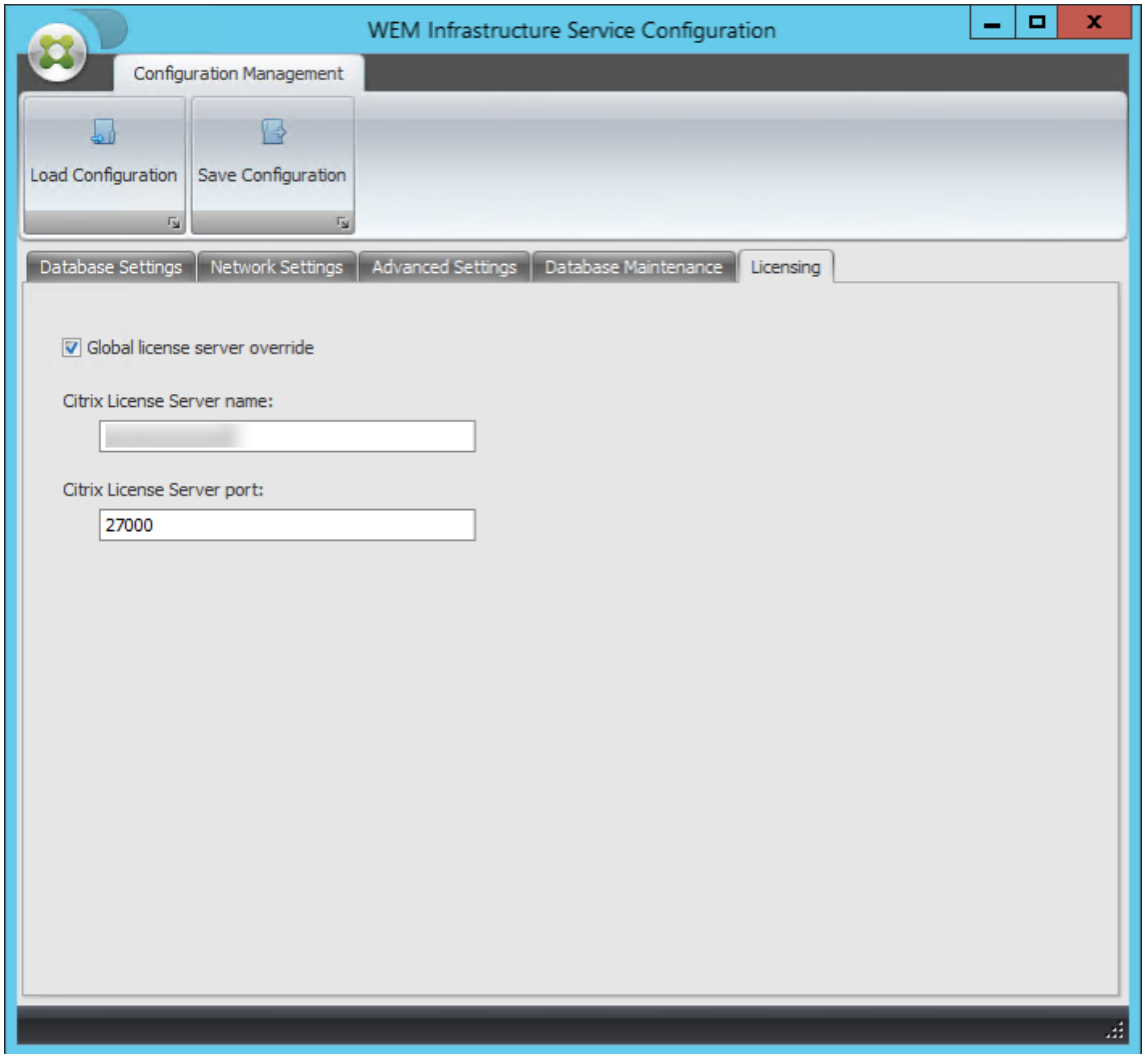


6. Select **Enable debug mode**.

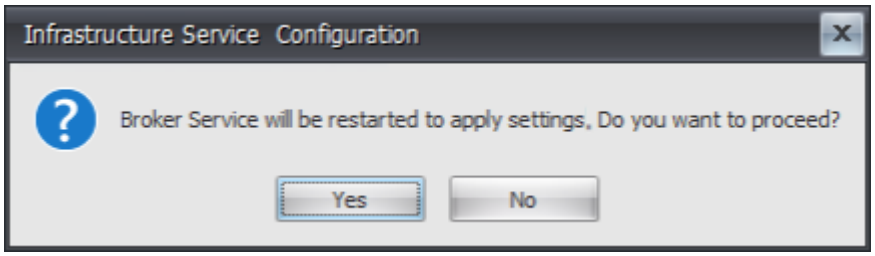


7. On the **Licensing** tab, select **Global license server override**, type your license information, and then click **Save Configuration.**

> **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.



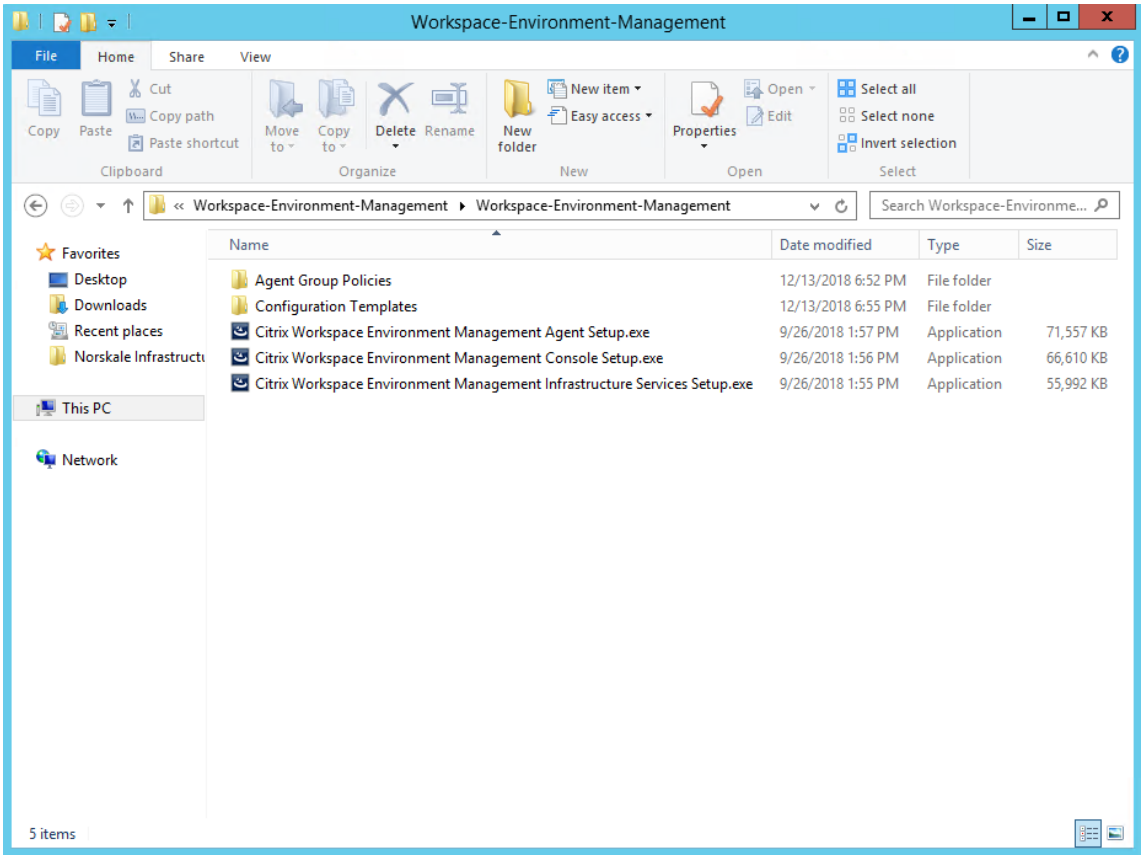
8. Click **Yes**.



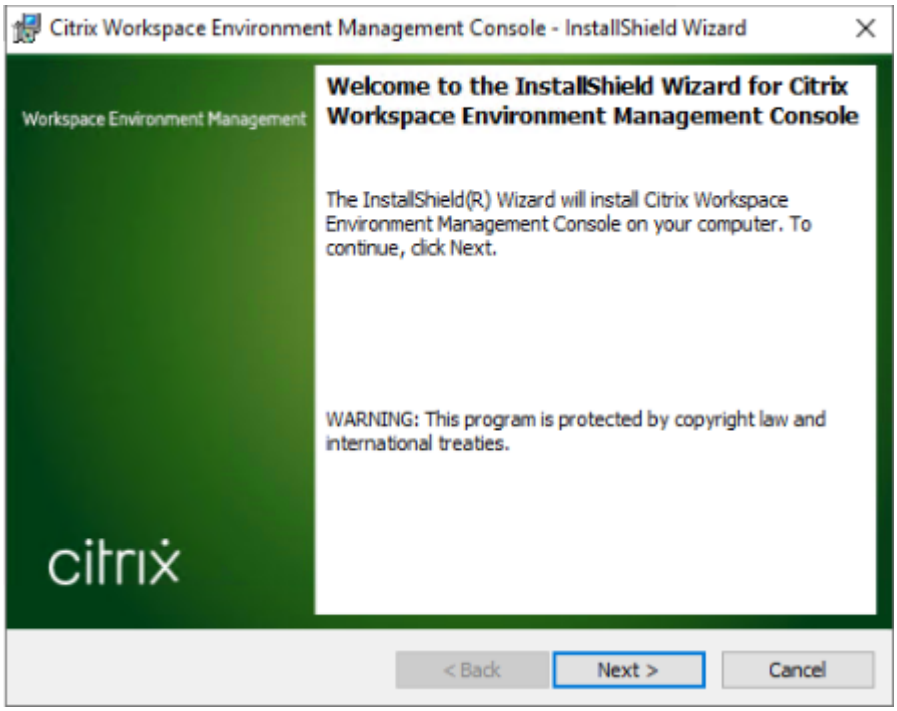
9. Close the **WEM Infrastructure Service Configuration** utility.

Step 4: Install the administration console

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

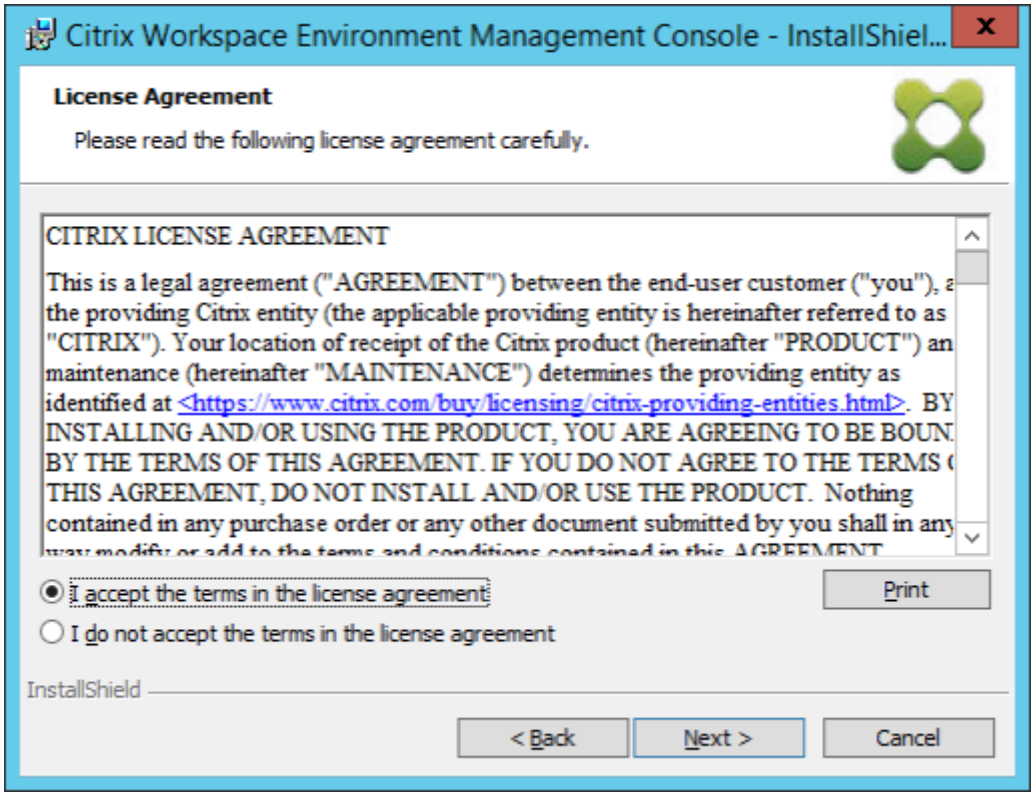


2. On the Welcome page, click **Next**.

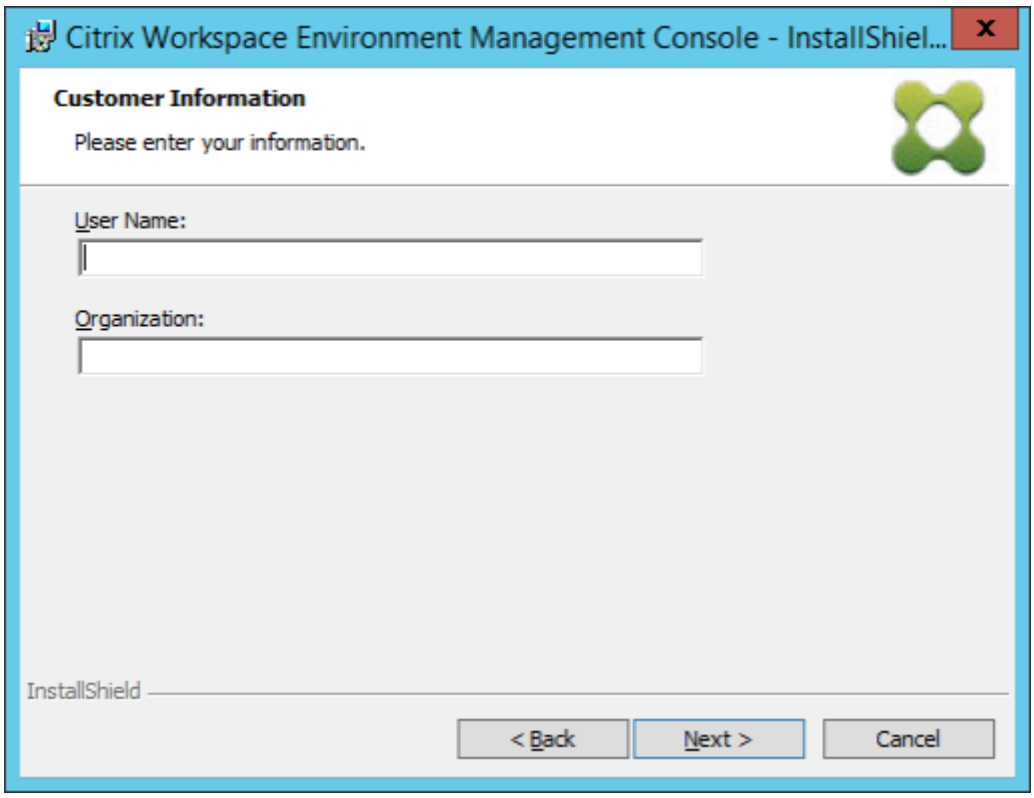


3. On the License Agreement page, select “I accept the terms in the license agreement” and then

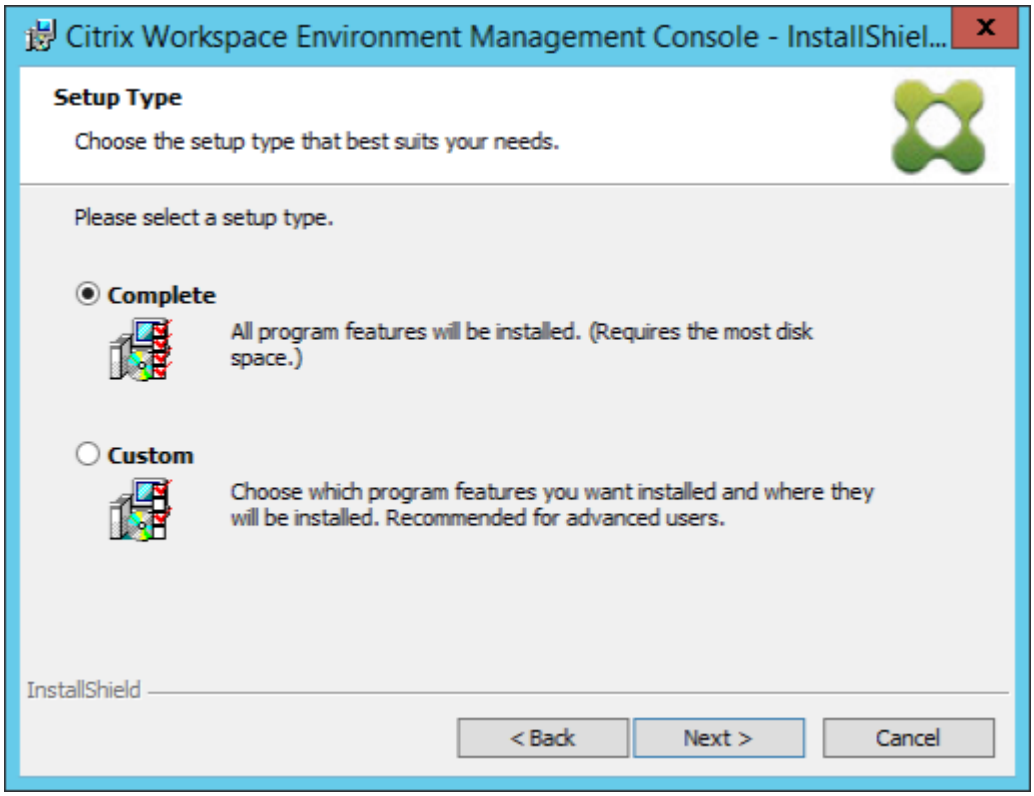
click **Next**.



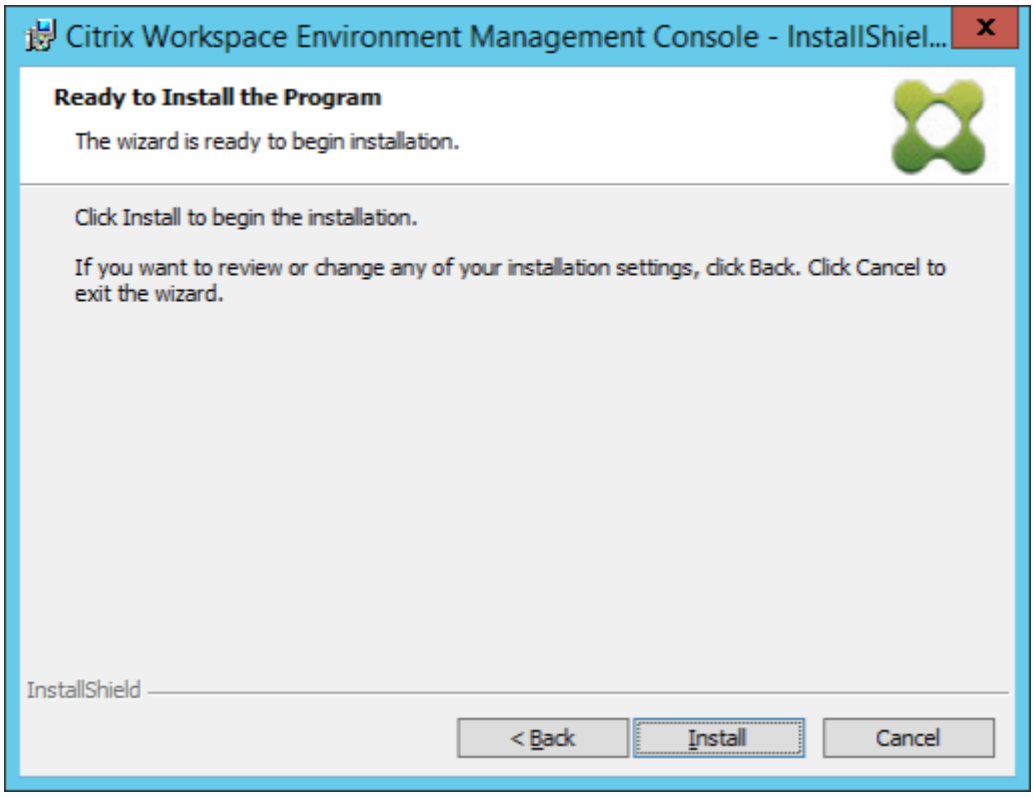
4. On the Customer Information page, type the required information and then click **Next**.



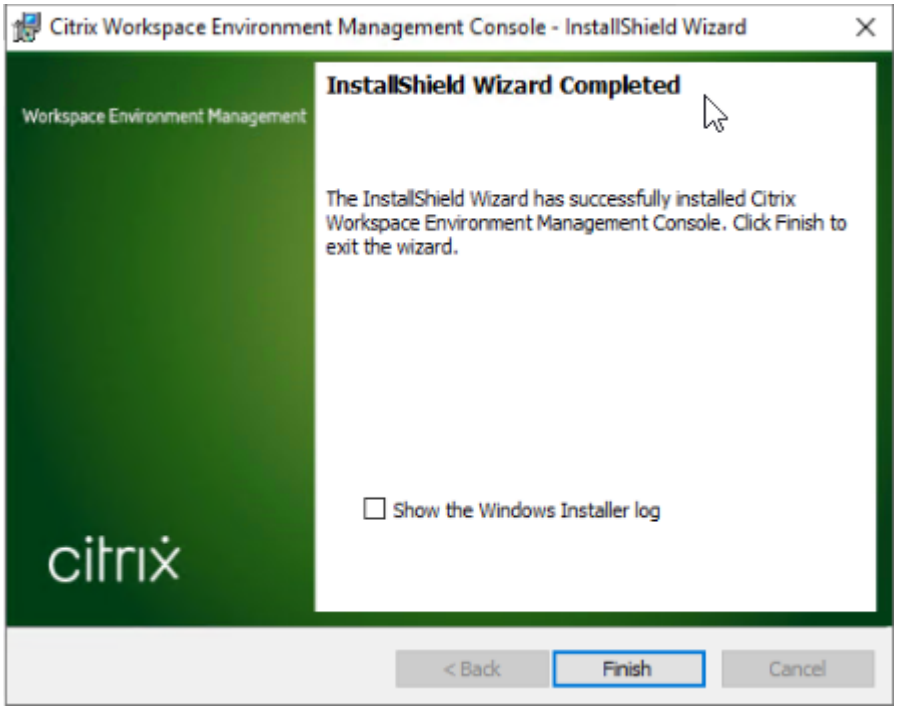
5. On the Setup Type page, select **Complete** and then click **Next**.



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

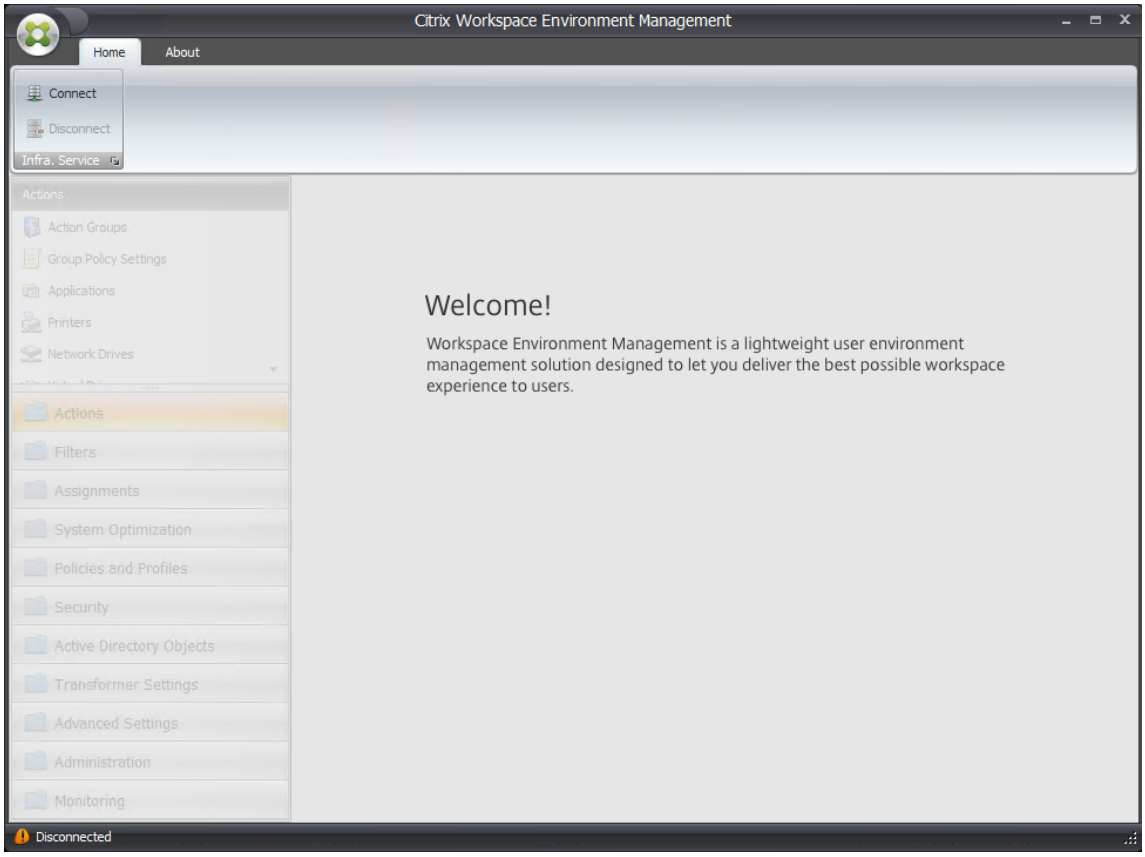


7. Click **Finish** to exit the wizard.



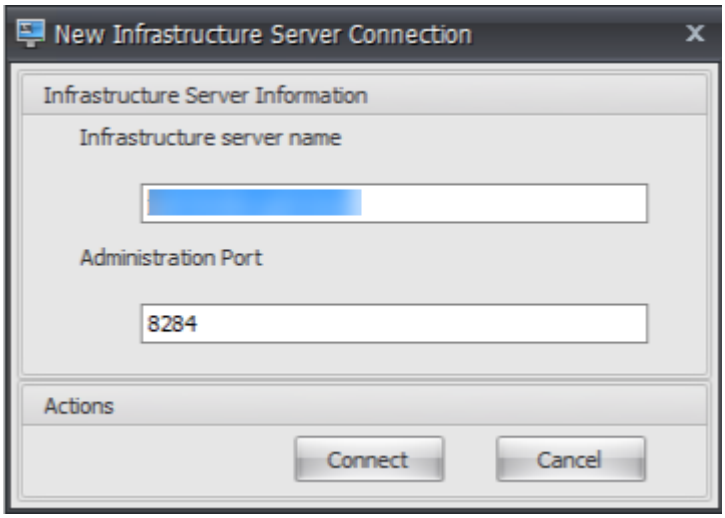
Step 5: Configure configuration sets

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

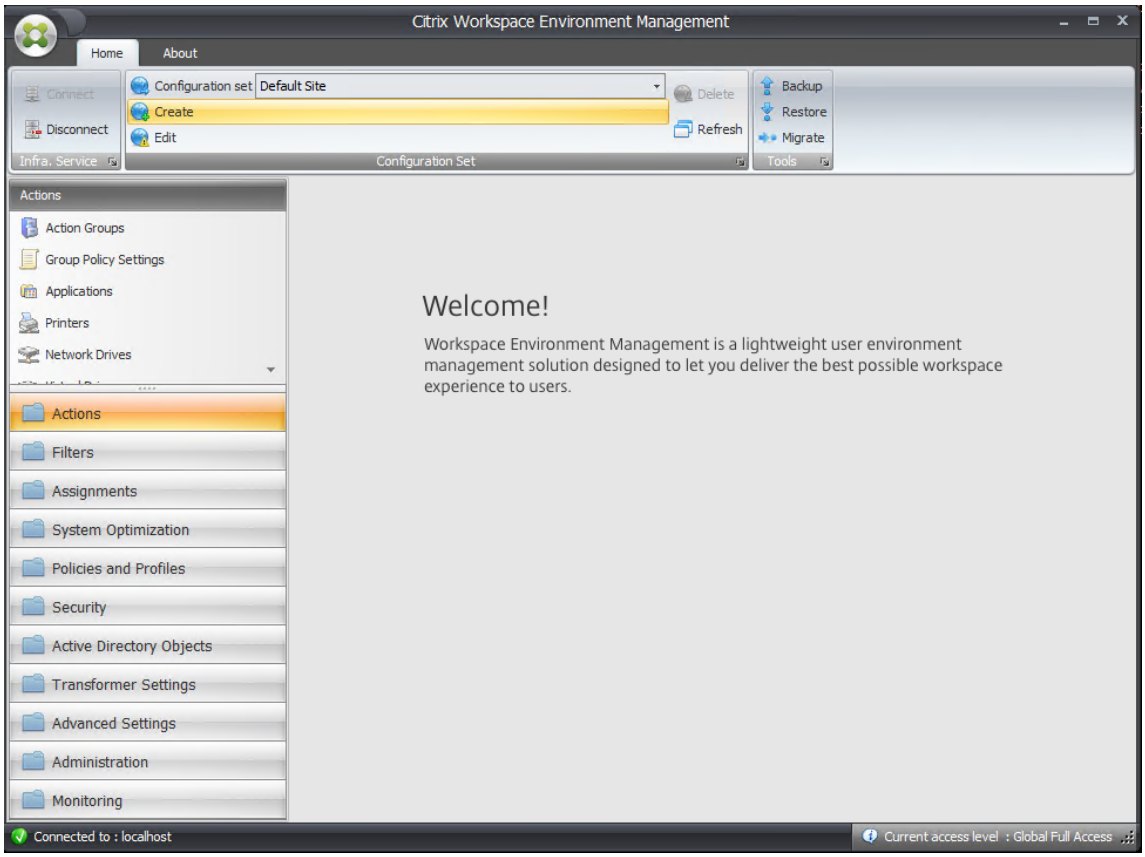


2. In the New Infrastructure Server Connection window, check the information and then click **Connect**.

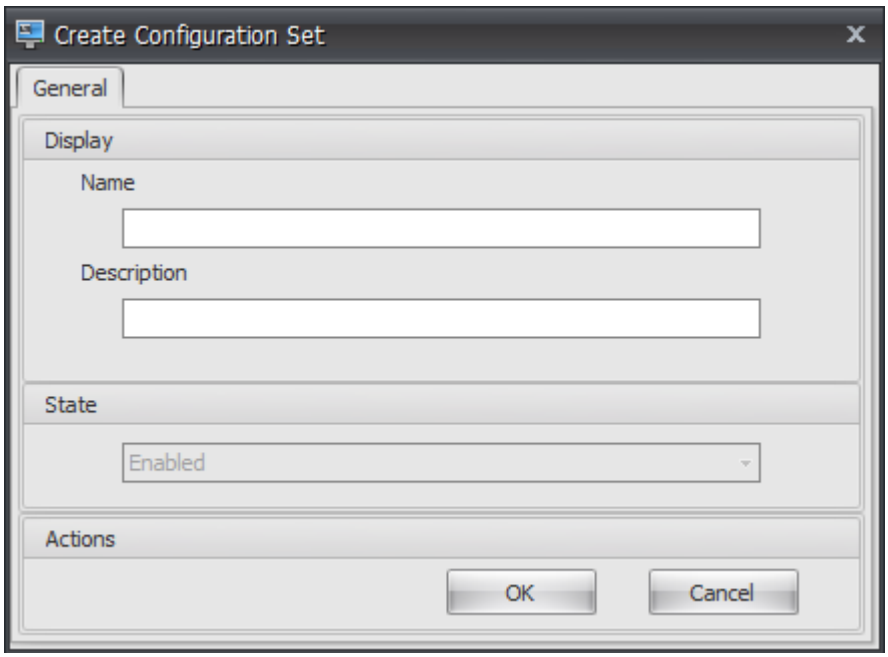
> **Note:**
>
> - For Infrastructure server name, type the machine name, fully qualified domain name, or IP address of the WEM infrastructure server.
> - For Administration port, the default port is 8284.



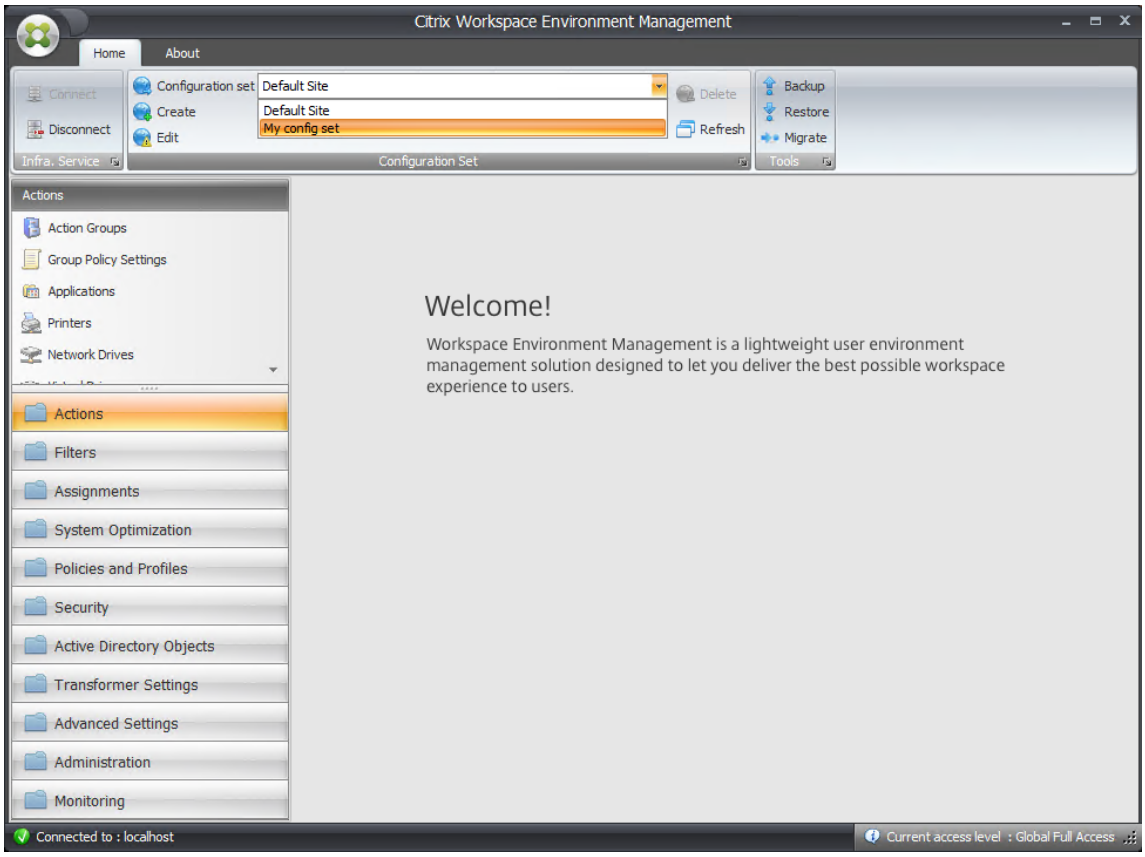
3. On the **Home** tab, on the ribbon, click **Create** to create your configuration set.



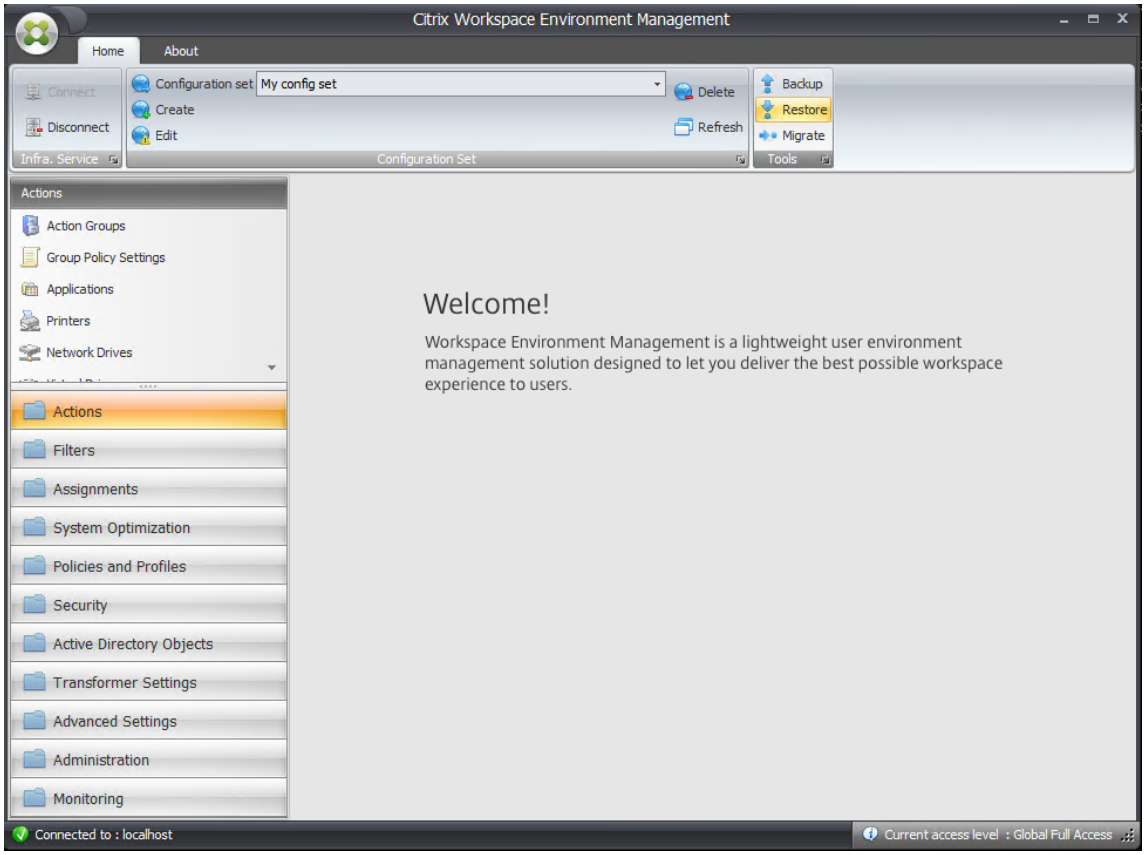
4. In the Create Configuration Set window, type a name and description for your configuration set and then click **OK**.



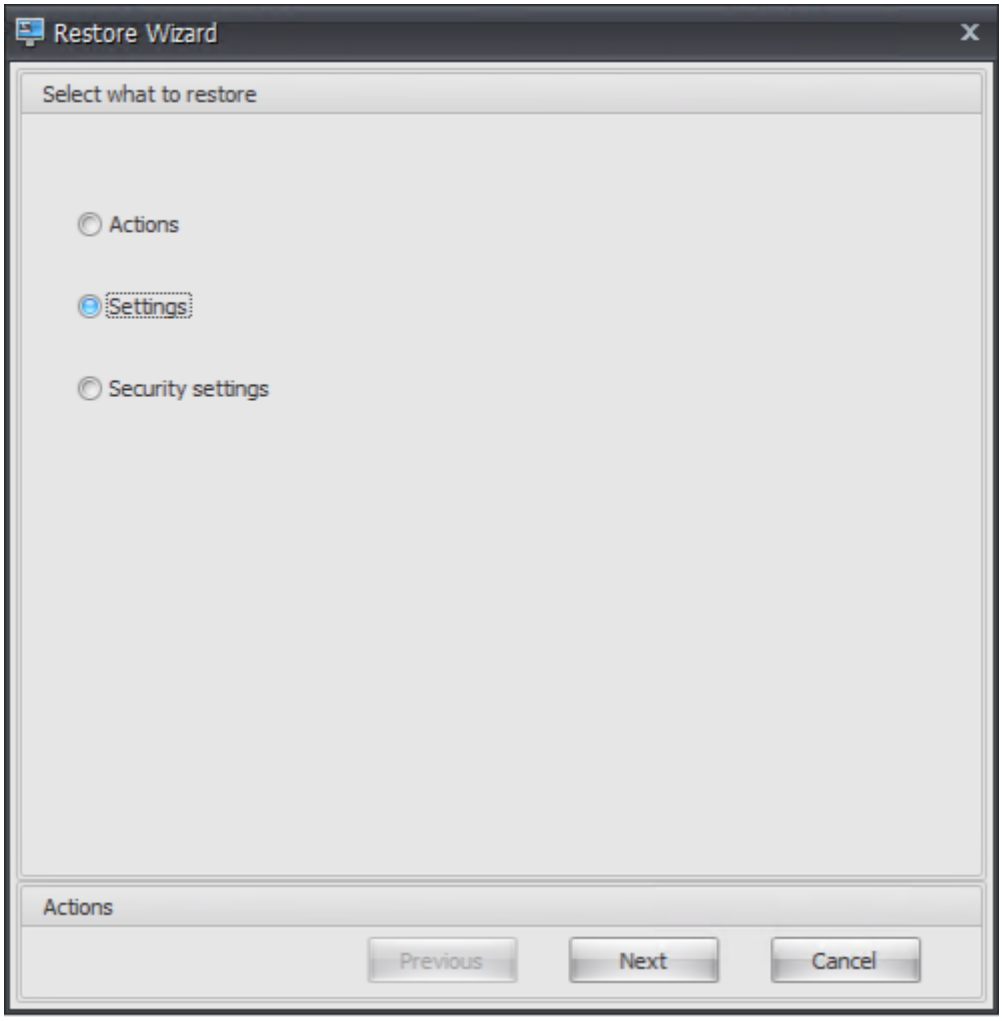
5. On the ribbon, under **Configuration Set**, select the newly created configuration set.



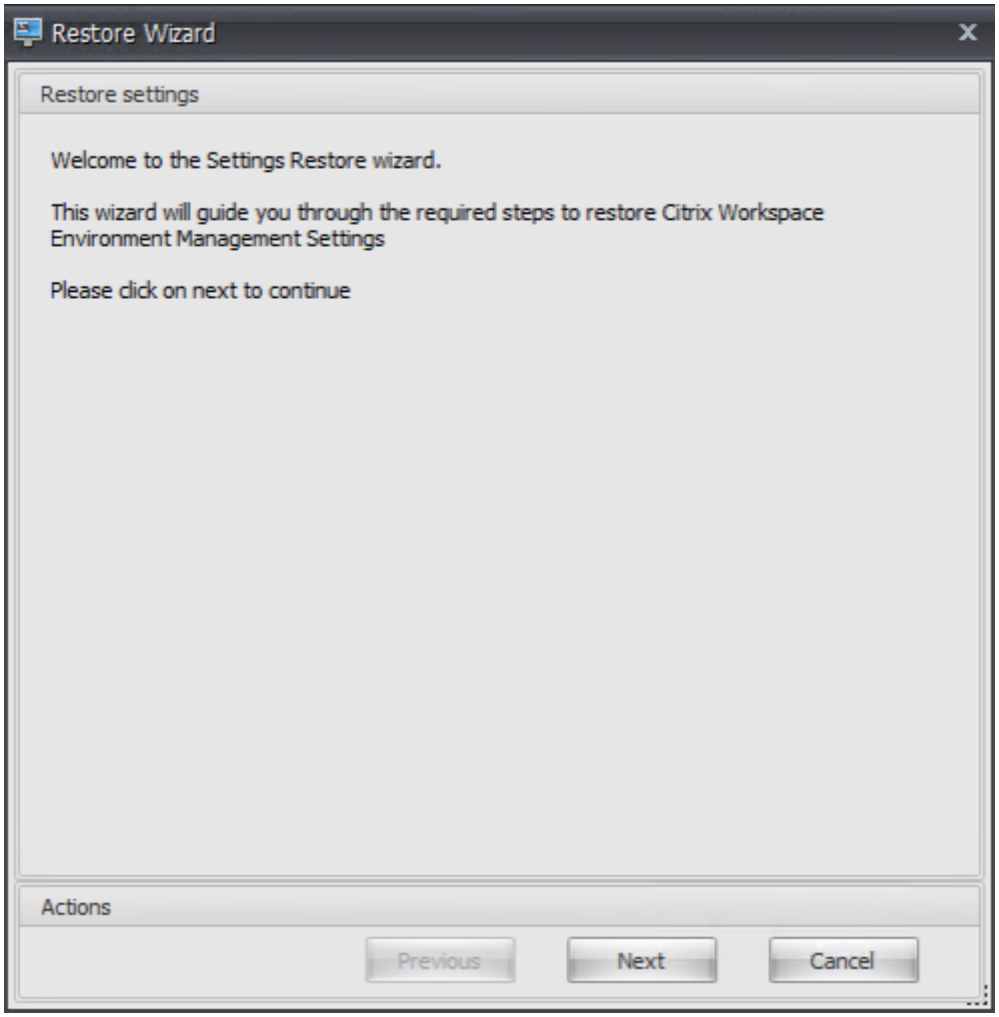
6. On the ribbon, under **Backup**, click **Restore**. The Restore wizard appears.



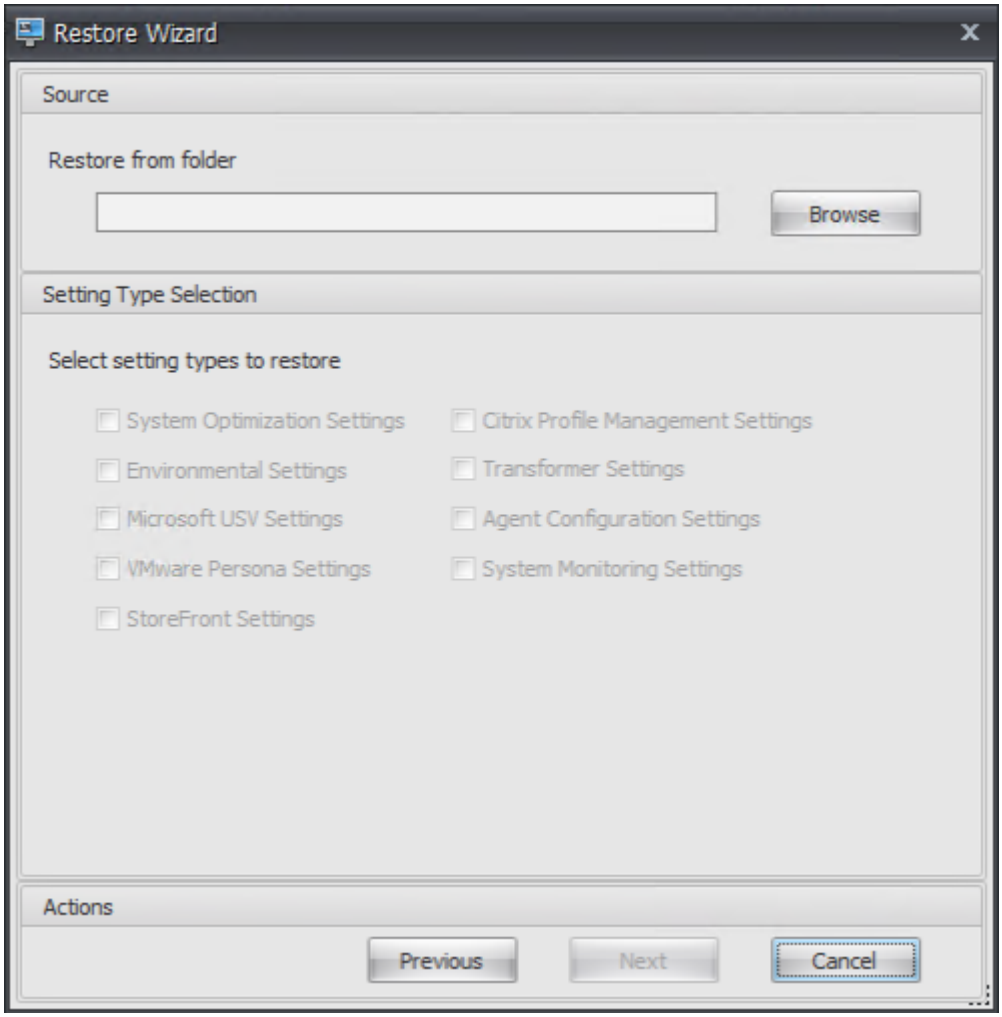
7. On the Select what to restore page, select **Settings** and then click **Next**.



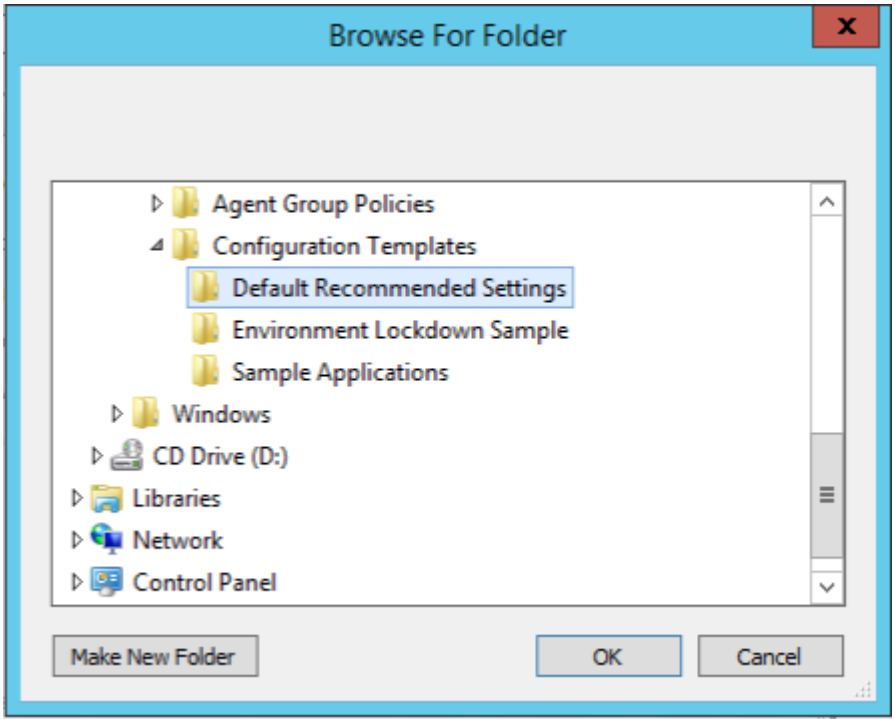
8. On the Restore settings page, click **Next**.



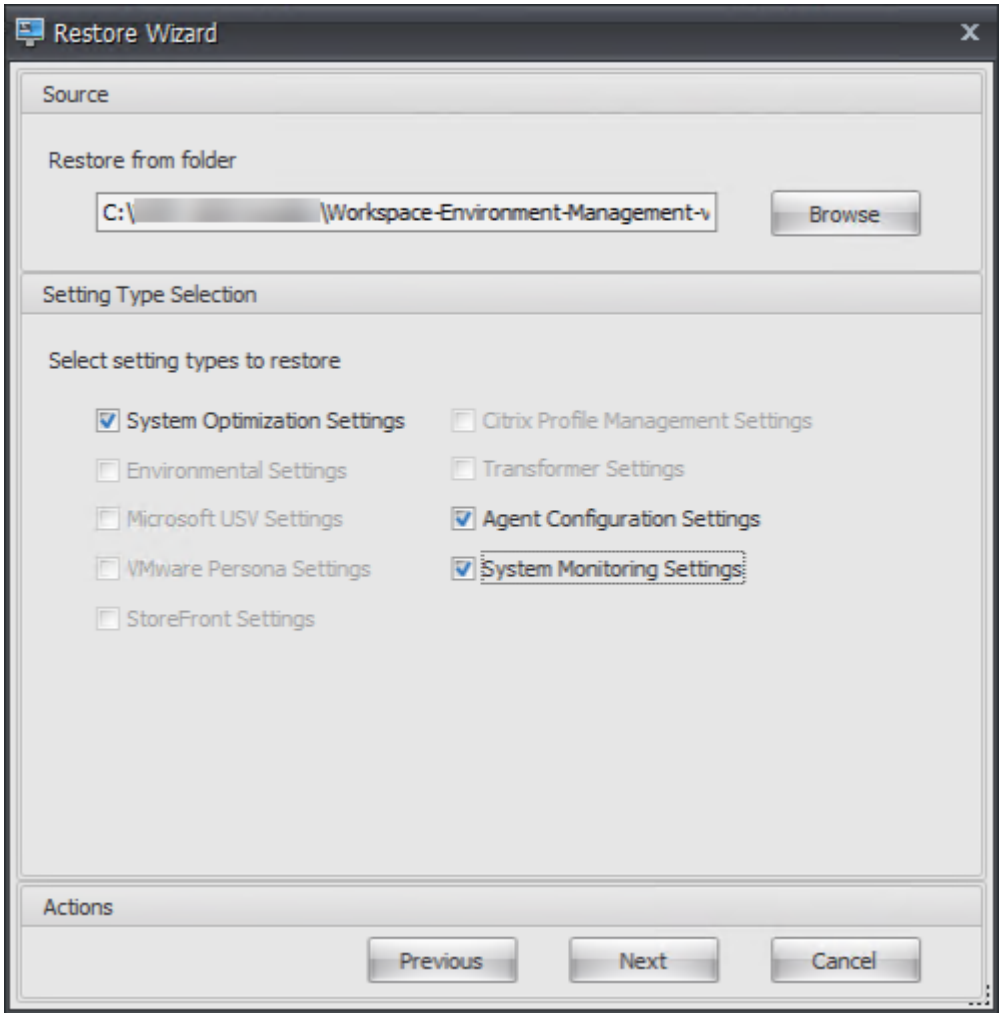
9. On the Source page, click **Browse**.



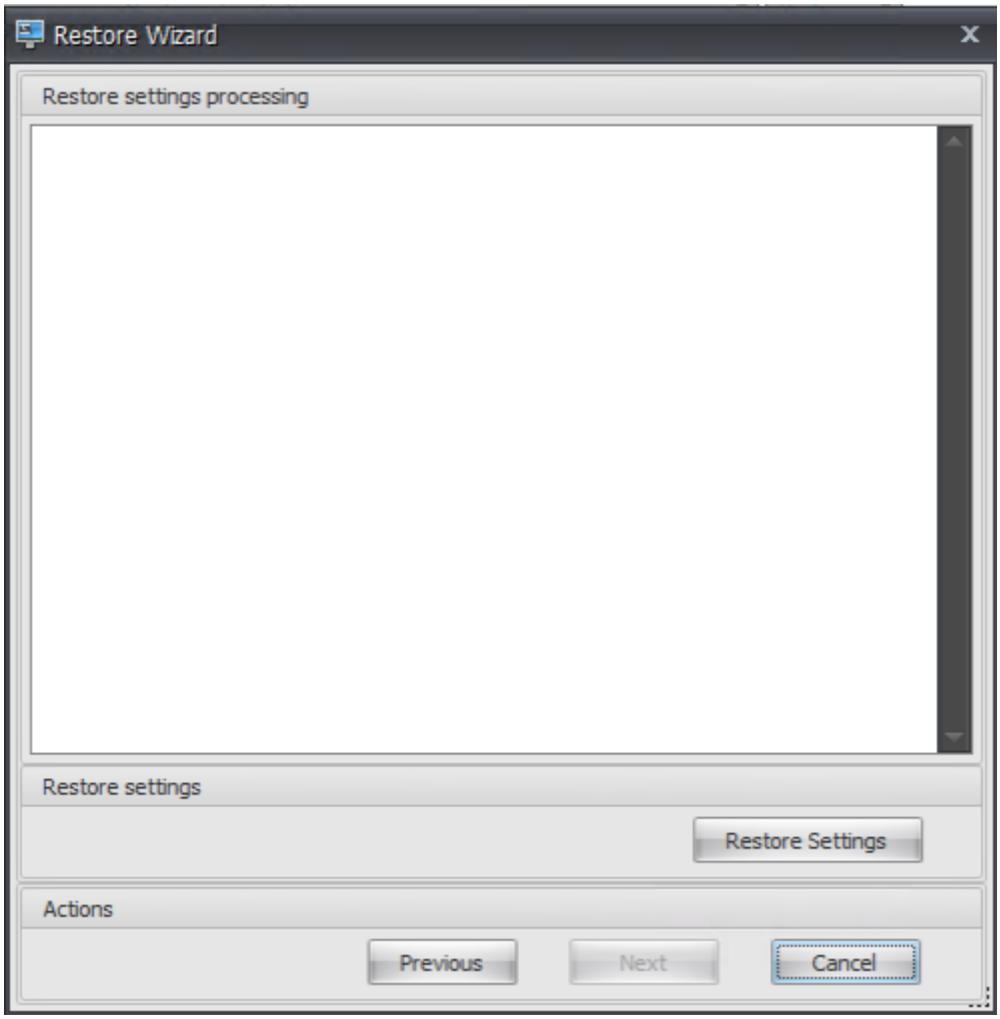
10. In the Browse For Folder window, browse to the **Default Recommended Settings** folder (provided with Workspace Environment Management) and then click **OK**.



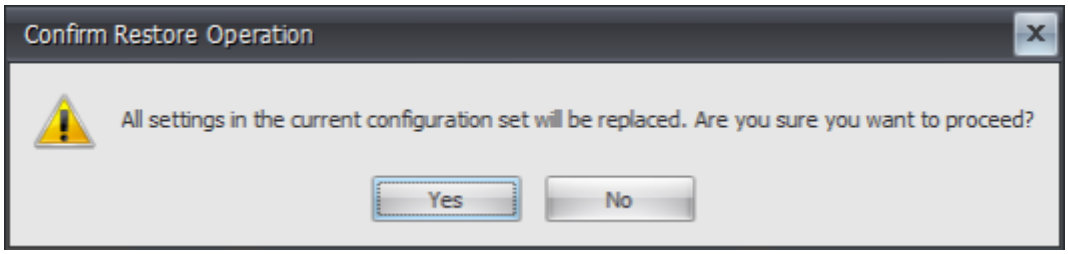
11. On the Source page, select **System Optimization Settings**, **Agent Configuration Settings**, and **System Monitoring Settings**, and then click **Next**.



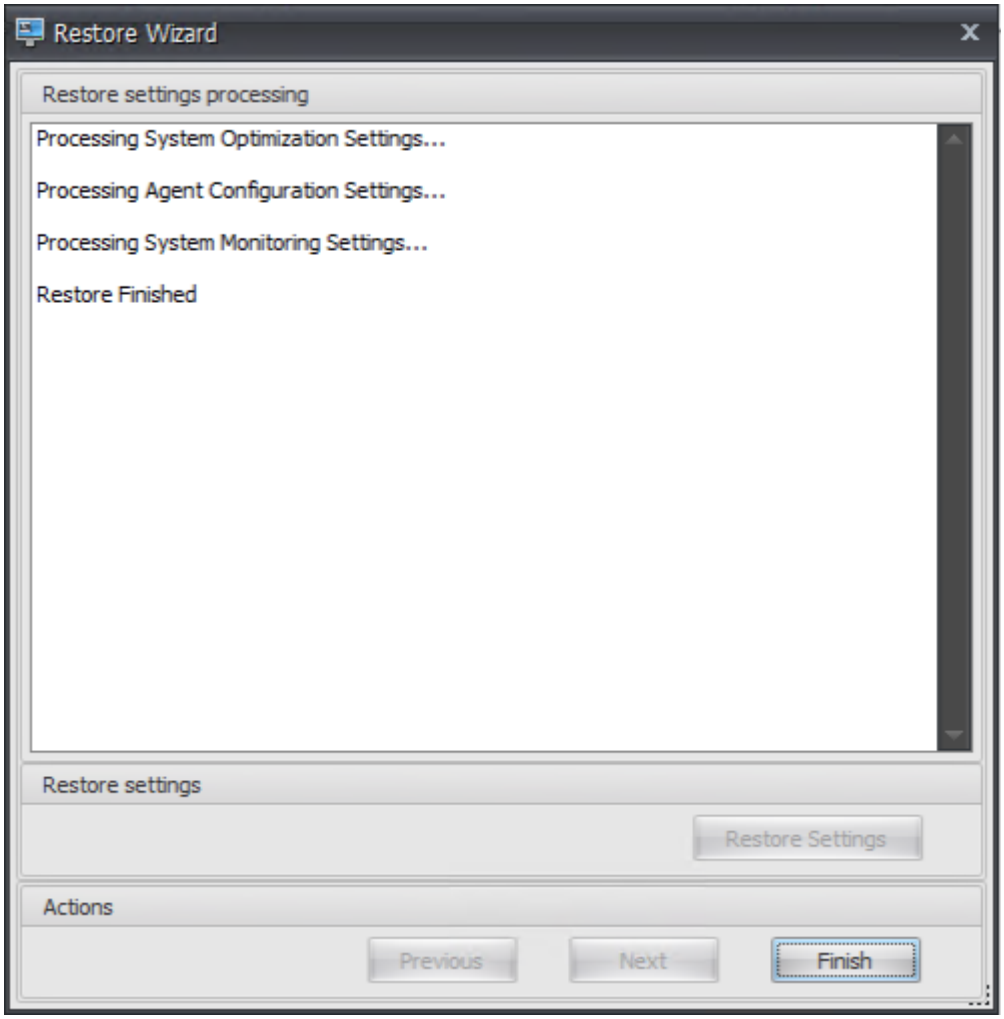
12. On the Restore settings processing page, under Restore settings, click **Restore Settings**.



13. Click **Yes**.



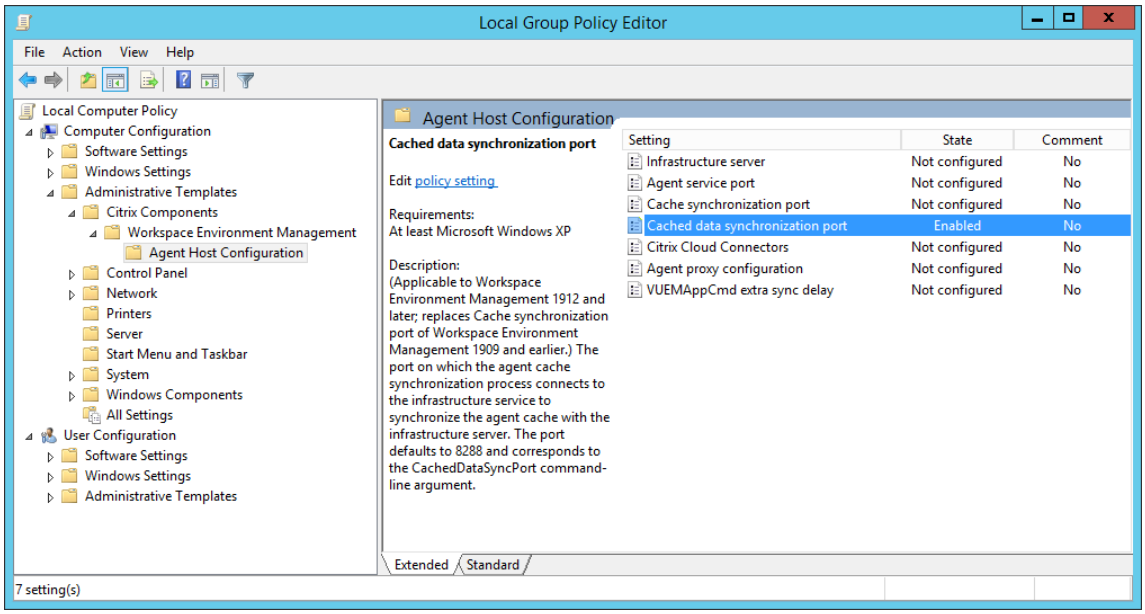
14. Click **Finish**.



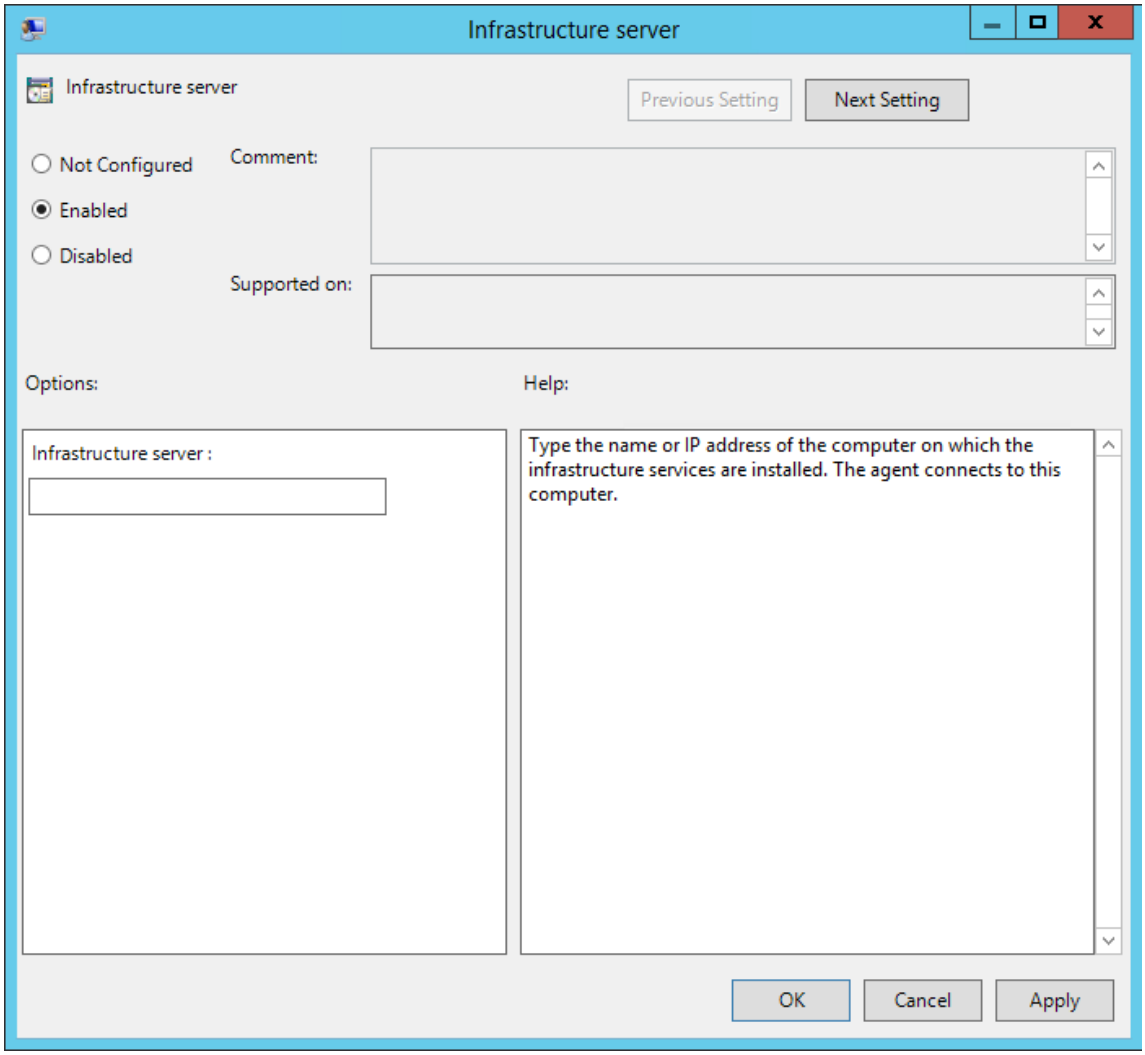
Step 6: Add the group policy template

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

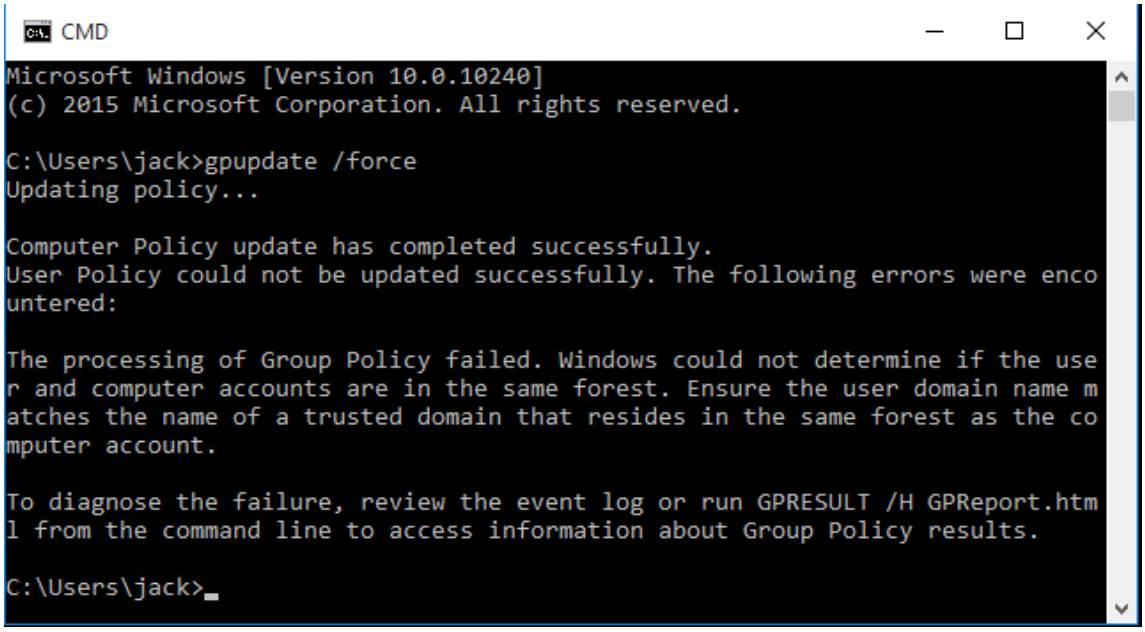
4. In the Group Policy Management Editor window, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **Classic Administrative Templates (ADM)** > **Citrix** > **Workspace Environment Management** > **Agent Host Configuration** and double-click **Infrastructure server**.



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



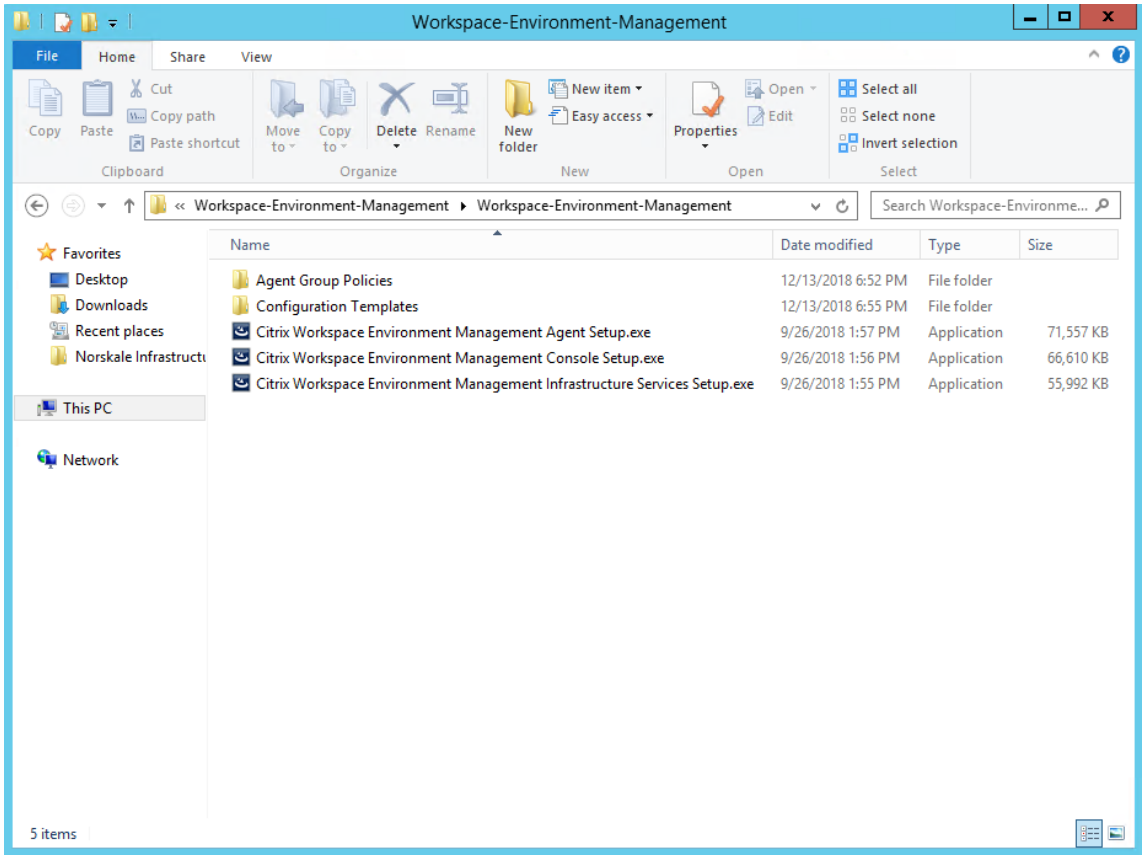
6. Go to the agent host, open a command line, and type `gpupdate /force`.



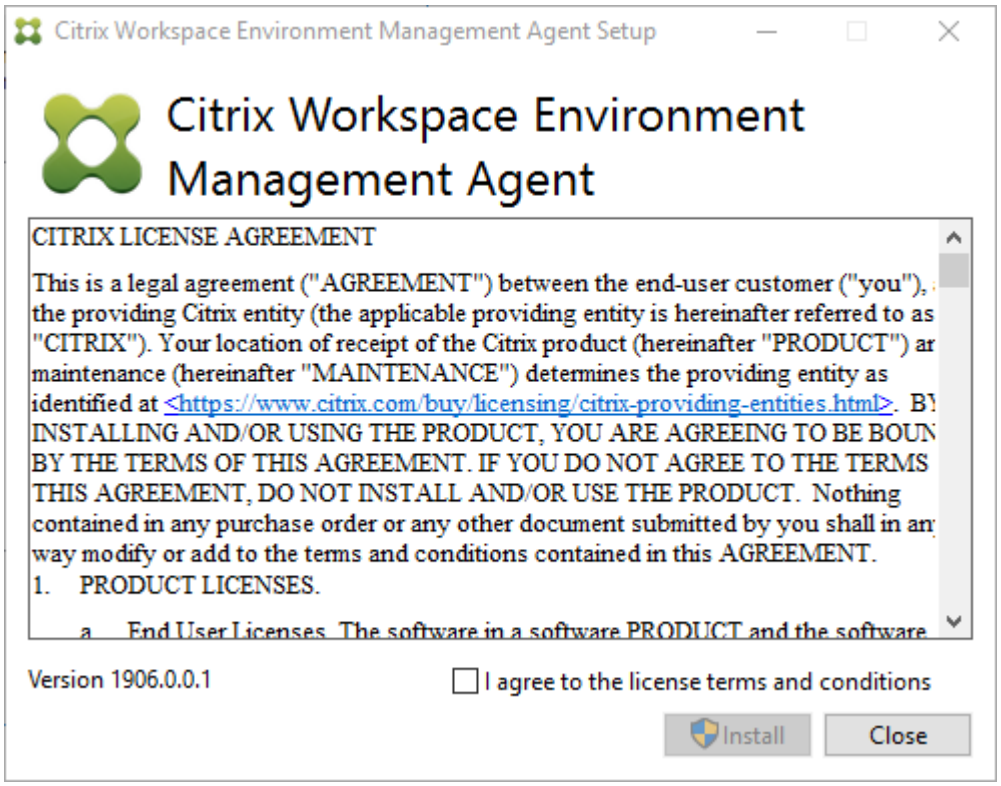
Step 7: Install the agent

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

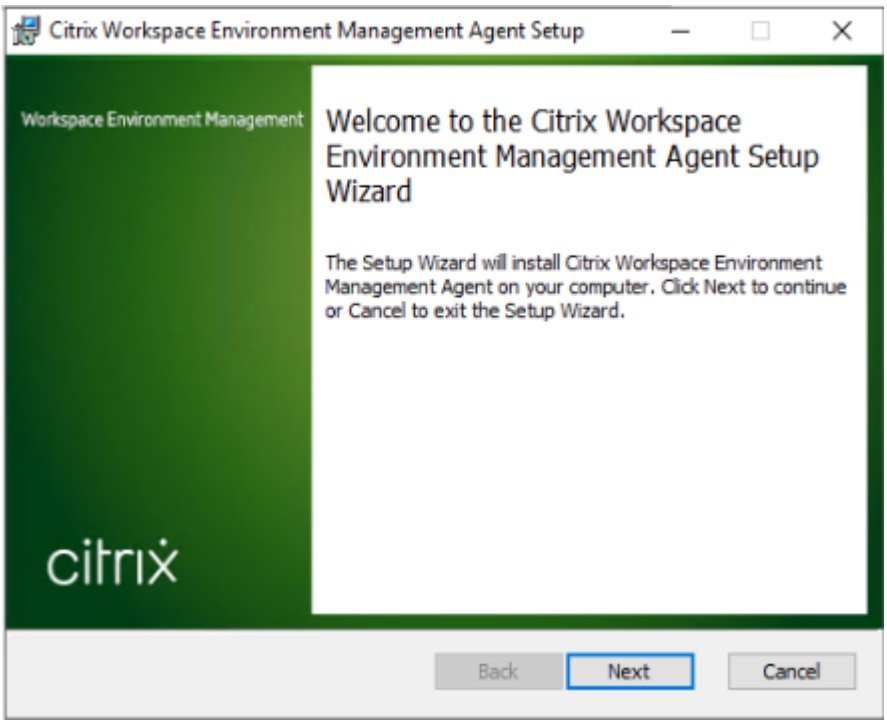
1. Run **Citrix Workspace Environment Management Agent Setup.exe** on your machine.



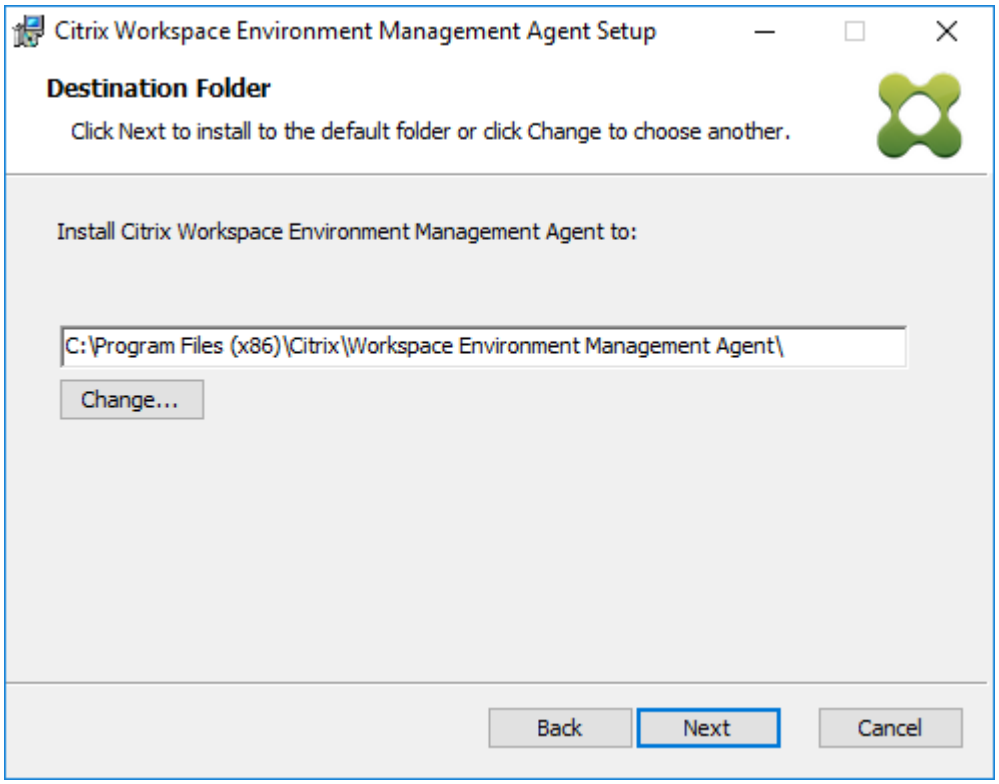
2. Select **I agree to the license terms and conditions** and then click **Install**.



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

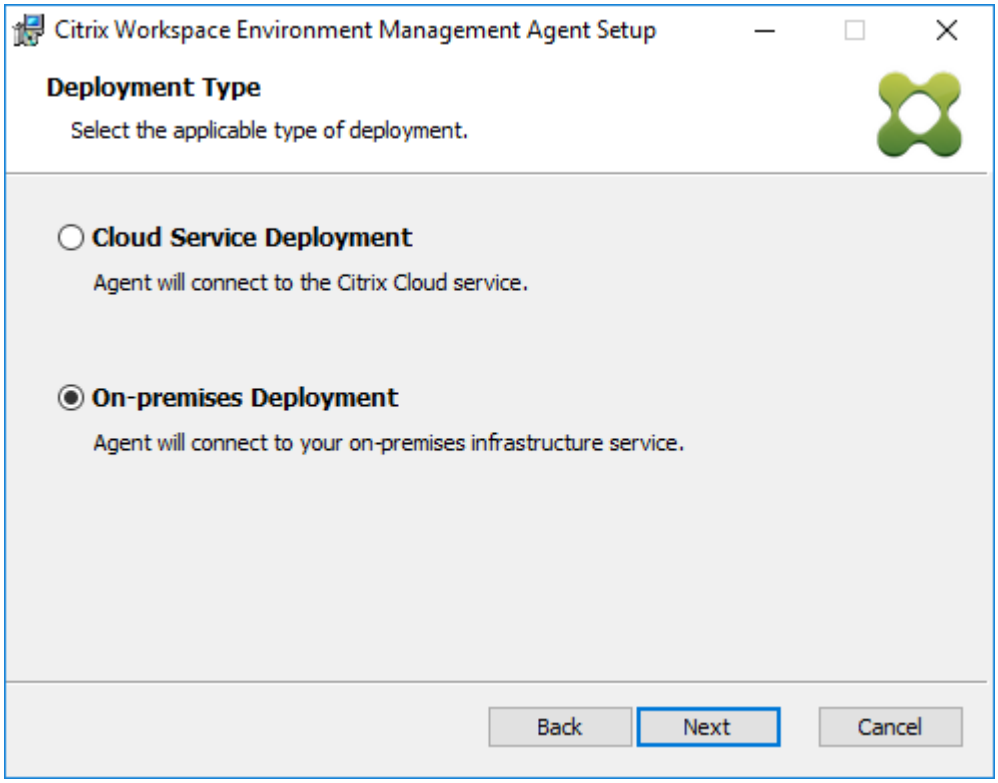


4. On the Destination Folder page, click **Next**.

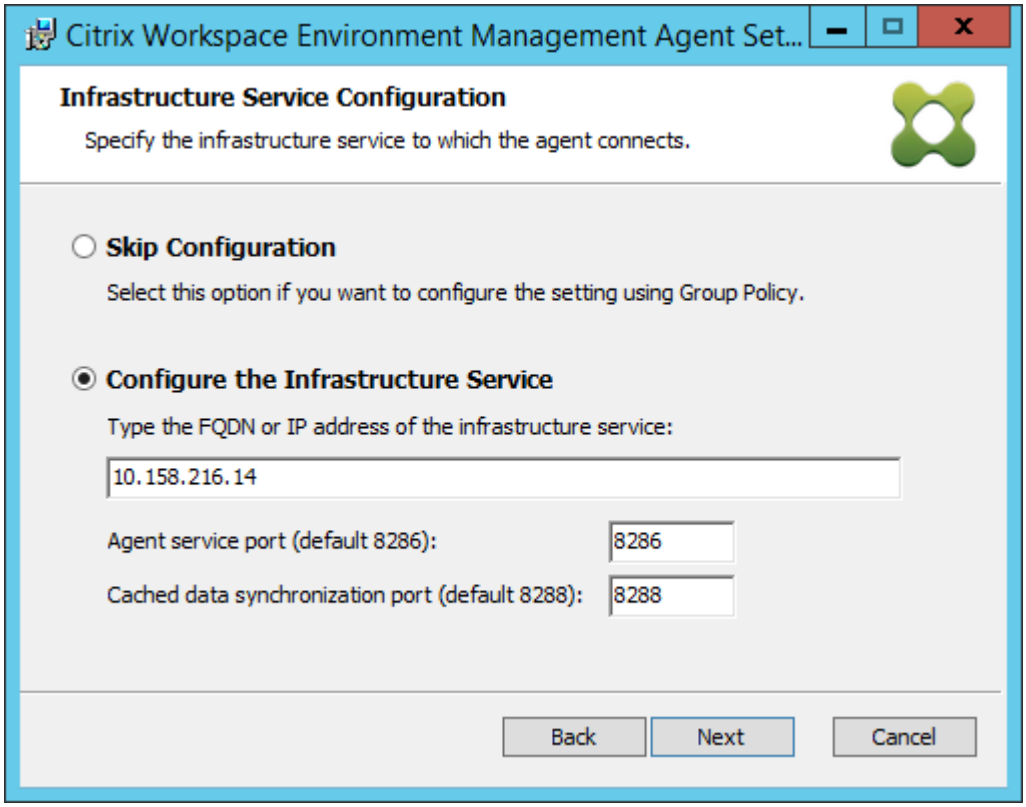


5. On the Deployment Type page, select the applicable type of deployment and then click **Next**.

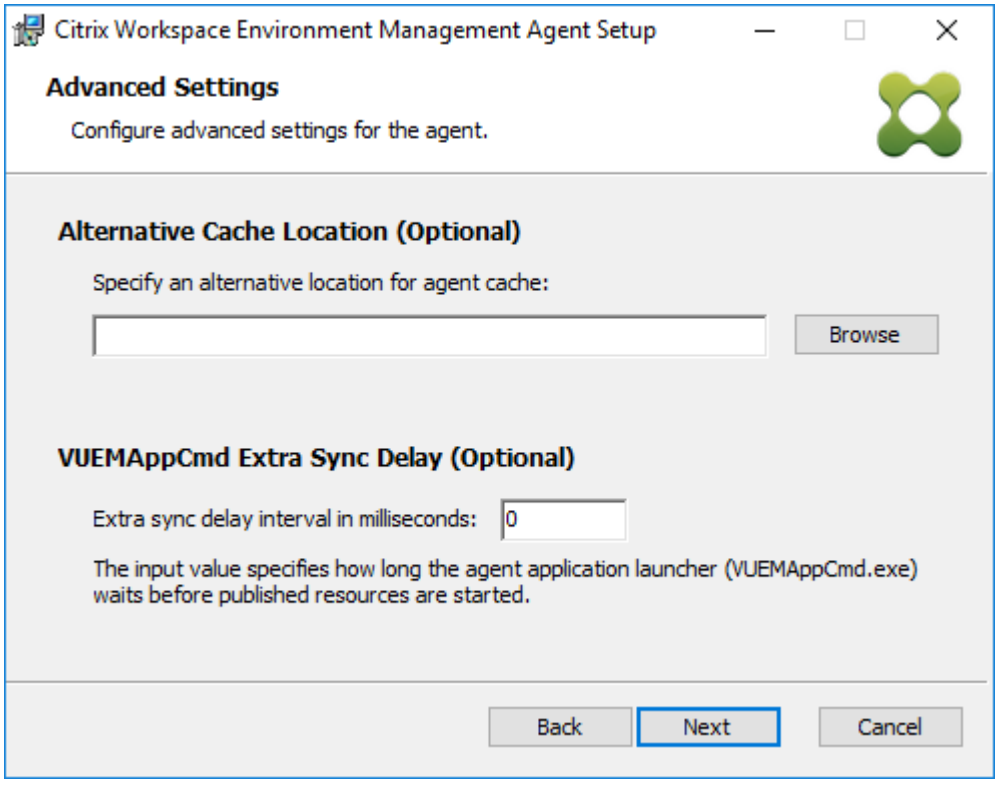
In this case, select **On-premises Deployment**.



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



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

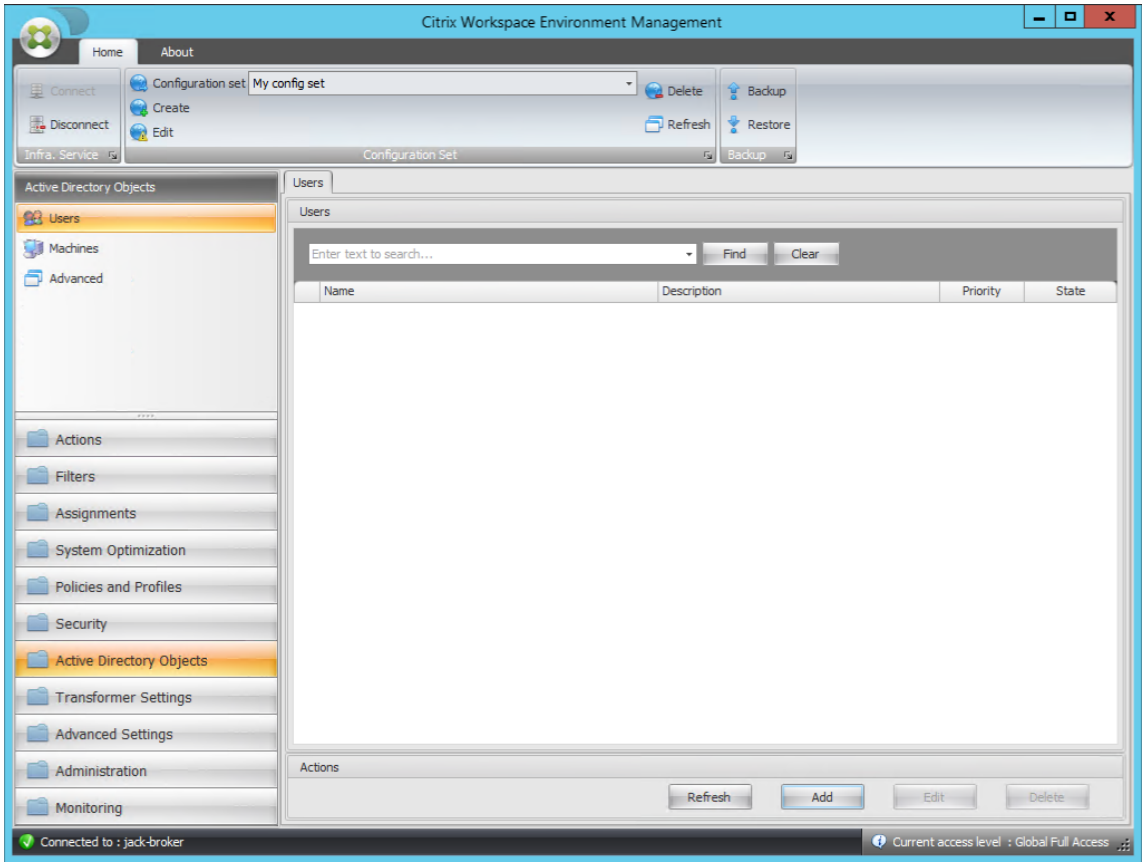


8. On the Ready to install page, click **Install**.

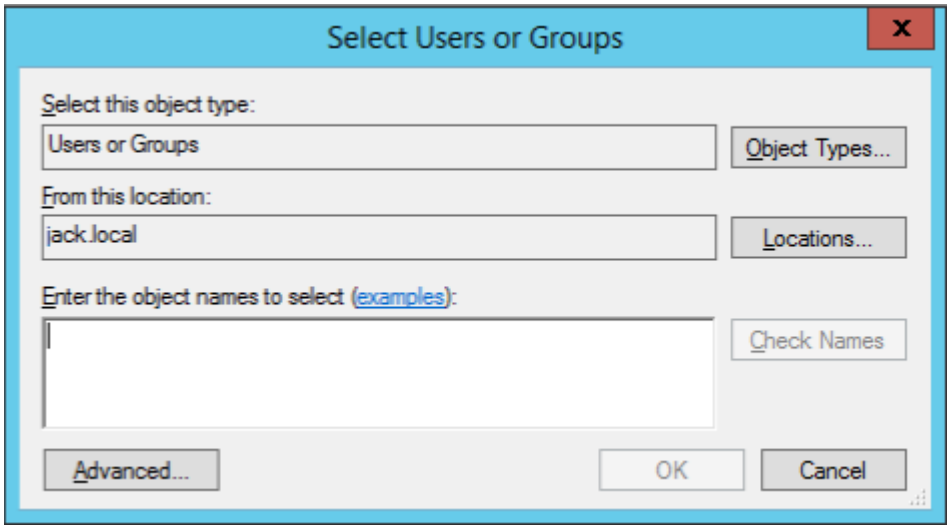
9. Click **Finish** to exit the installation wizard.

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

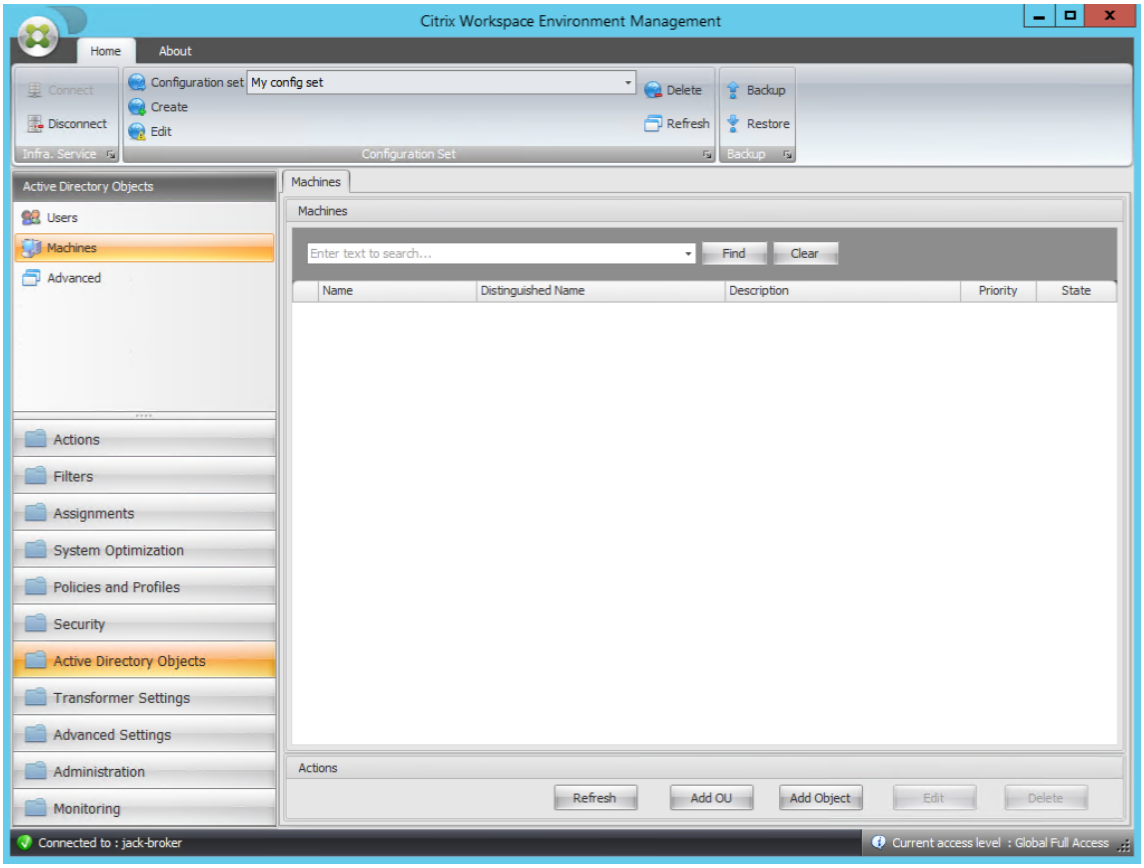
1. From the **Start** menu, open the **WEM Administration Console**, click **Active Directory Objects**, and then click **Add**.



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



3. Click **Machines**.



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

October 16, 2020

Software prerequisites

.NET Framework 4.7.1 or later. This component is necessary for the Workspace Environment Management agent. If not already installed, it is automatically installed during agent installation. However, we recommend that you install this prerequisite manually before you install the agent. Otherwise, you need to restart your machine to continue with the agent installation, and it might take a long time to complete.

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 2012 or later. Workspace Environment Management requires **sysadmin** access to a SQL Server instance to create its database, and **read/write** access to the database to use it. During the database creation, Workspace Environment Management creates a SQL login and then adds a database user mapping to the login. The user is *automatically* granted read/write access to the database. The SQL Server instance must use case-insensitive collation. Otherwise, database creation or upgrade fails.

> **Note:**
>
> In case of an upgrade, we recommend using a user account that has the **sysadmin** server role.

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

> **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

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

Infrastructure services

Supported operating systems:

- Windows Server 2012 R2 Standard and data center editions
- Windows Server 2016 Standard and data center editions
- Windows Server 2019 Standard and data center 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-bit and 64-bit
- Windows Server 2012 R2 Standard and data center editions
- Windows Server 2016 Standard and data center editions
- Windows Server 2019 Standard and data center editions

Agent

Supported operating systems:

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

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

In WEM 4.4, Windows XP was supported.

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

SQL Server Always On

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

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

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

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

    > **Note:**
    >
    > The WEM database is created on the primary SQL Server.

2. Go to your primary SQL Server and then back up the WEM database you created.
    - To select the WEM database on the **Add Database to Availability Group > Select Databases** page, you must type the password (the password you created in step 1). To do so, right-click the corresponding blank area in the Password column, type the password, and then click **Refresh**.
    - Select the **Full** recovery model for the database backup.
3. On the SQL Server, add the WEM database to the availability group and then configure the availability group listener.

4. Go to the WEM infrastructure service machine and then open the **WEM Infrastructure Service Configuration** utility.

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

Hardware prerequisites

Infrastructure services (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 Net Logon Dependencies list to ensure that the agent service is running before logons can be made.

Antivirus exclusions

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

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

On-access scanning must be disabled for the entire "Citrix" installation folder for the agent and the entire "Norskale" installation folder for the 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

- Citrix.Wem.Agent.Service.exe
- Citrix.Wem.Agent.LogonService.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

December 18, 2019

Install and configure the following components:

- Infrastructure services
- Administration console
- Agent

Infrastructure services

October 29, 2020

There is one Windows infrastructure service: **Norskale Infrastructure Service** (NT SERVICE\Norskale Infrastructure Service). It manages Workspace Environment Management (WEM) infrastructure services. Account: LocalSystem or specified user account that belongs to the administrator user group on the infrastructure server where the infrastructure service runs.

Install the infrastructure services

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

To Install the infrastructure services, run **Citrix Workspace Environment Management Infrastructure Services Setup.exe** on your infrastructure 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. By default, the infrastructure services install into the following folder: C:\Program Files (x86)\Norskale\Norskale Infrastructure Services. By default, the PowerShell SDK module installs into the following 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 opens. 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 opens. The default port is 8285. Any valid port is an accepted value.

AdminPort: The infrastructure services setup 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 opens. 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 a service principal name

> **Important:**
>
> - Do not create multiple service principal names (SPNs) for separate domains that reside in the same forest. All the infrastructure services in an environment must be run using the same service account.
> - When you use **load balancing**, all instances of the infrastructure services must be installed and configured using the same service account name.
> - **Windows authentication** is a specific method of authentication for SQL instances that use AD. The other option is to use a SQL account instead.

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

- If you do not use Windows authentication or load balancing, use the following command:
  - **setspn -C -S Norskale/BrokerService [*hostname*]**

  where [*hostname*] is the name of the infrastructure server.
- If you use Windows authentication or load balancing (requiring 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.

Group Managed Service Account

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

1. On your domain controller, create a gMSA. For more information about creating a gMSA, see https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-

accounts/getting-started-with-group-managed-service-accounts.

2. Bind the Citrix WEM SPN with the account. For information about the WEM SPN, see Create a service principal name.
3. Configure SQL Server settings to enable the account to access the database.
    a) On your primary SQL Server, navigate to **Security > Logins**, right-click **Logins**, and then select **New Login**.
    b) In the **Login - New window**, click **Search**.
    c) In the **Select User or Group** window, configure settings as follows and click **OK** to exit the window.
        - **Object Types**. Select only **Service Accounts**.
        - **Locations**. Select **Managed Service Accounts**.
        - Object name. Type the account name that you created in Step 1.
    d) On the **User Mapping** page, select the database to which you want to apply gMSA and then select **db-owner** as the role membership for the database.
    e) On the **Status** page, verify that the **Grant** and **Enabled** options are selected.
    f) Click **OK** to exit the **Login - New** window.
4. Use the service account you added to start the Norskale Infrastructure Service.
    a) On your infrastructure server, open the Windows Services manager, right-click the Norskale Infrastructure Service, and then select **Properties**.
    b) On the **Log On** page, select **This account**, click **Browse**, and configure settings as described in the third substep of Step 3.
    c) Click **OK** to exit the **Norskale Infrastructure Service Properties** window.
    d) In the Windows Services manager, restart the Norskale Infrastructure Service.

Configure load balancing

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

To configure WEM with a load balancing service:

1. Create a Windows infrastructure service account for the WEM infrastructure service to connect to the WEM database.
2. When you create the WEM database, select the **Use Windows authentication for infrastructure service database connection** option and specify the infrastructure service account name. For more information, see Create a Workspace Environment Management database.

3. Configure each infrastructure service to connect to the SQL database using Windows authentication instead of SQL authentication: select the **Enable Windows account impersonation** option and provide the infrastructure service account credentials. For more information, see Configure the Infrastructure Service.
4. Configure the SPNs for the WEM infrastructure services to use the infrastructure service account name. For more information, see Create a service principal name.

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

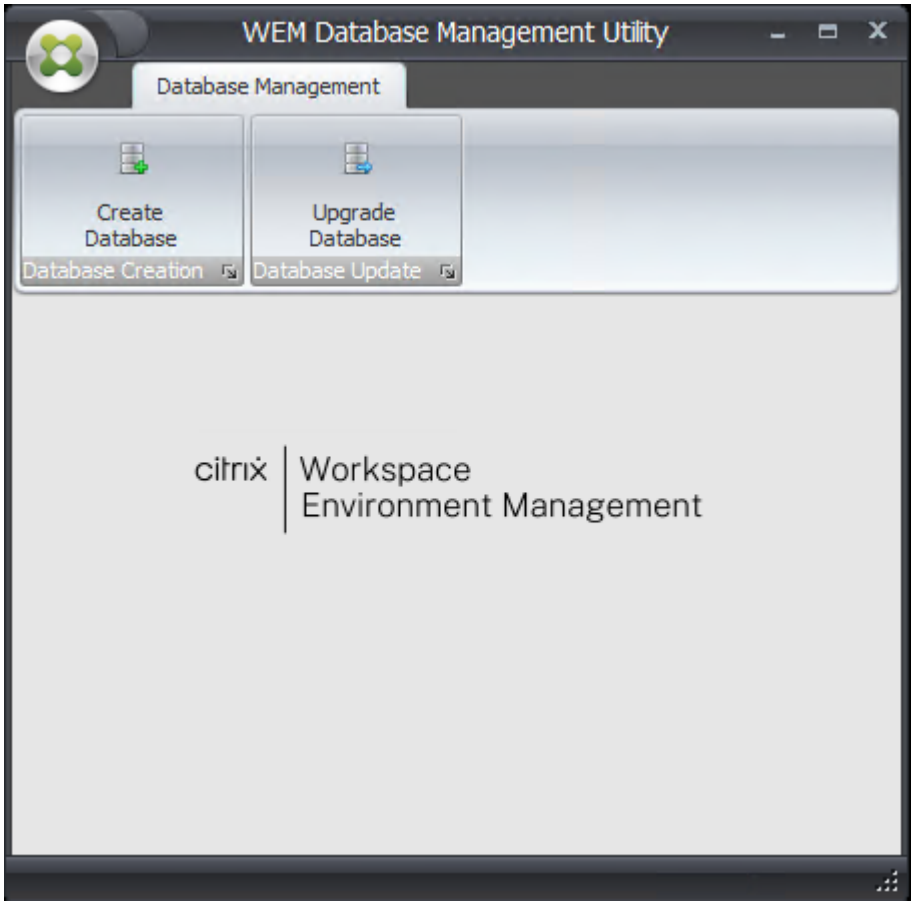
5. Create a virtual IP address (VIP) that covers the number of infrastructure servers you want to put behind a VIP. All the infrastructure servers covered by a VIP are eligible when agents connect to the VIP.
6. When you configure the Agent Host Configuration GPO, set the infrastructure server setting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

Create a Workspace Environment Management database

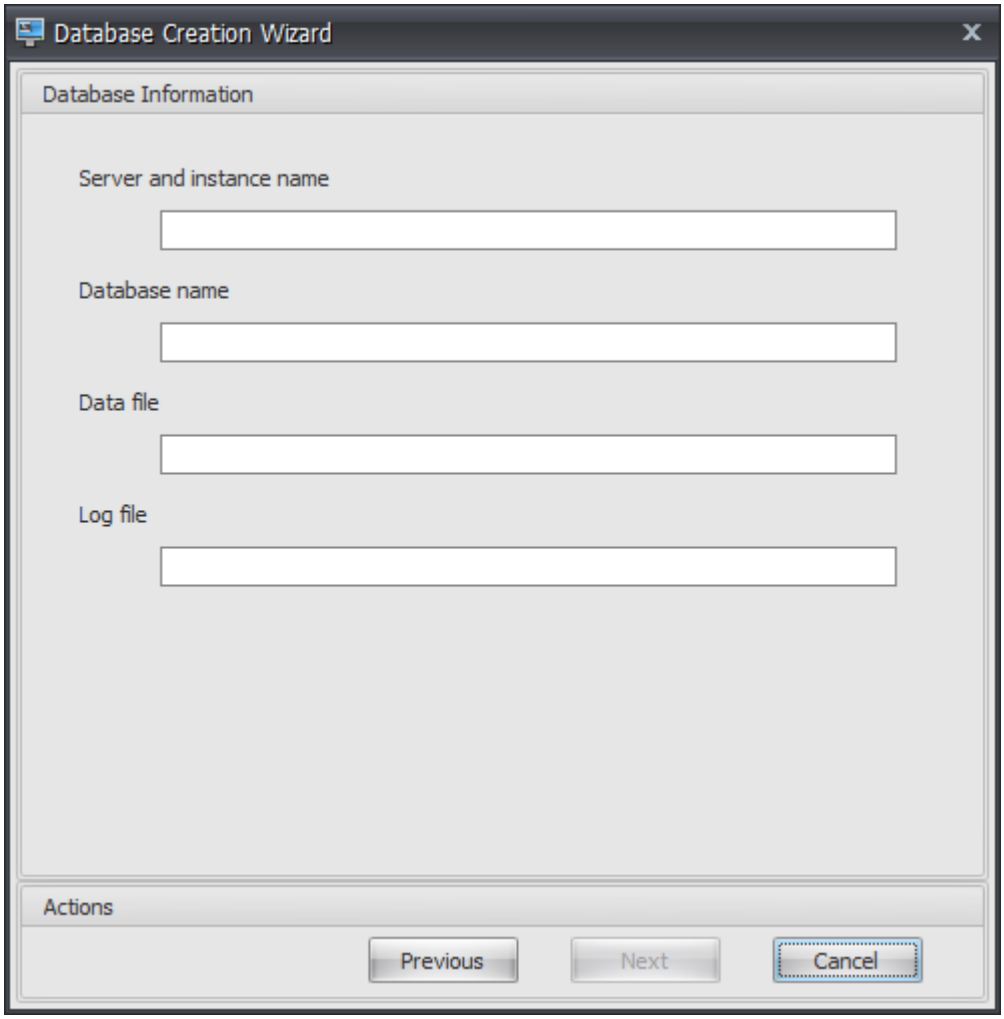
> **Tip:**
>
> You can also create the database using the WEM PowerShell SDK module. For SDK documentation, see Citrix Developer Documentation.
>
> **Note:**
>
> - If you are using Windows authentication for your SQL Server, run the database creation utility under an identity that has sysadmin permissions.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

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

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



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



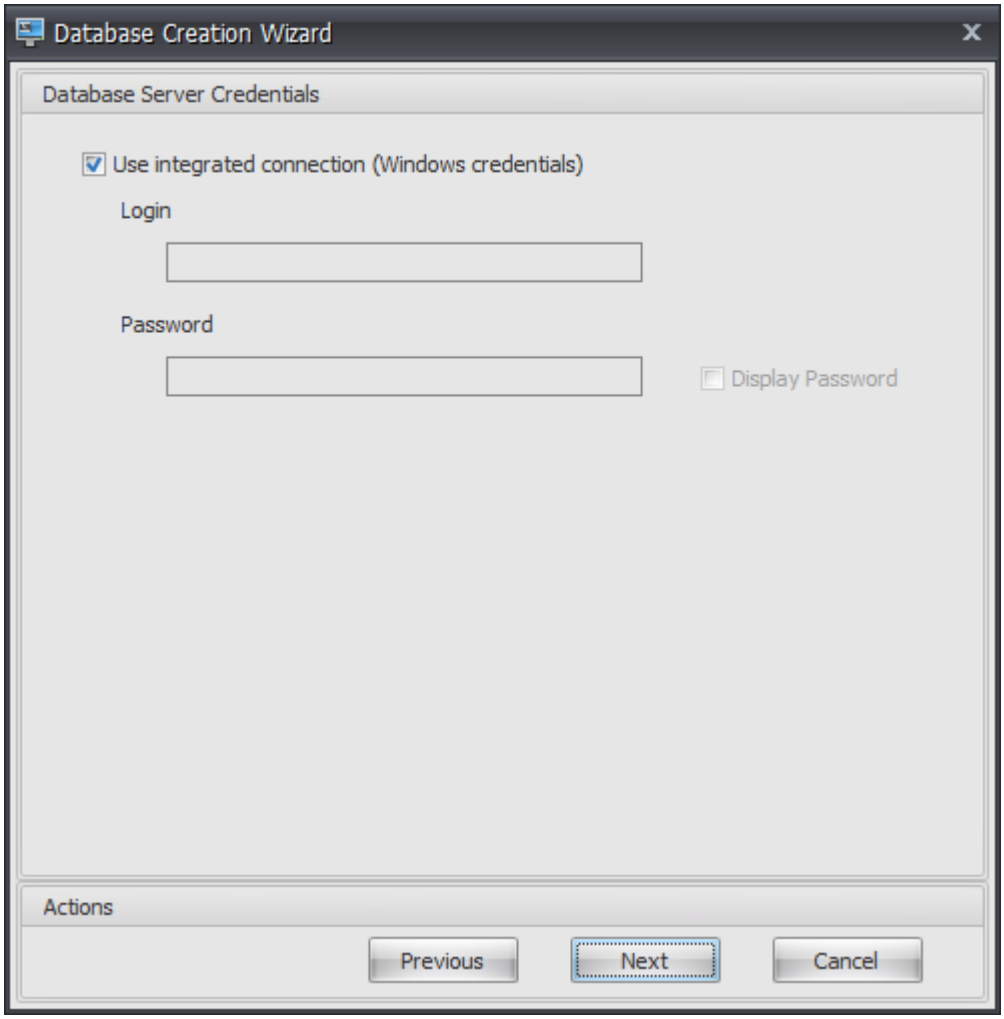
3. Type the following Database Information, then click **Next**:

   - **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.

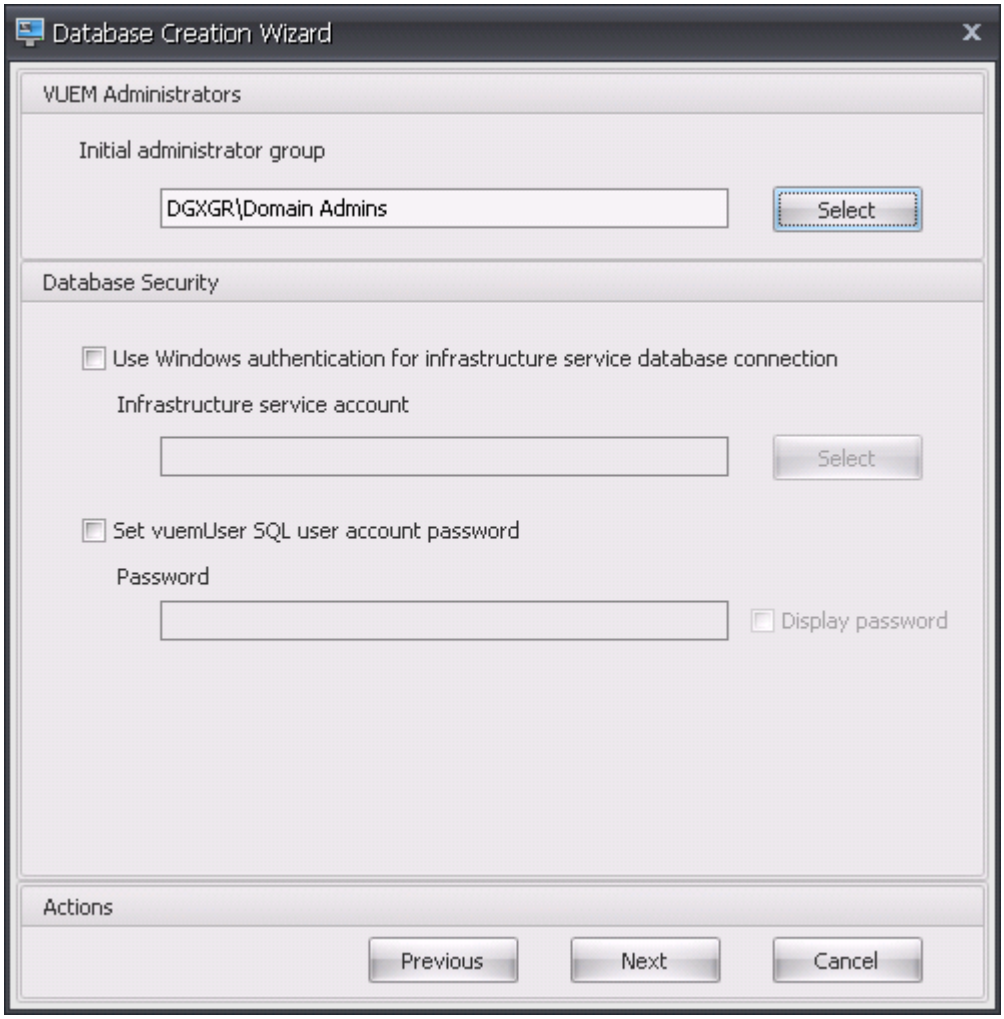
   - **Data file**: path to the **.mdf** file location on the SQL Server.
   - **Log file**: path to the **.ldf** file location on the SQL Server.

> **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.



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.



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.

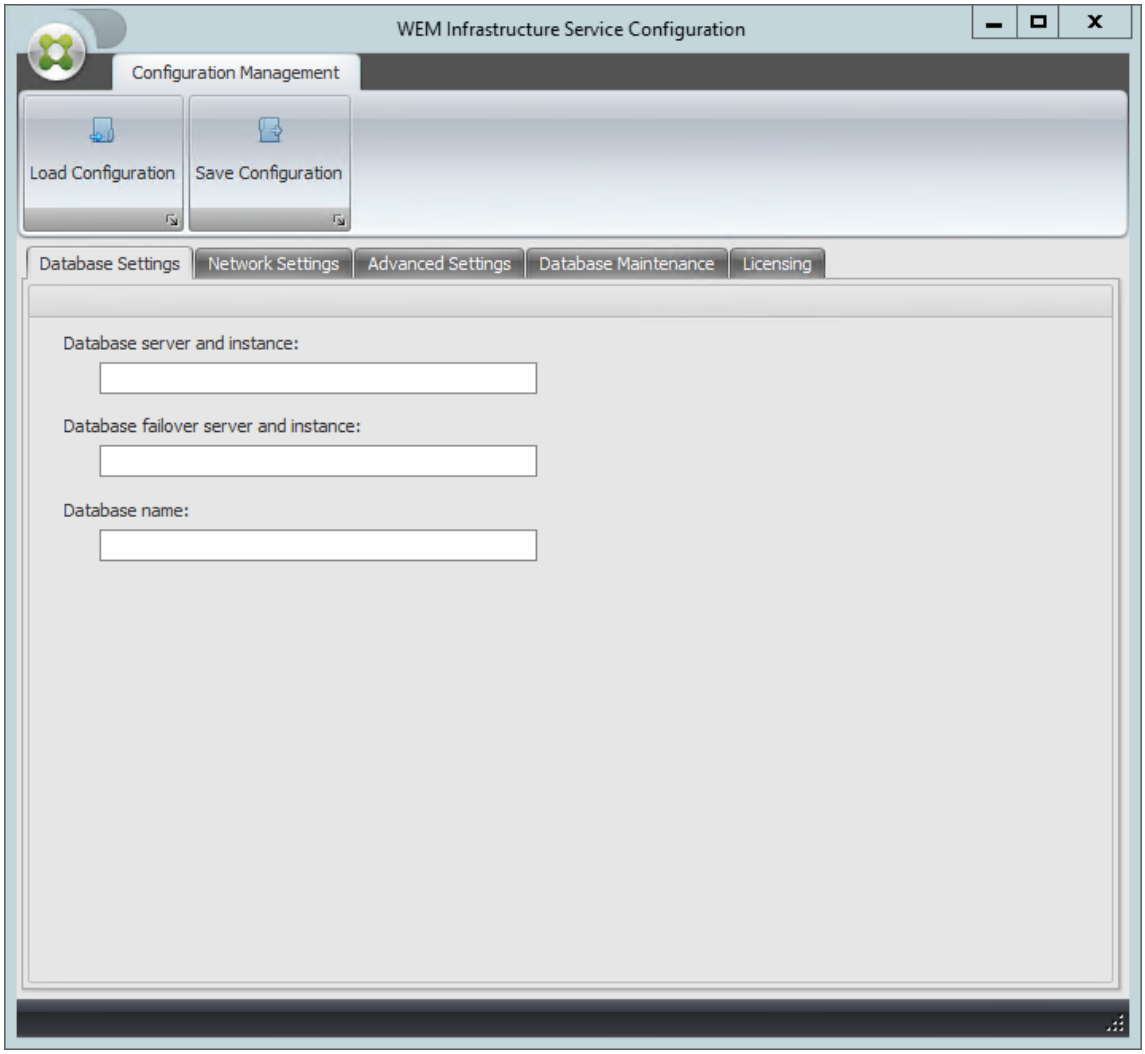
   If an error occurs during the database creation, check the log file "Citrix WEM Database Management Utility Debug Log.log" in the infrastructure services installation directory.

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.

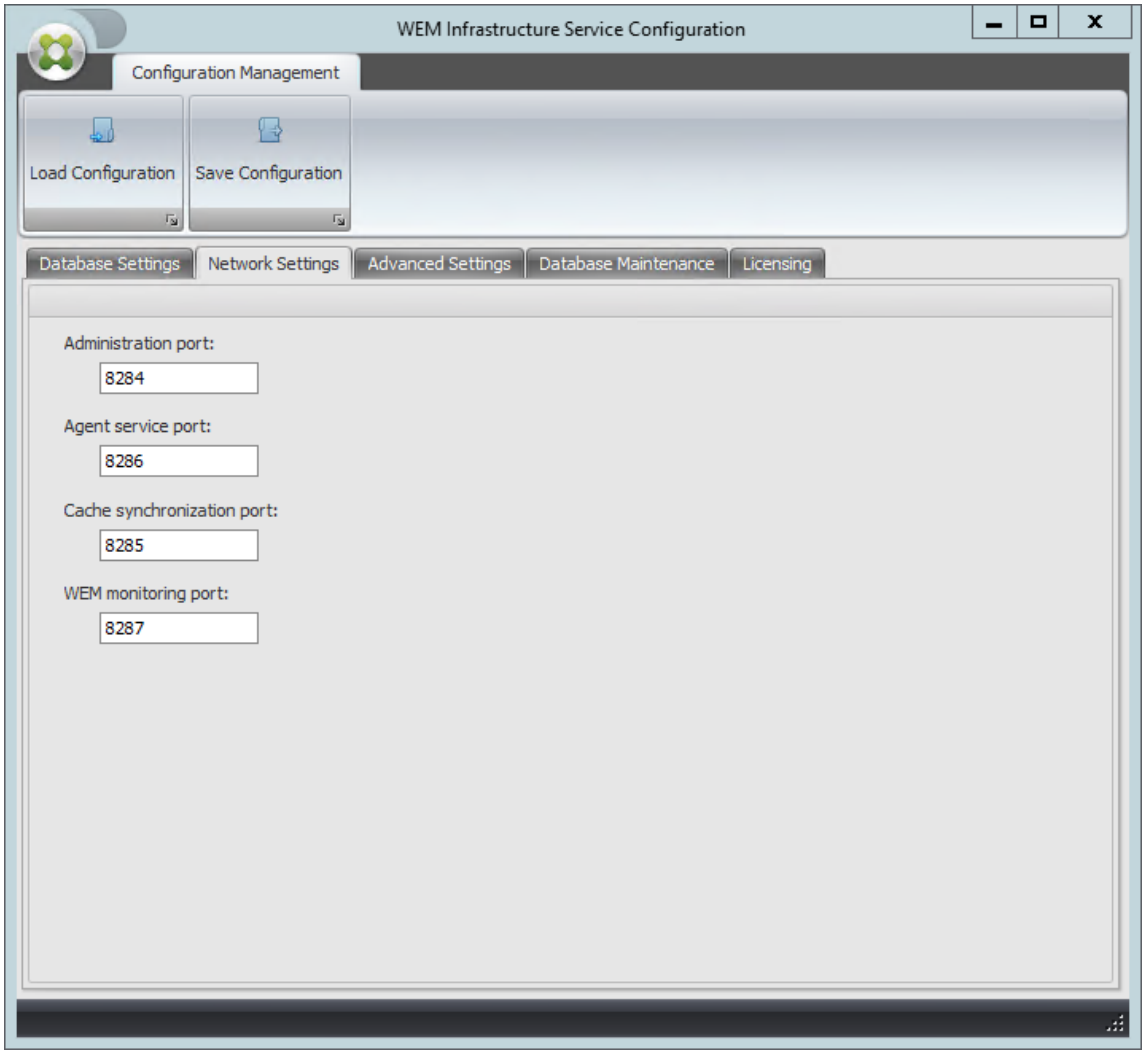
Before the infrastructure service runs, you must configure it using the **WEM Infrastructure Service Configuration** utility, as described here.

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

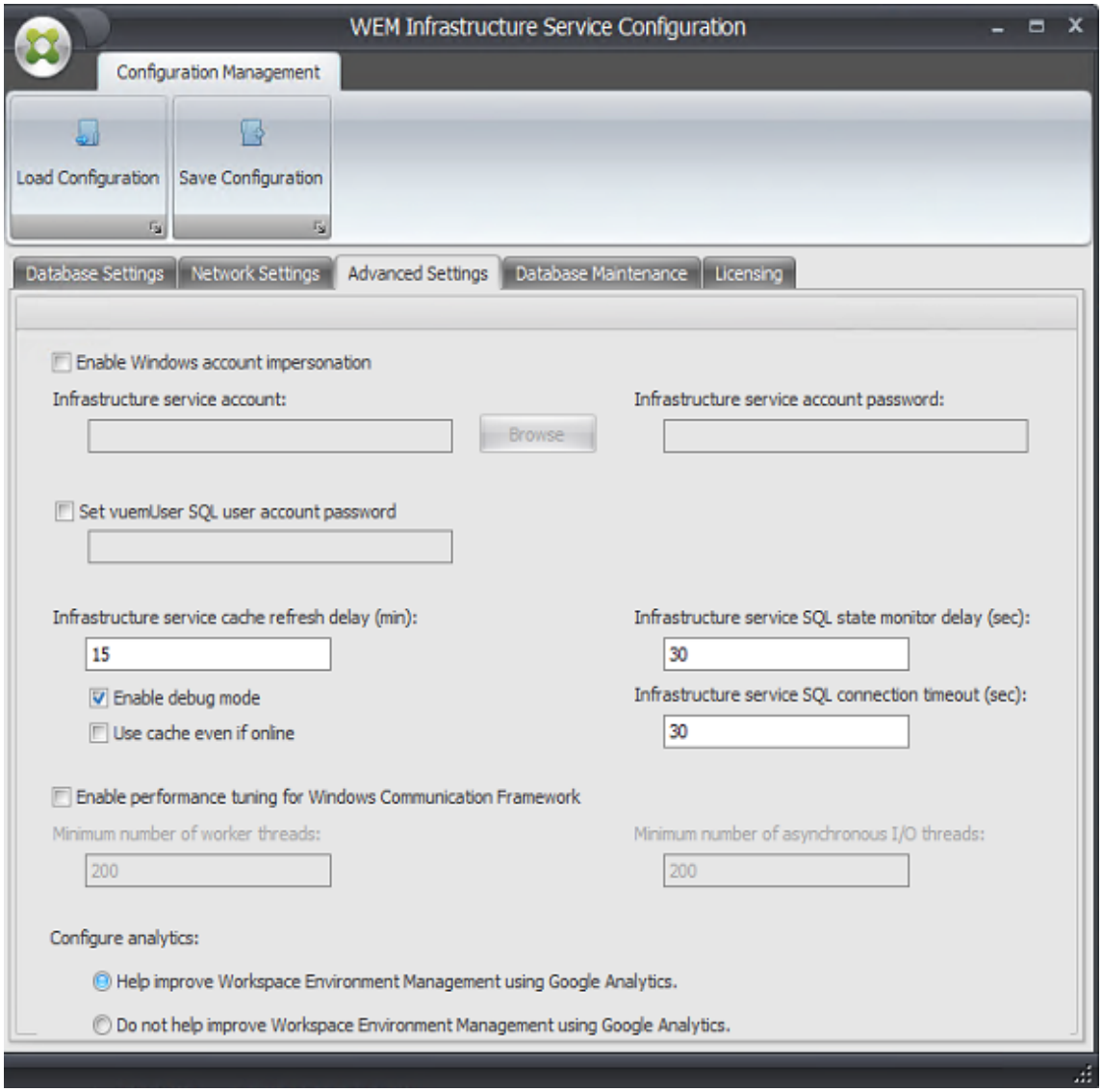


2. In the **Database Settings** tab enter the following details:

   - **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.



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.]



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

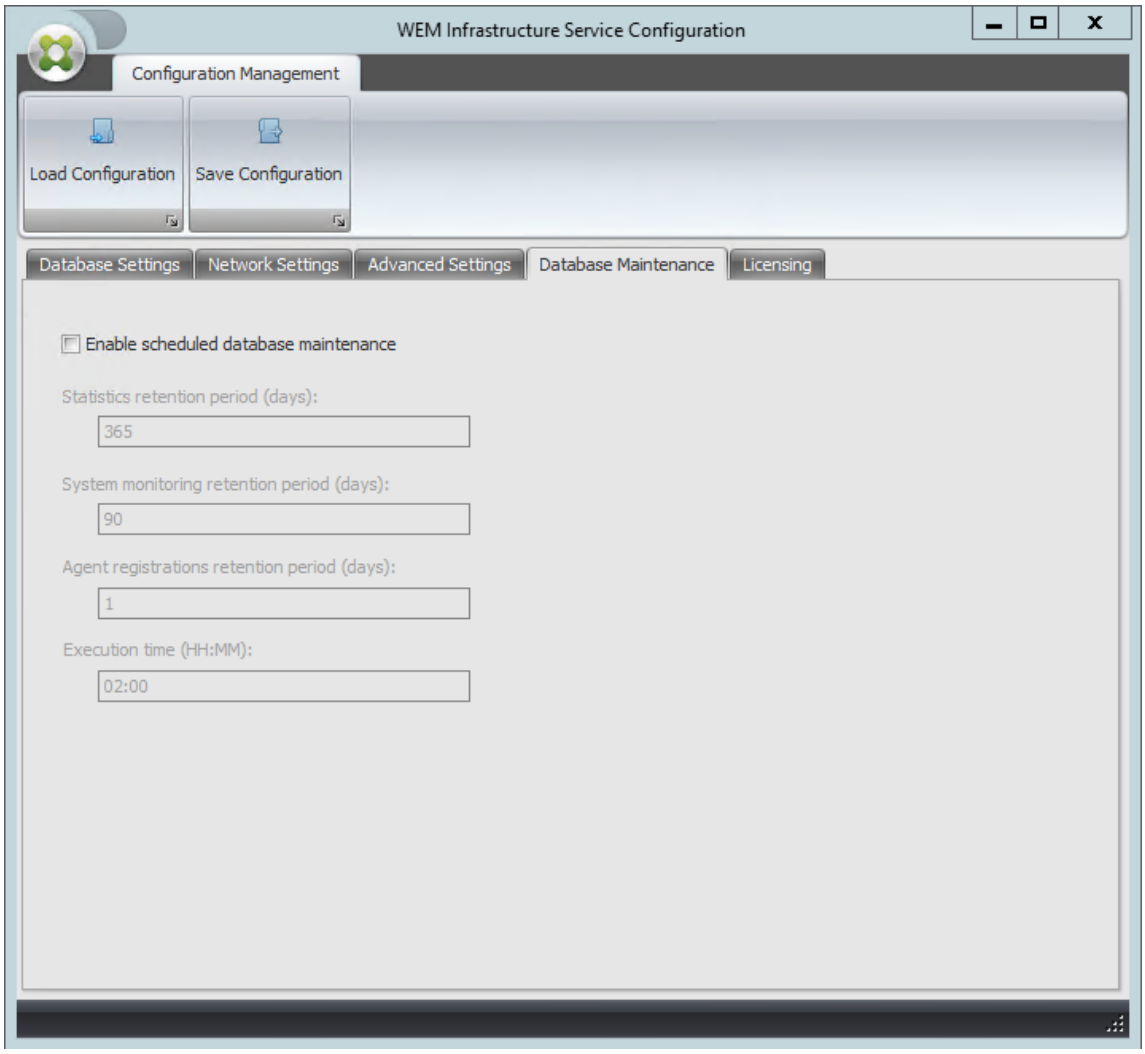
service refreshes its cache. The cache is used if the infrastructure service is unable to connect to SQL.

- **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.
- **Enable performance tuning**. Lets you optimize the performance in scenarios where the number of connected agents exceeds a certain threshold (by default, 200). As a result, it takes shorter time for the agent or the administration console to connect to the infrastructure service.
  - **Minimum number of worker threads**. Specifies the minimum number of worker threads that the thread pool creates on demand. Set the number of worker threads in the range of 30-3000. Determine the value based on the number of connected agents. By default, the minimum number of worker threads is 200.
  - **Minimum number of asynchronous I/O threads**. Specifies the minimum number of asynchronous I/O threads that the thread pool creates on demand. Set the number of asynchronous I/O threads in the range of 30-3000. Determine the value based on the number of connected agents. By default, the minimum number of asynchronous I/O threads is 200.

> **Important:**
>
> This feature is especially useful when the agent or the administration console intermittently disconnects from the infrastructure service.
>
> **Note:**
>
> The values you set in the Enable performance tuning fields are used when new requests are made and before switching to an algorithm for managing thread creation and destruction. For more information, see https://docs.microsoft.com/en-us/dotnet/api/system.threading.threadpool.setminthreads?view=netframework-4.8 and https://support.microsoft.com/en-sg/help/2538826/wcf-service-may-scale-up-slowly-under-load.

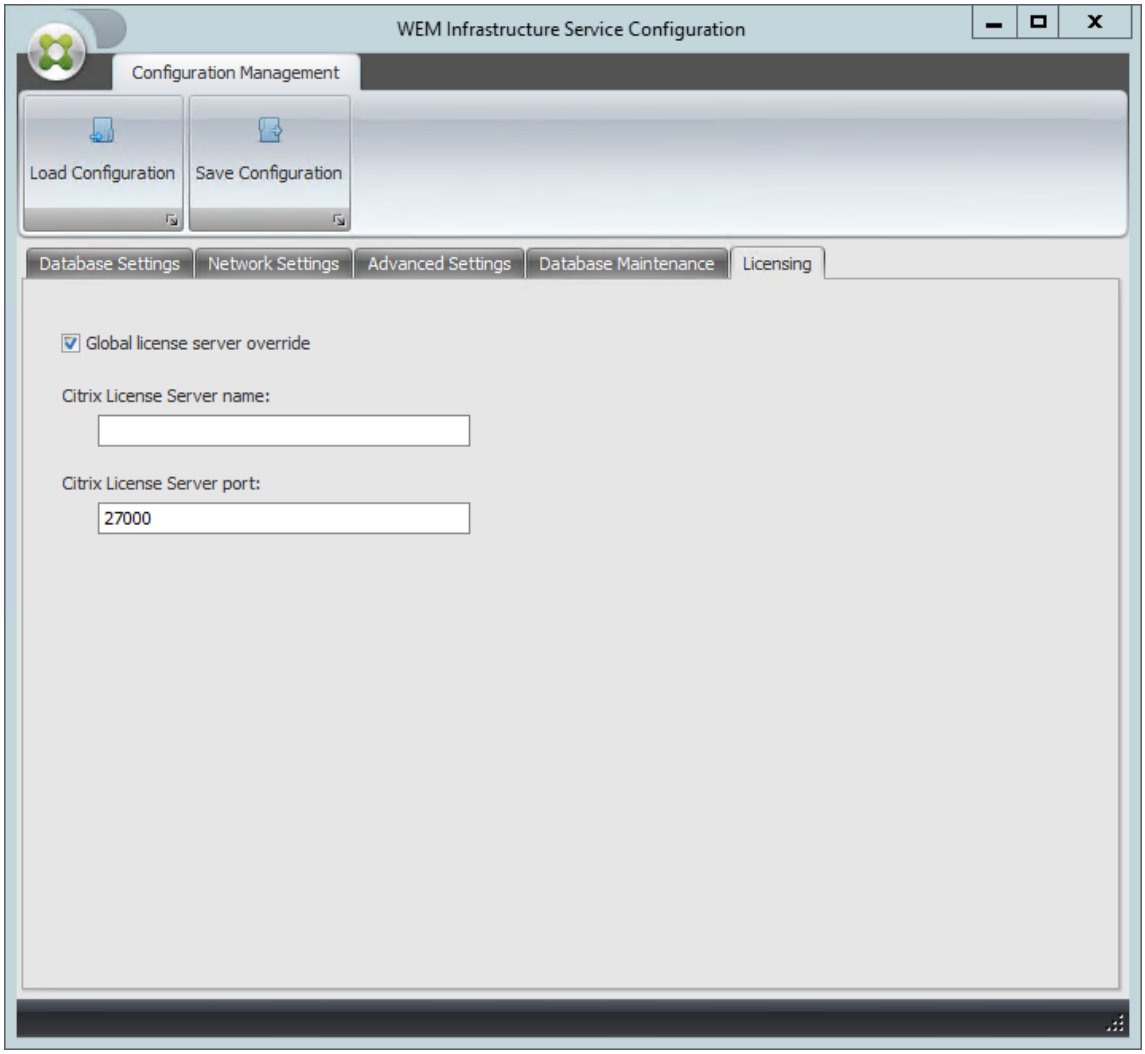
- **Help improve Workspace Environment Management using Google Analytics**. If selected, the infrastructure service sends anonymous analytics to the Google Analytics server.

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



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 per-

formed. Default is 02:00.



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

    - **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

July 8, 2020

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:

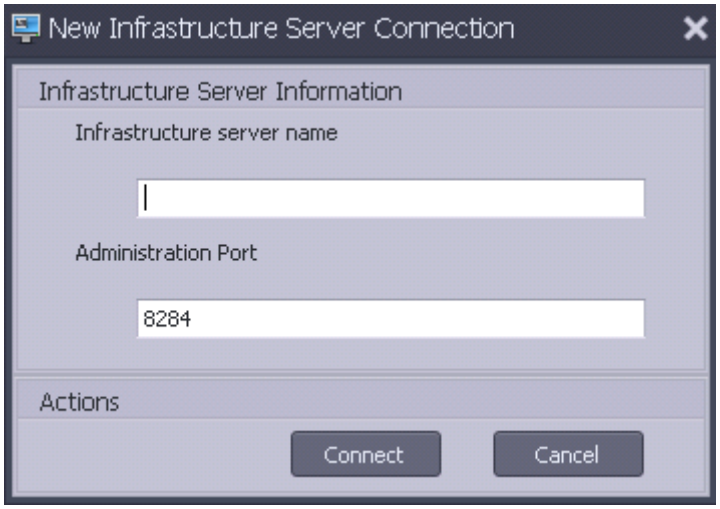
```
”path:\\to\\Citrix Workspace Environment Management Console Setup.exe ”/v”
argument=\\”value\\””
```

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.

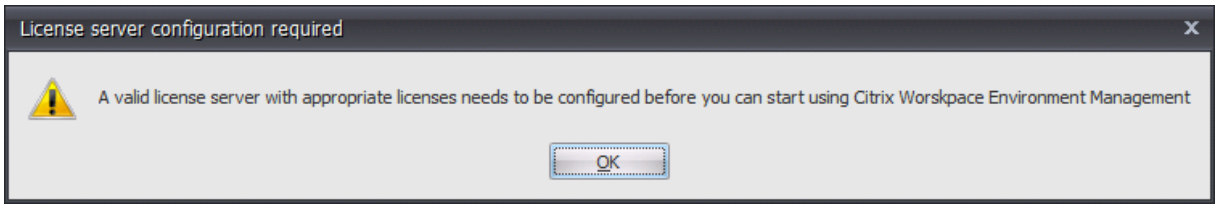


Enter the following values then click **Connect**:

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.

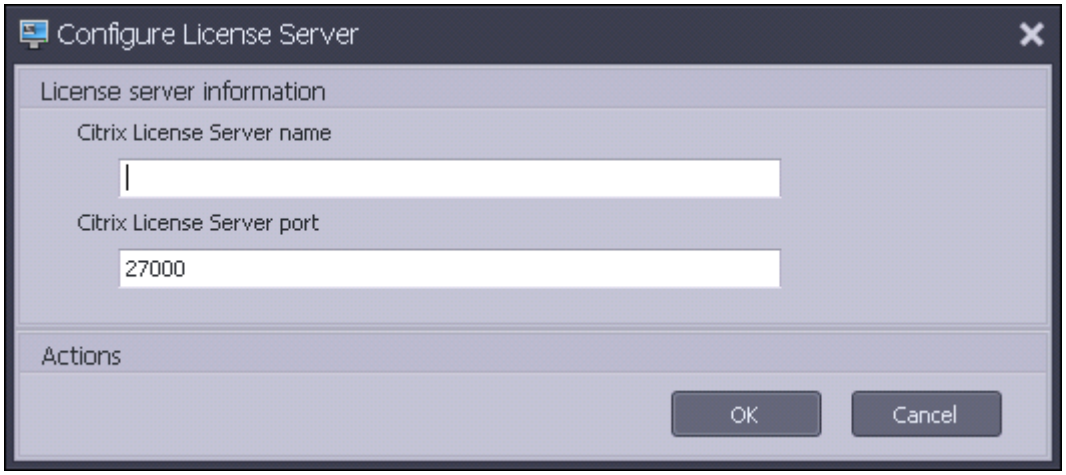
Administration port. The port on which the administration console connects to the infrastructure service.

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



Configure the database with a license server

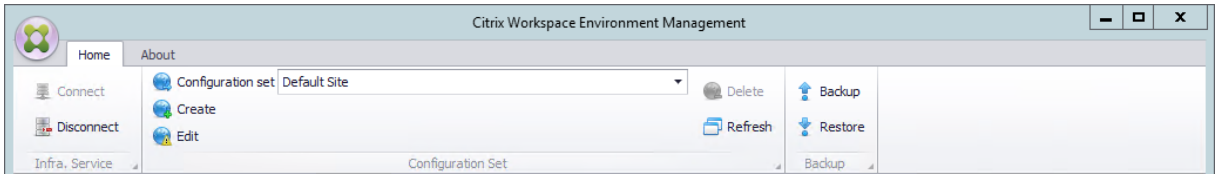
To configure the database with a license server, in the administration console ribbon, click **About** then click **Configure License Server** and enter your Citrix License Server details. The Citrix License Server address must resolve from the administration console environment exactly as entered.



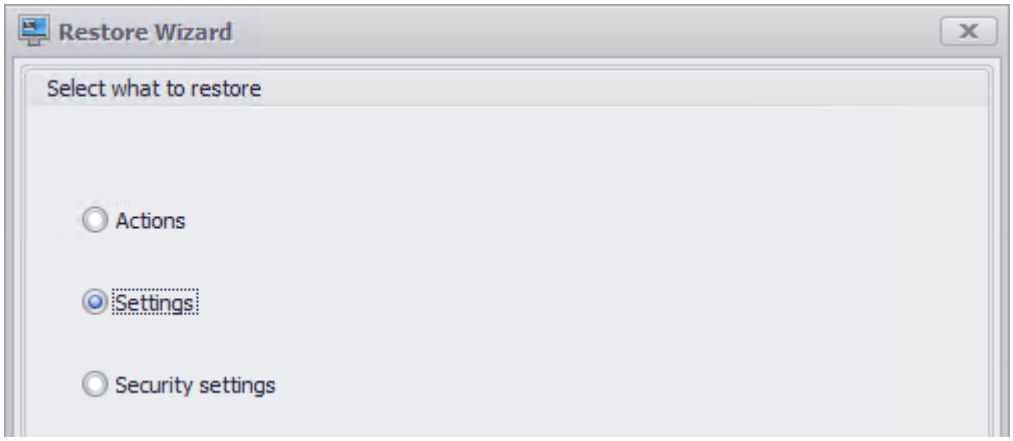
Import quickstart settings

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**.



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

Agent

October 29, 2020

Install and configure the agent

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

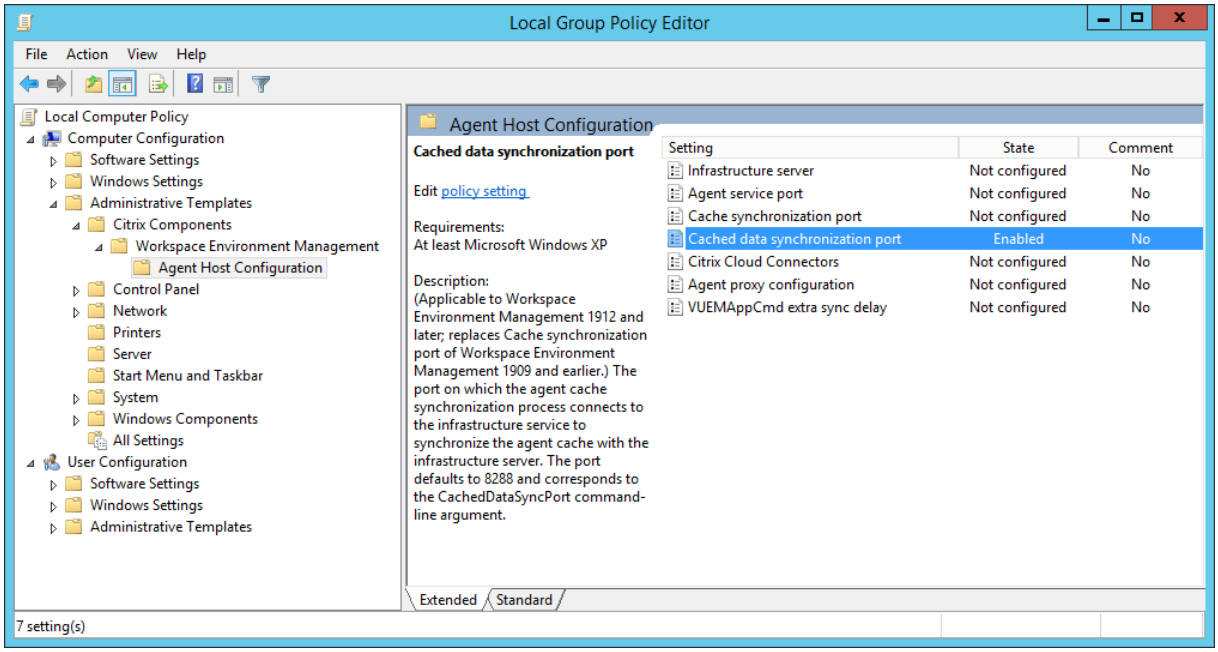
Step 1: Configure group policies (optional)

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

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

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

Use the **Group Policy Management Editor** to configure a GPO with the following settings:



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

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

Cache synchronization port. (Applicable to Workspace Environment Management 1909 and earlier; replaced by *Cached data synchronization port* in Workspace Environment Management 1912 and later.) The port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server. The cache synchronization port must be the same as the port you configured for the cache synchronization port (**WEM Infrastructure Service Configuration > Network Settings**) during the infrastructure services configuration. The port defaults to 8285 and corresponds to the `AgentCacheSyncPort` command-line argument.

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

- `citrix_wem_agent_bundle.exe /quiet CachedDataSyncPort=9000`

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

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

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

Step 2: Install the agent

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

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

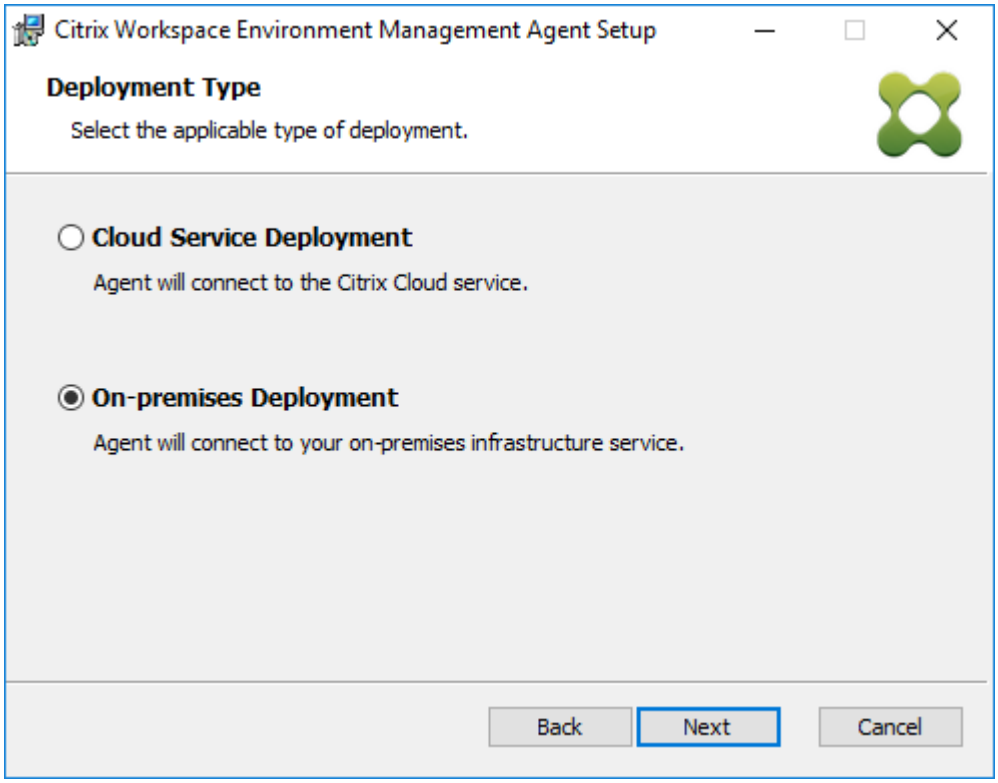
- C:\Program Files (x86)\Citrix\Workspace Environment Management Agent (on 64-bit OS)
- C:\Program Files\ Citrix\Workspace Environment Management Agent (on 32-bit OS)

To install the agent interactively, complete these steps:

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

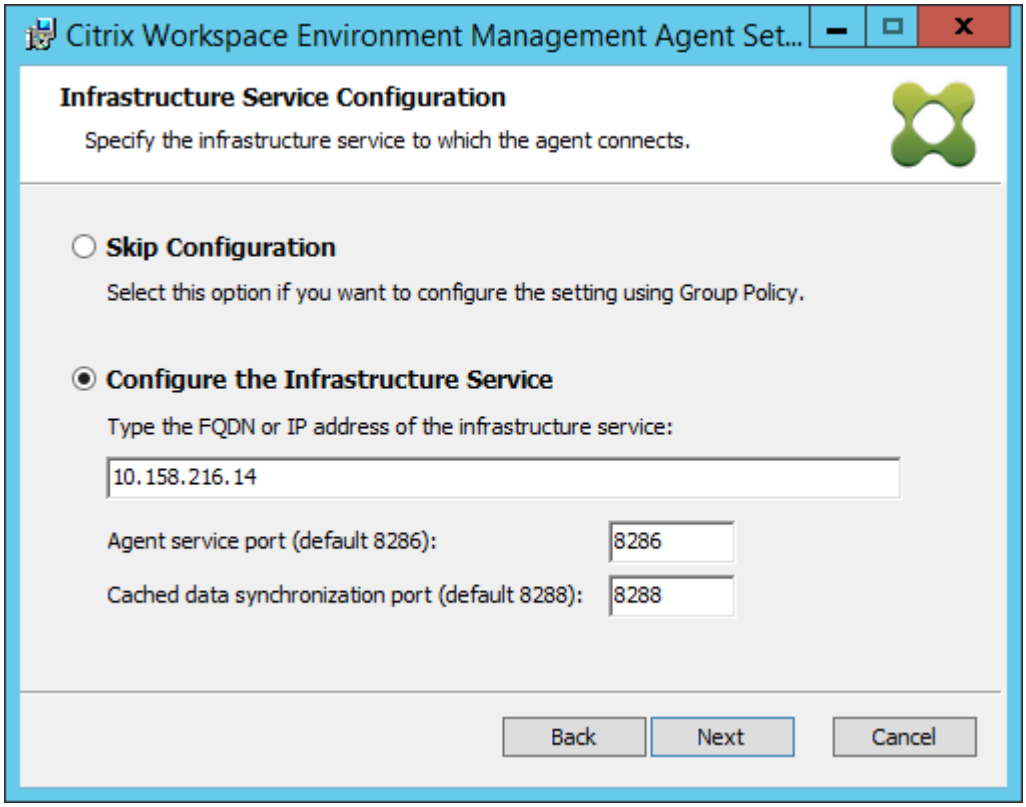
   > **Note:**
   >
   > The Welcome page can take some time to appear. This delay happens when the required software is missing and is being installed in the background.

4. On the Destination Folder page, click **Next**.
   - By default, the destination folder field is automatically populated with the default folder path. If you want to install the agent to another folder, click **Change** to navigate to the folder and then click **Next**.
   - If you already installed the WEM agent, the destination folder field automatically populates with the existing installation folder path.
5. On the Deployment Type page, select the applicable type of deployment and then click **Next**. In this case, select **On-premises Deployment**.



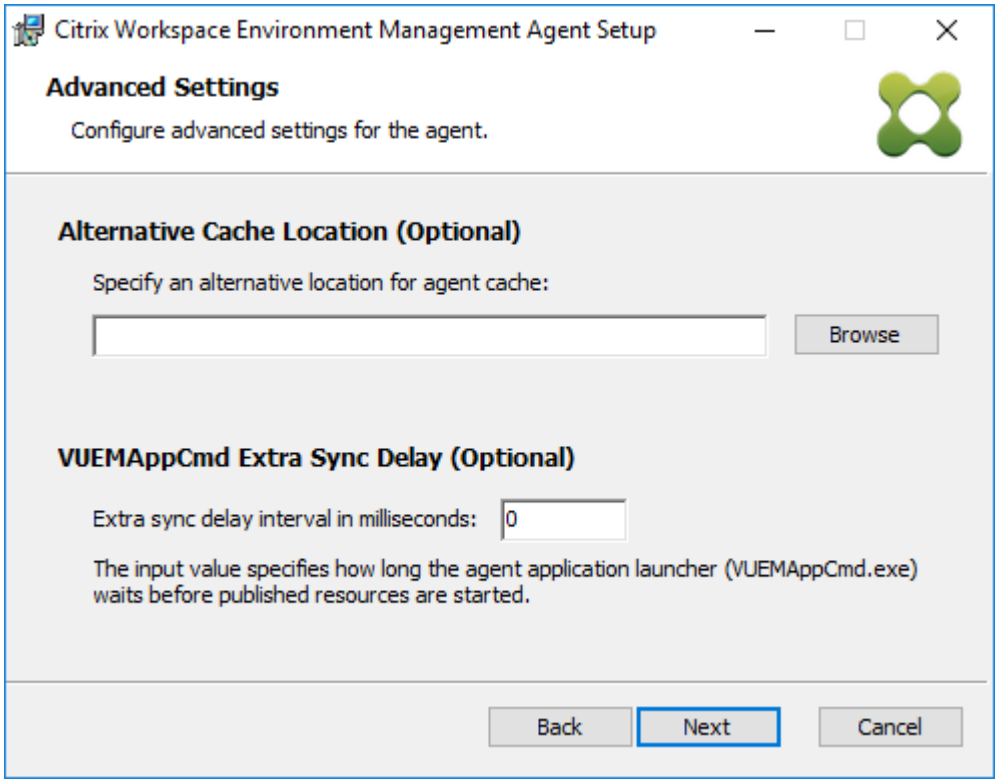
6. On the Infrastructure Service Configuration page, specify the infrastructure service to which the agent connects and then click **Next**.

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



7. On the Advanced Settings page, configure advanced settings for the agent and then click **Next**.
   - **Alternative Cache Location (Optional)**. Lets you specify an alternative location for the agent cache. Click Browse to navigate to the applicable folder.
   - **VUEMAppCmd Extra Sync Delay (Optional)**. Lets you specify how long the agent application launcher (VUEMAppCmd.exe) waits before published resources start. Setting this delay ensures that the necessary agent work completes first. The default value is 0.

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



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

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

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

> **Tip:**
>
> You might want to consult the log files to troubleshoot the agent installation. By default, log files recording all actions that occur during installation are created in %TEMP%. You can use the `/log log.txt` command to designate a specific location for the log files to be saved.

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

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

Step 3: Build the agent service cache (optional)

By default, the agent service cache is built the first time the agent runs. You can choose to build the agent service cache before the agent runs. Doing so is useful if you want to build an image that in-

cludes the WEM agent host as pre-installed software.

To build or rebuild the agent service cache, run *AgentCacheUtility.exe* in the agent installation folder using the command line. The executable accepts these command-line arguments:

- **-help**: displays a list of allowed arguments
- **-refreshcache** or **-r**: triggers a cache build or refresh

Step 4: Restart the machine to complete the installation

Good to know

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

Agent settings

The WEM agent settings include:

- **AgentLocation**. Lets you specify the agent installation location. Specify a valid folder path.
- **AgentCacheLocation**. Lets you specify an alternative location for the agent cache. If configured, the agent local cache file is saved in the designated location instead of in the agent installation folder.
- **AgentCacheSyncPort**. Lets you specify the port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server.
- **AgentServicePort**. Lets you specify the port on which the agent connects to the infrastructure server.
- **InfrastructureServer**. Lets you specify the FQDN or IP address of the infrastructure server where the infrastructure service is running.
- **VUEMAppCmdDelay**. Lets you specify how long the agent application launcher (VUEMAppCmd.exe) waits before the Citrix Virtual Apps and Desktops published resources start. The default value is 0 (milliseconds). The value you type for the extra sync delay interval must be an integer greater than or equal to zero.

Be aware of the following:

- If you configure the settings through the command line, the WEM agent installer uses the configured settings.
- If you don't configure the settings through the command line and there are previously configured settings, the installer uses the settings that were previously configured.

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

System settings

The system settings associated with the agent host machine include:

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

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

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

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

- **ServicesPipeTimeout**. Lets you configure the value of the ServicesPipeTimeout registry key. The key is created during installation under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control**. This registry key adds a delay before the service control manager is allowed to report on the

state of the WEM agent service. The delay prevents the agent from failing by keeping the agent service from launching before the network is initialized. This argument accepts any value, in milliseconds. If not specified, a default value of 60000 (60 seconds) is used.

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

Examples

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

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

For example:

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

Upgrade a deployment

June 18, 2020

Introduction

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

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

From	To	In-place upgrade supported
4.6 and earlier	4.7	Yes
4.6 and earlier	1808 or later	No (upgrade to version 4.7 before upgrading to the target version)

From	To	In-place upgrade supported
4.7	1808 or later	Yes

> **Tip:**
>
> The WEM database, infrastructure service, and administration console must all be of the same version.

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.

Upgrade the operating system of an infrastructure server

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

Step 2: Upgrade the database

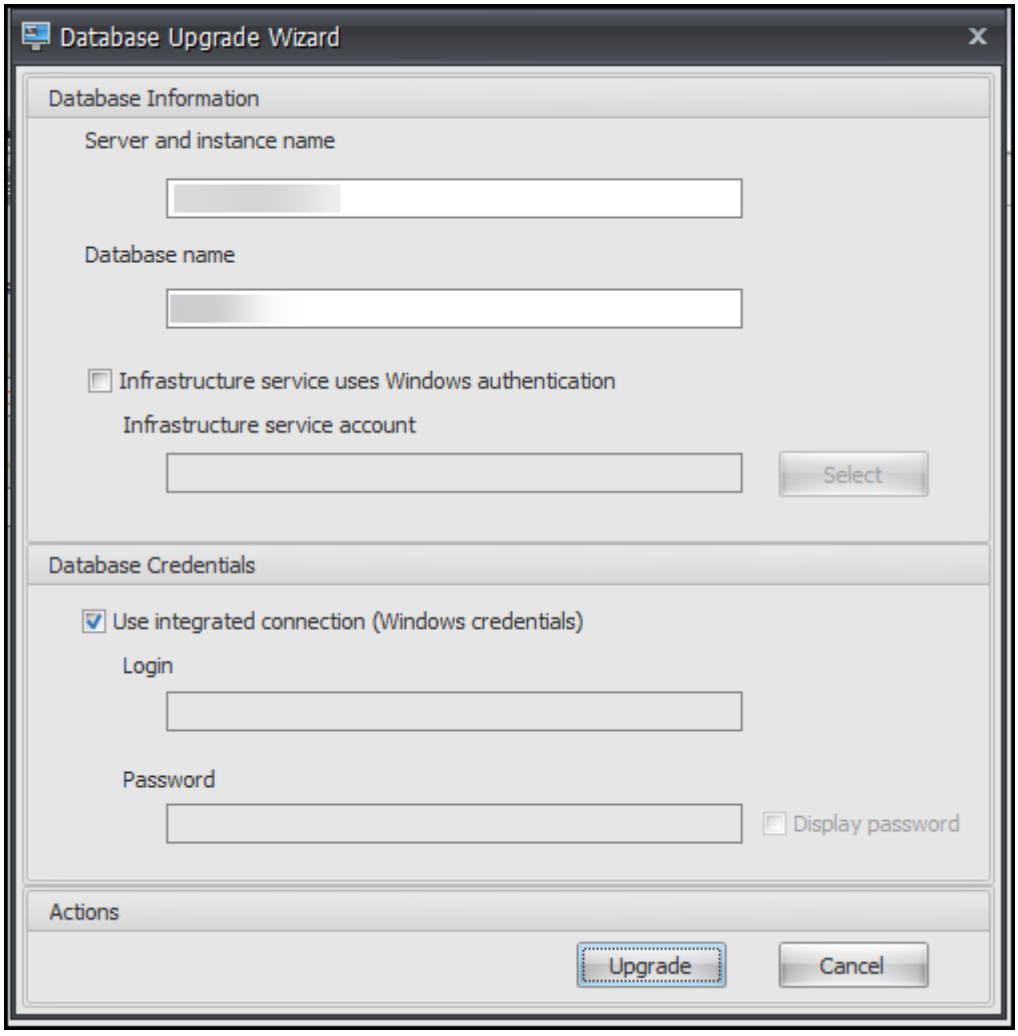
> **Important:**
>
> The database upgrade process is not reversible. Ensure that you have a valid database backup before launching the upgrade process.
>
> **Tip:**
>
> You can also upgrade the database using the Workspace Environment Management PowerShell

> SDK module. For SDK documentation, see Citrix Developer Documentation.

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

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

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



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

- **Database name**. Name of the database to be upgraded.
- **Infrastructure service uses Windows authentication**. By default, this option is not selected. In this case, the infrastructure service connects to the database using the vuemUser SQL user account. (The vuemUser SQL user account is created during the installation process.) Verify that Mixed-Mode Authentication is enabled for the SQL instance.

  When selected, the infrastructure service connects to the database using a Windows account. In this case, the Windows account you select must not already have a login on the SQL instance. In other words, do not use the same Windows account that you used to create the database to run the infrastructure service.
- **Use integrated connection**. By default, this option is selected. The option lets the wizard use the Windows account of the identity under which the wizard is running to connect to SQL Server and to create the database. If this Windows account does not have sufficient permissions to create the database, run the database management utility as a Windows account with sufficient privileges, or clear this option and type a SQL account with sufficient privileges instead.

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

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

Step 3: 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.
> - The version of the WEM infrastructure service must be equal to or greater than the version of the WEM agent. Citrix recommends that you upgrade the agent to the latest version so that you can use the most recent features.

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

User experience

May 12, 2020

Start the administration console

1. From the **Start** menu select **Citrix > Workspace Environment Management > WEM Administration Console**. By default, the administration console launches in a disconnected state.
2. On the administration console ribbon click **Connect**.
3. In the New Infrastructure Server Connection window, type the address of your infrastructure server and click **Connect**.

Configure your installation

In the administration console:

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

Ribbon

May 4, 2020

Home tab

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

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

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

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

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

Create. Opens the Create configuration set window. Allows you to configure multiple WEM sites (configuration sets).

- **Name**. Site (configuration set) name as it appears in the configuration set list in the Ribbon.
- **Description**. Site (configuration set) description as it appears in the site edition window.
- **Site State**. Toggles whether the site (configuration set) is Enabled or Disabled. When Disabled, the WEM Agents cannot connect to the site (configuration set).

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

Delete. Deletes the site (configuration set). You cannot delete "Default site" because it is required for WEM to function. You can, however, rename it.

Refresh. Refreshes the site (configuration set) list.

> **Note:**
>
> The list does not automatically refresh when sites are created from different administration consoles.

Backup. Opens the **Backup** wizard to save a backup copy of your current configuration to the WEM administration console machine. You can back up actions, settings, security settings, and Active Directory (AD) objects.

- **Actions**. Backs up selected WEM actions. Each type of action is exported as a separate XML file.
- **Settings**. Backs up selected WEM settings. Each type of setting is exported as a separate XML file.
- **Security Settings**. Backs up all settings present on the Security tab. Each type of rule is exported as a separate XML file.
- **AD objects**. Backs up the users, computers, groups, and organizational units that WEM manages. The **Backup** wizard lets you specify which type of AD objects to back up. There are two types of AD objects:
  - Users. Single users and user groups
  - Machines. Single machines, machine groups, and OUs
- **Configuration set**. Backs up the WEM configuration set you selected. Each type of configuration set is exported as a separate XML file. You can back up only the current configuration set. You can back up the following items associated with a configuration set:
  - Actions
  - AppLockers

  - Assignments (related to actions and action groups)
  - Filters
  - Users
  - Settings (WEM settings)

  You cannot back up the following:

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

Restore. Opens the **Restore** wizard to revert to a previously backed up version of your WEM service configuration. When prompted, select the applicable folder that contains the backup copies (.XML files).

- **Security Settings**. Restores all settings present on the Security tab. The settings in the backup files *replace* the existing settings in your current site. When you switch to or refresh the **Security** tab, any invalid application security rules are detected. Those 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 the **Restore** wizard to handle application security rule assignments:

  - If you select **Yes**, restore attempts to restore rule assignments to users and user groups in your current site. Reassignment succeeds only if the backed up users or groups are present in your current site or AD. Any mismatched rules are restored but remain unassigned, and they are listed in a report dialog which you can export in CSV format.
  - If you select **No**, all rules in the backup are restored without being assigned to users and user groups in your site.

- **AD objects**. Restores the backed up AD objects to the existing site. The **Restore** wizard gives you granular control over AD objects to be imported. On the **Select the AD objects you want to restore** page, you can specify which AD objects you want to restore and whether to overwrite (replace) existing WEM AD objects.

- **Configuration set**. Restores the backed up configuration set to WEM. You can restore only one configuration set at a time. It might take some time for the WEM administration console to reflect the configuration set you restored. To view the restored configuration set, select it from the Configuration set menu in the Ribbon. When restoring a configuration set, WEM automatically renames it to `<configuration set name>_1` if a configuration set with the same name already exists.

> **Note:**
>
> - Restored actions are *added* to existing site actions.

> - Restored settings *replace* existing site settings.
> - Restored AD objects are *added* to or *replace* existing site AD objects, depending on whether you selected **Overwrite mode** in the AD objects page of the Restore wizard.
> - If you selected **Overwrite mode**, all existing AD objects are deleted before the restore process starts.

Migrate. Opens the **Migrate** wizard to migrate a zip backup of your Group Policy Objects (GPOs) to WEM.

> **Important:**
>
> - The **Migrate** wizard migrates only the settings (GPOs) that WEM supports.
> - We recommend that you back up your existing settings before you start the migration process.

We recommend that you perform the following steps to back up your GPOs:

1. Open the Group Policy Management Console.
2. In the **Group Policy Management** window, right-click the GPO you want to back up and then select **Back Up**.
3. In the **Back Up Group Policy Object** window, specify the location where you want to save the backup. Optionally, you can give the backup a description.
4. Click **Back Up** to start the backup and then click **OK**.
5. Navigate to the backup folder and then compress it into a zip file.

> **Note:**
>
> WEM also supports migrating zip files that contain multiple GPO backup folders.

After you back up your GPOs successfully, click **Migrate** to migrate your GPOs to WEM. On the **File to Migrate** page, click **Browse** and then navigate to the applicable file.

- **Overwrite**. Overwrites existing WEM settings (GPOs) when there are conflicts.
- **Convert**. Converts your GPOs to XML files suitable for import to WEM. Select this option if you want to have granular control over settings to be imported. After the conversion completes successfully, use the **Restore** wizard to manually import the XML files.

  > **Note:**
  >
  > You can name the output folder, but you cannot specify the names for the files to be saved.

About tab

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

Configure License Server. Allows you to specify the address of your Citrix License Server, without which the administration console does not let you modify any settings. Alternatively, you can use the

Licensing tab in the Infrastructure Services Configuration utility to specify these credentials. Citrix License Server information is stored in the same location in the database in both cases.

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

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

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

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

Actions

November 6, 2020

Workspace Environment Management streamlines the workspace configuration process by providing you with easy-to-use actions. The actions include managing applications, printers, network drives, external tasks, and more. You can use assignments to make actions available to users. Workspace Environment Management also provides you with filters to contextualize your assignments.

- Actions include managing:
  - Action Groups
  - Group Policy Settings
  - Applications
  - Printers
  - Network Drives
  - Virtual Drives
  - Registry Entries
  - Environment Variables
  - Ports
  - Ini Files

  - External Tasks
  - File System Operations
  - User DSN
  - File Associations
- Filters
- Assignments

Action Groups

August 25, 2020

The Action Groups feature lets you first define a group of actions and then assign all the defined actions in the action group to a user or user group in a single step. With this feature, you no longer have to assign each action present in the **Actions** pane one by one. As a result, you can assign multiple actions in a single step.

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

Action Group list

Action Groups

Displays a list of your existing action groups. Use **Find** to filter the list by name, display name, or description.

Actions

> **Important:**
>
> - The action group includes only actions already present in each action category (applications, printers, and network drives, and so on). For example, unless you have added applications on the **Application List** tab, the action groups on the **Action Group List** tab do not display any applications available for you to assign under **Applications**.
> - If you configure the options for actions in an assigned action group (**Action Group List > Name > Configured**), the configured options will not impact the users to which the action group is assigned.

The **Actions** section displays the actions available to you. You can perform the following operations:

- **Add**. Lets you create an action group that contains all the actions you want to assign to a user or user group.
- **Edit**. Lets you edit an existing action group.
- **Copy**. Lets you replicate an action group from an existing one.
- **Delete**. Lets you delete an existing action group.

To create an action group, follow the steps below.

1. On the **Administration Console > Actions > Action Groups > Action Group List** tab, click **Add**.
2. In the **New Action Group** window, type the required information, select the applicable option from the dropdown, and then click **OK**.

To edit an action group, select the applicable group from the list and then click **Edit**.

To clone an action group, select the group you want to clone and then click **Copy**. Note that the clone is automatically created after you click **Copy**. The clone inherits the name of the original and has a suffix "-Copy." You can click **Edit** to change the name.

> **Note:**
>
> When you clone an action group, actions (if any) associated with the Network and Virtual Drives are not cloned unless the **Allow Drive Letter Reuse in assignment process** option is enabled. To enable that option, go to the **Advanced Settings > Configuration > Console Settings** tab.

To delete an action group, select the applicable group from the list and then click **Delete**.

> **Note:**
>
> If you delete or edit an action group that is already assigned, the changes you make will impact all users to which the group is assigned.

Fields and controls

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

Description. Lets you specify additional information about the action group.

Action Group State. Toggles the action group between enabled and disabled state. When disabled, the agent does not process the actions included in the action group even if you assign that action group to a user or user group.

Configuration

Lets you search for the specific action that you want to assign or you have configured. Use Find to filter the option by name, display name, or description.

Available. These are the actions available to you to add to the action group you created.

Click the plus sign to expand the actions under the specific action category. Double-click an action or click the arrow buttons to assign or unassign it.

> **Note:**
>
> - If you add an action to an action group that is already assigned to users, the action will be assigned to those users automatically.
> - If you delete an action from an action group that is already assigned to users, the action will be unassigned from those users automatically.

Configured. These are the actions already assigned to the action group you created. You can expand individual actions to configure them. You can also configure the options for each specific action; for example, application shortcut locations, default printers, drive letter, and so on.

Assignments

> **Important:**
>
> If you configure the options for actions in an assigned action group in the Assigned pane on the **Action Assignment** tab, the configured options will automatically impact the users to which the action group is assigned.

After you finish configuring the actions for the action group on the **Actions > Action Groups > Action Group List** tab, you might want to assign the configured actions to the applicable user or user group. To do so, go to the **Assignments > Action Assignment > Action Assignment** tab. On that tab, double-click a user or user group to see the Action Groups node in the **Available** pane that contains the action groups you created. You can click the plus sign next to the Action Groups node to view the action groups you created. Double-click an action group or click the arrow buttons to assign or unassign it. When you assign an action, you are prompted to select the rule you want to use to contextualize that action.

For more information about how assignments work, see Assignments.

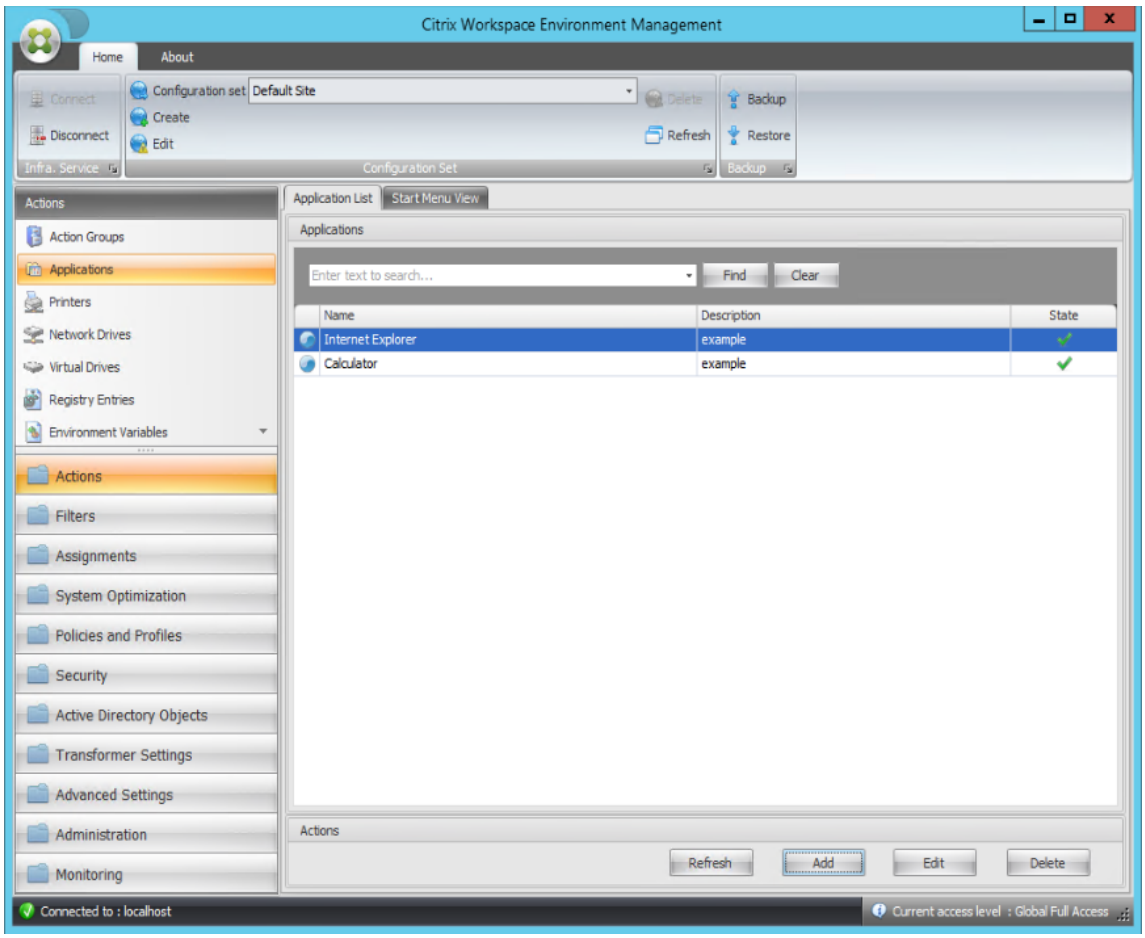
When assigning action groups, there are several scenarios to be aware of:

- If you assign an action group, all actions included in it are assigned.
- One or more actions might overlap in different action groups. For overlapping action groups, the group that is processed last overwrites groups that were processed earlier.
- After the actions in an action group are processed, consider assigning the actions that overlap with those in another action group. In this case, the unassigned actions overwrite those that were processed earlier, resulting in the actions processed later being unassigned. The other actions remain unchanged.

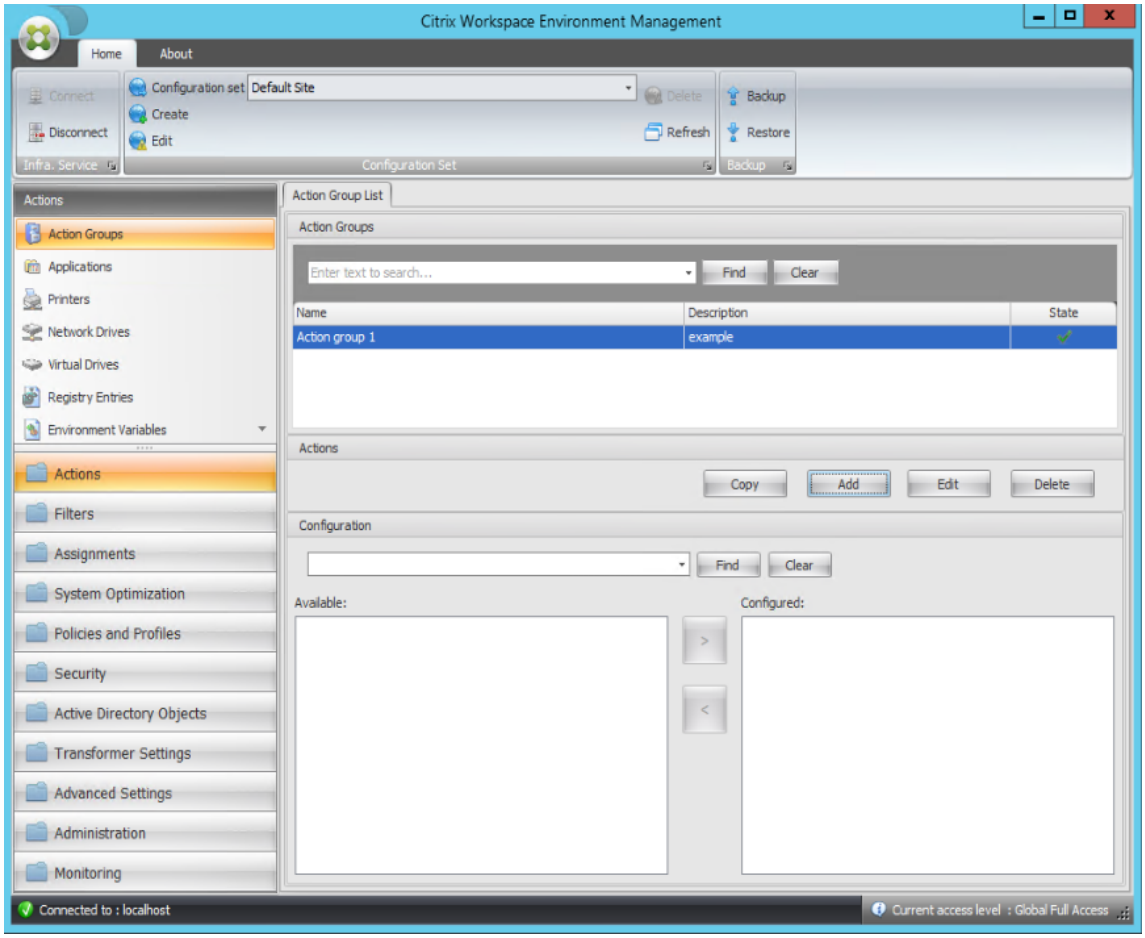
Example scenario

For example, to use the Action Groups feature to assign two applications (iexplore.exe and calc.exe) to a user at one time, follow the steps below.

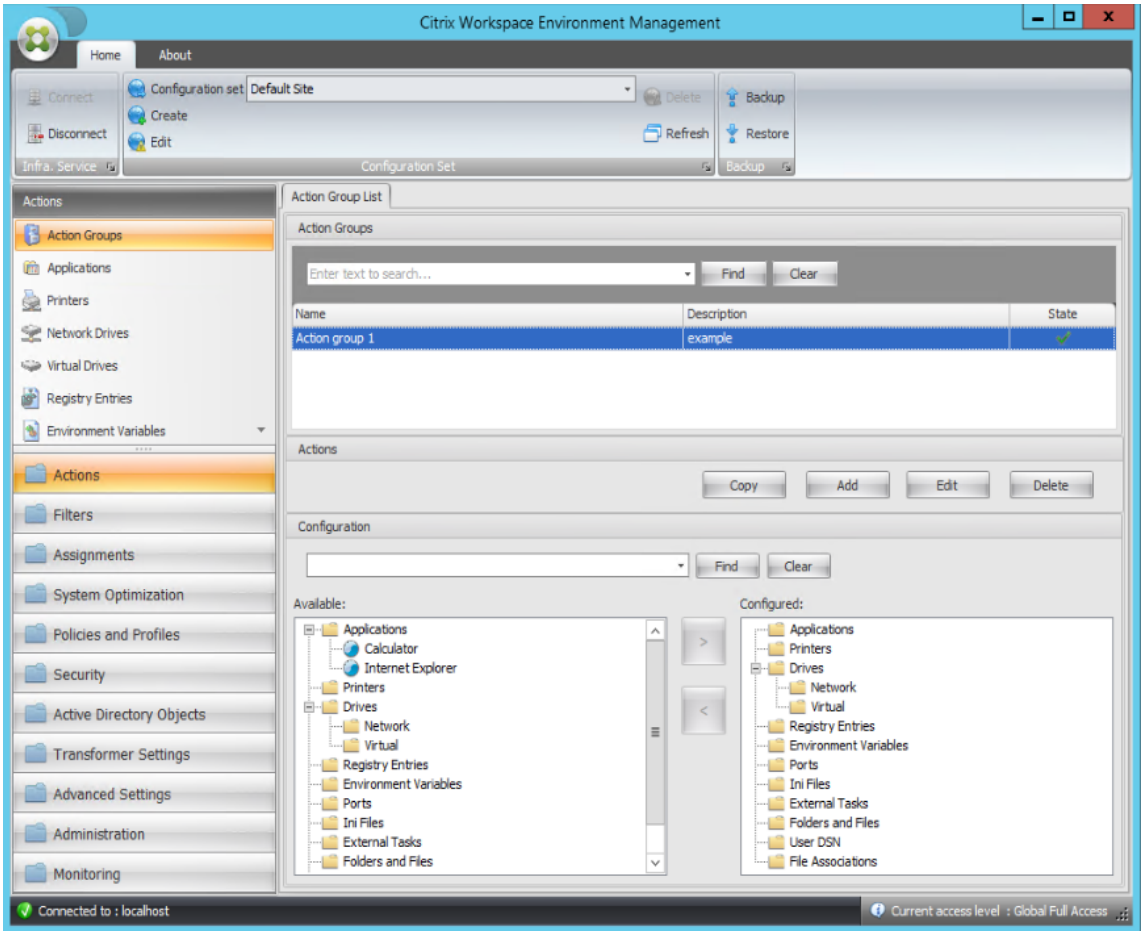
1. Go to the **Administration Console > Actions > Applications > Application List** tab and then add the applications (iexplore.exe and calc.exe).



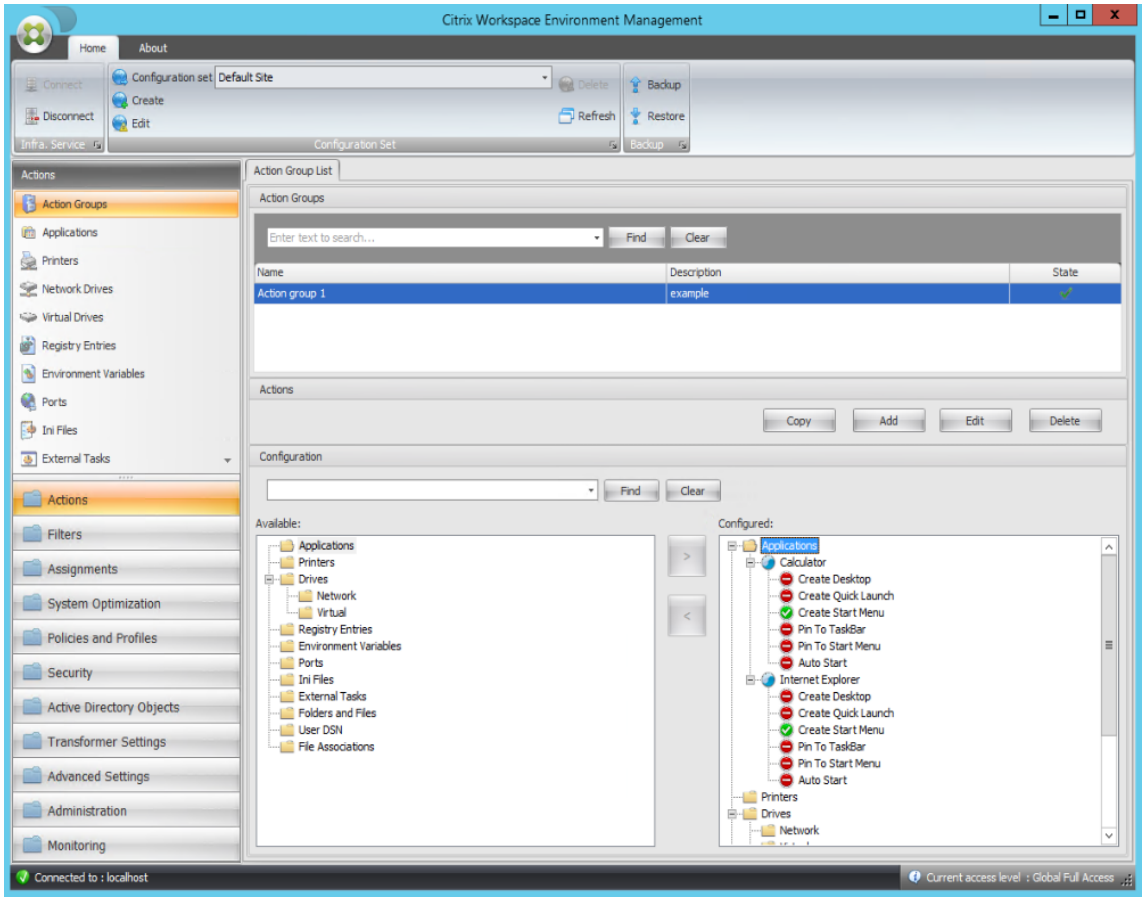
2. Go to the **Administration Console > Actions > Action Groups > Action Group List** tab and then click **Add** to create an action group.



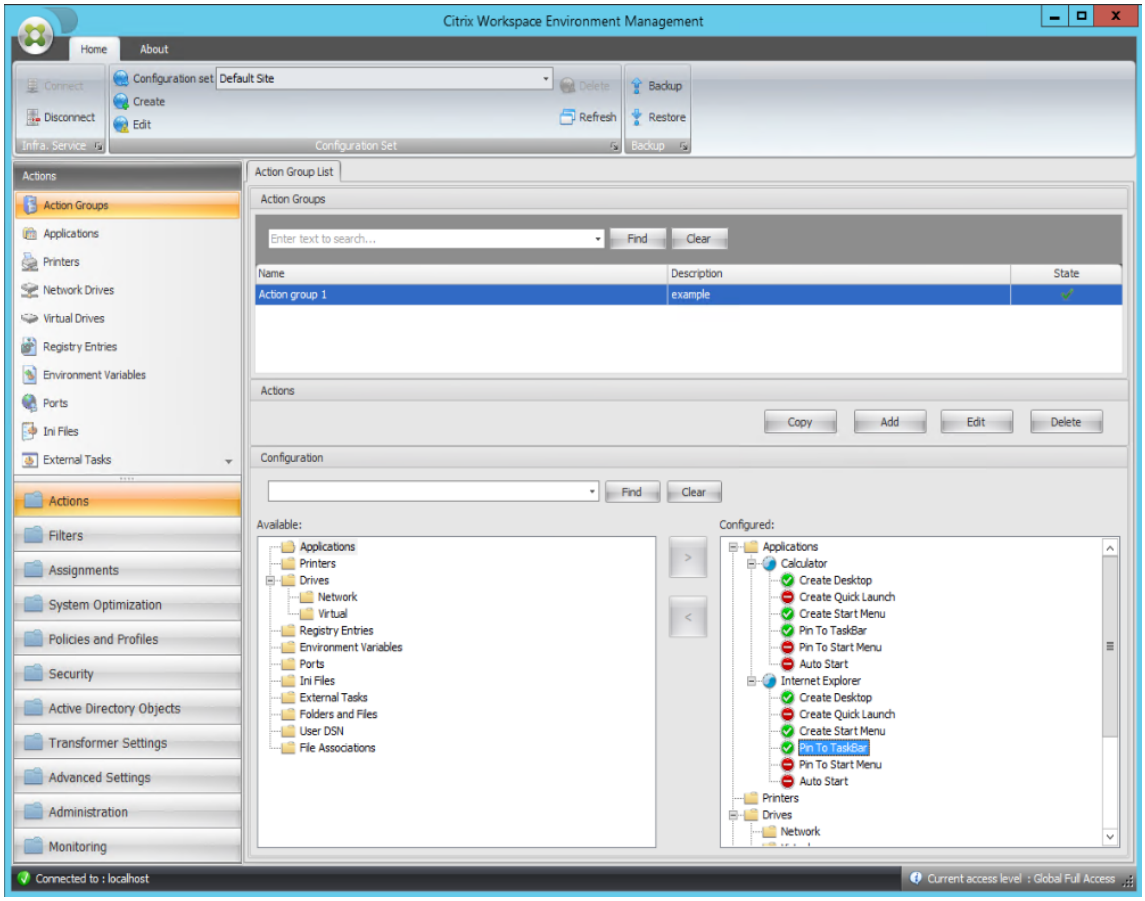
3. On the **Action Group List** tab, double-click the action group you created to display the action list in the **Available** and **Configured** panes.



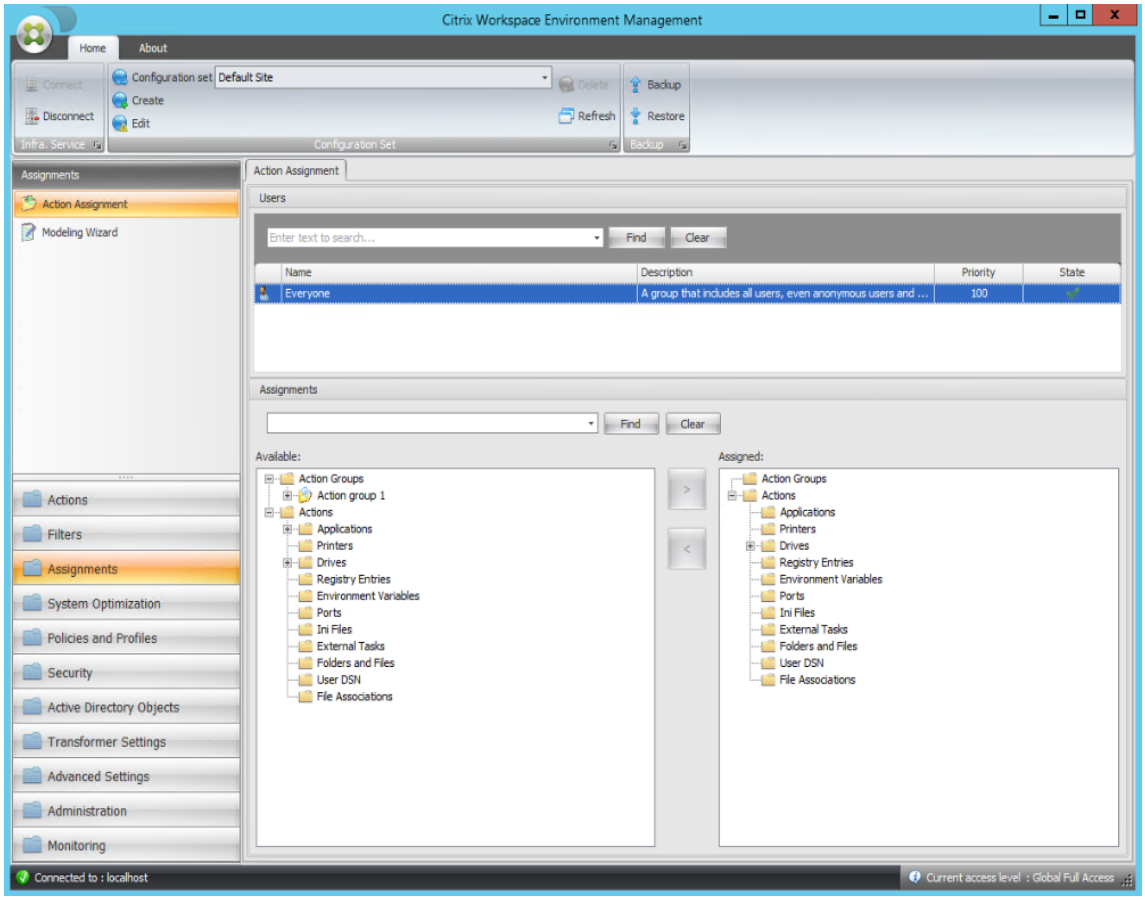
4. In the **Available** pane, double-click each application to move it to the **Configured** pane. You can also do so by selecting the application and then clicking the right arrow.



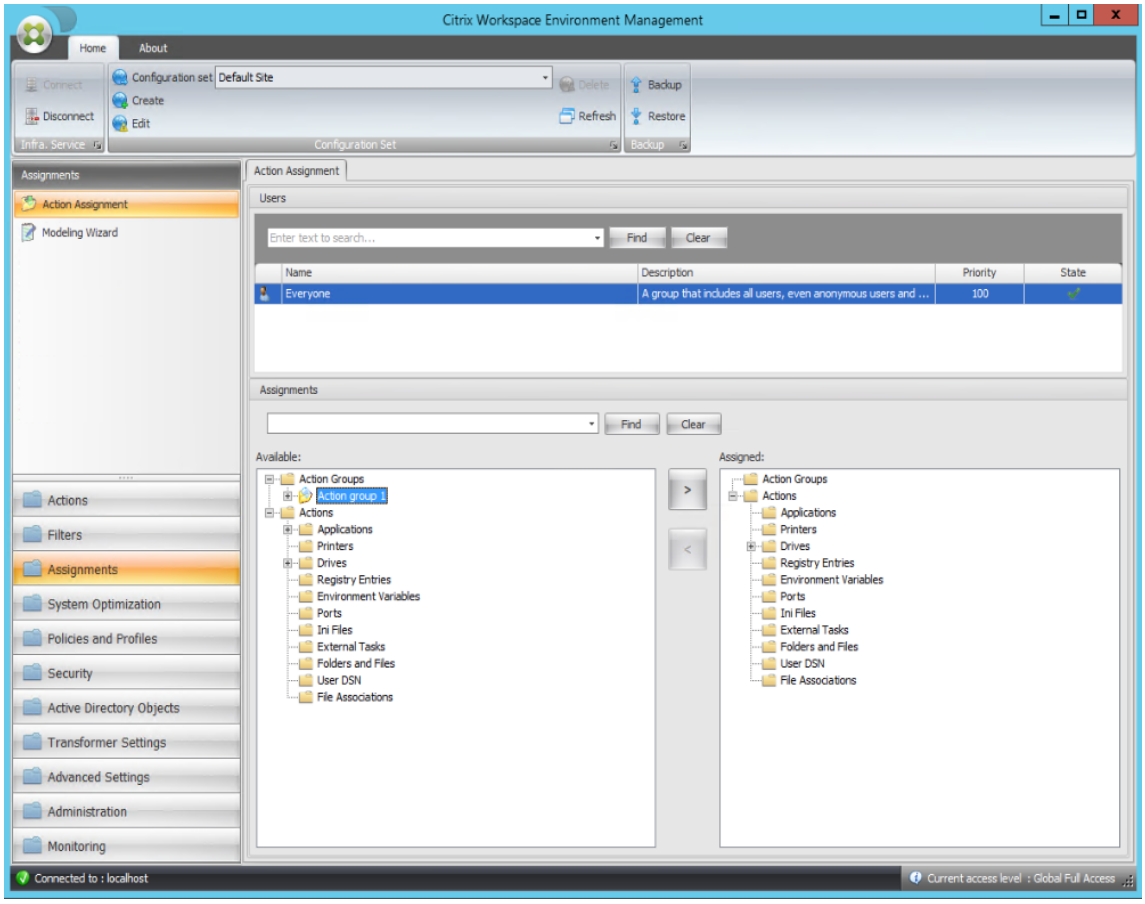
5. In the **Configured** pane, configure the options for each application. In this example, enable **Create Desktop** and **Pin To TaskBar**.



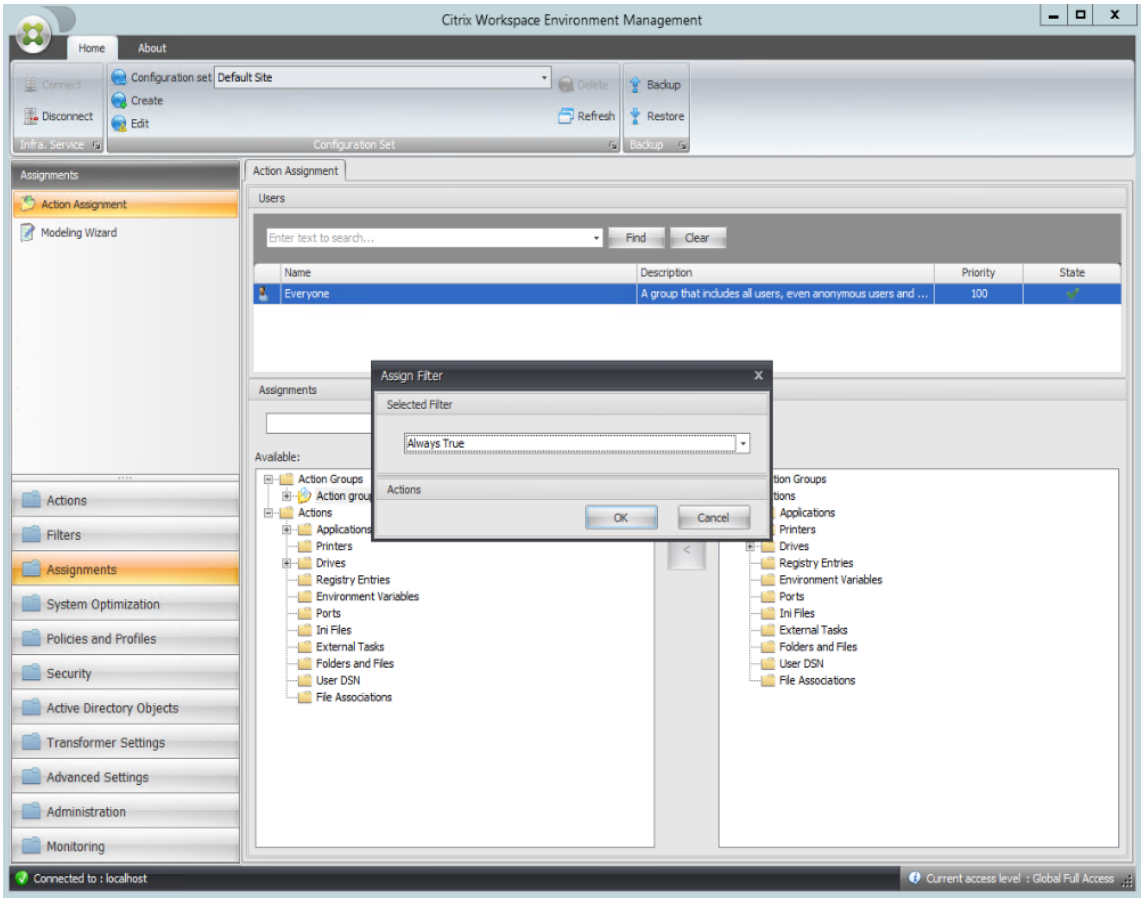
6. Go to the **Administration Console > Assignments > Action Assignment** tab and then double-click the applicable user to display the action group in the **Available** and **Assigned** panes.



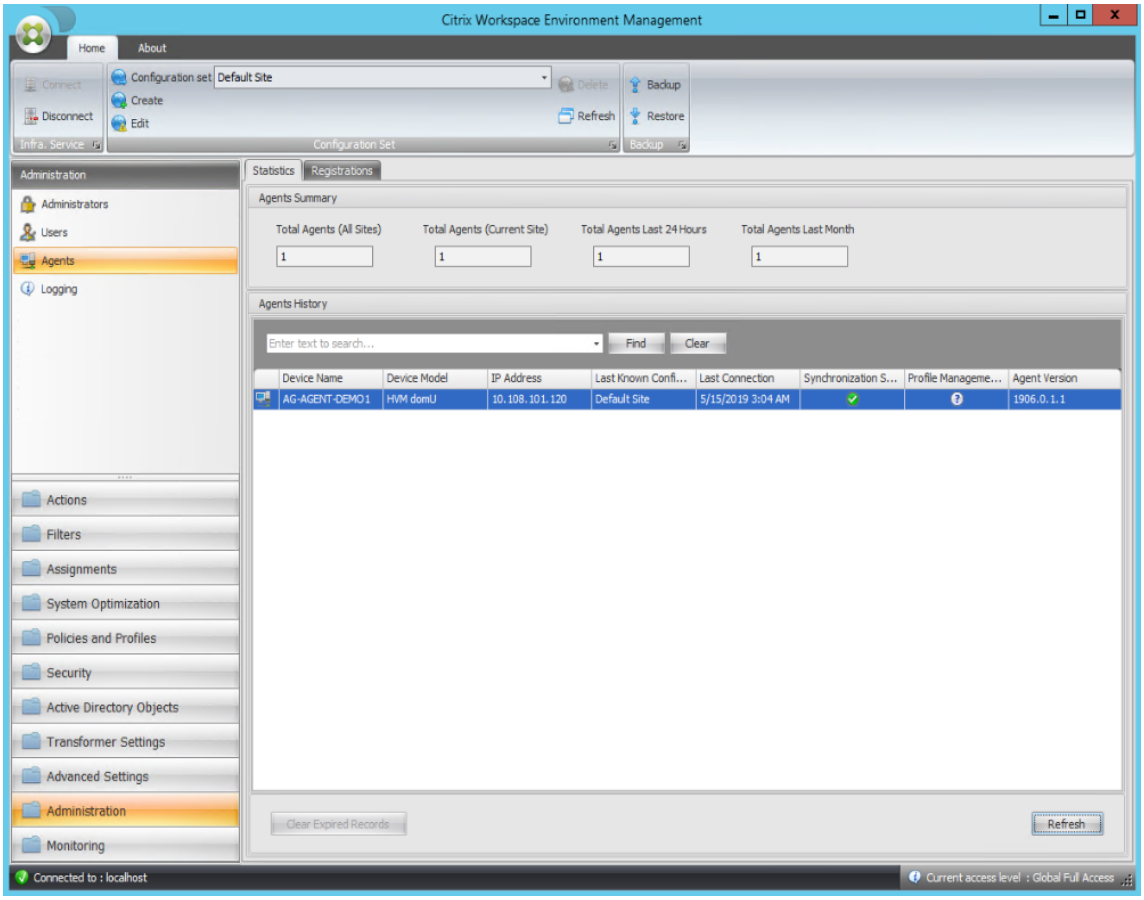
7. In the **Available** pane, double-click the action group you created (in this example, Action group 1) to move it to the **Assigned** pane. You can also do so by selecting the action group and then clicking the right arrow.



8. In the **Assign Filter** window, select **Always True** and then click **OK**.



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



10. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.
11. On the machine where the agent is running (agent host), verify that the configured actions are taking effect.

In this example, the two applications are successfully assigned to the agent host, and their shortcuts are added to the desktop and pinned to the taskbar.

Group Policy Settings

June 3, 2020

In previous releases, you could migrate only Group Policy Preferences (GPP) into Workspace Environment Management (WEM). For more information, see the description of the **Migrate** wizard in Ribbon. You can now also import Group Policy settings (registry-based settings) into WEM.

After importing the settings, you can have an itemized view of the settings associated with each GPO before you decide which GPO to assign. You can assign the GPO to different users or user groups, just like you assign other actions. You can also assign the GPO to groups containing AD machines. WEM applies machine settings that the GPO contains to machines in the assigned group.

Group Policy settings

Enable Group Policy Settings Processing. Controls whether to enable WEM to process Group Policy settings. If disabled, you cannot configure Group Policy settings, and WEM does not process Group Policy settings even if they are already assigned to users or user groups. By default, this option is disabled.

Group Policy Object list

Displays a list of your existing GPOs. Use **Find** to filter the list by name or description.

- **Refresh**. Refreshes the GPO list.
- **Import**. Opens the **Import Group Policy Settings** wizard, which lets you import Group Policy settings into WEM.
- **Edit**. Lets you edit an existing GPO. Currently, WEM supports editing the name and description for each GPO. It does not support editing registry operations associated with each GPO.
- **Delete**. Deletes the GPO you select.

On your domain controller, you can perform the following steps to back up your Group Policy settings:

1. Open the Group Policy Management Console.
2. In the **Group Policy Management** window, right-click the GPO you want to back up and then select **Back Up**.
3. In the **Back Up Group Policy Object** window, specify the location where you want to save the backup. Optionally, you can give the backup a description.
4. Click **Back Up** to start the backup and then click **OK**.
5. Navigate to the backup folder and then compress it into a zip file.

> **Note:**
>
> WEM also supports importing zip files that contain multiple GPO backup folders.

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

1. Use **Upload**, available in the menu on the WEM service **Manage** tab, to upload the zip file of your GPOs to the default folder in Citrix Cloud.
2. Navigate to the **Administration Console > Actions > Group Policy Settings** tab, select **Enable Group Policy Settings Processing**, and then click **Import** to open the import wizard.
3. On the **File to Import** page of the import wizard, click **Browse** and then select the applicable file from the list. You can also type the name of the file and then click **Find** to locate it.
    - **Overwrites GPOs you imported previously**. Controls whether to overwrite existing GPOs.

4. Click **Start Import** to start the import process.

After importing the settings, you can have an itemized view of the settings associated with each GPO. To do so, select a GPO and then click **Edit**.

Name. The name of the GPO as it appears in the GPO list.

Description. Lets you specify additional information about the GPO, which appears in the GPO list.

Registry Operations. Displays registry operations that the GPO contains.

> **Note:**
>
> To ensure that Group Policy settings can be processed properly, verify that Citrix WEM User Logon Service is enabled on the WEM agents.

Applications

May 4, 2020

Controls the creation of application shortcuts.

> **Tip:**
>
> - You can use Citrix Studio to edit the application settings and then add an executable file path that points to **VUEMAppCmd.exe**. **VUEMAppCmd.exe** ensures that the Workspace Environment Management agent finishes processing an environment before Citrix Virtual Apps and Desktops published applications are started. For more information, see Editing application settings using Citrix Studio.
> - You can use dynamic tokens to extend Workspace Environment Management actions to make them more powerful.

Application List

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

To add an application

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

Fields and controls

General

- **Name**. The display name of the application shortcut, as it appears in the application list.
- **Description**. This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.
- **Application Type**. The type of application the shortcut starts, which can be one of **Installed application**, **File/Folder**, **URL**, or **StoreFront store**. The following values are required depending on the selection:
  - **Command Line**. The path to the application executable as the client machine sees it. The **Browse** button allows you to browse to a locally installed executable.
  - **Working Directory**. The shortcut working directory. Automatically filled out if you browse to the executable.
  - **Parameters**. Any launch parameters for the application.
  - **Target**. (File/Folder) The name of the target file or folder the application opens.
  - **Shortcut URL**. (URL) The URL of the application shortcut you are adding.
  - **Store URL**. (StoreFront store) The URL of the StoreFront store containing the resource you want to start from the shortcut.
  - **Store Resource**. (StoreFront store) The resource on the StoreFront store that you want to start from the shortcut. The **Browse** button allows you to browse and select the resource.

    > **Tip:**
    >
    > To add an application that is based on a StoreFront store, you must provide valid credentials. A dialog appears the first time you click **Browse** to view store resources. The dialog prompts you to type credentials that you use to log on to Citrix Workspace app for Windows. After that, the Store Resources window appears, displaying a list of published applications retrieved by Citrix Workspace app for Windows running on the WEM administration console machine.
- **Start Menu Integration**. Select where the application shortcut is created in the Start menu. By default, a new shortcut is created in Programs.

Options

- **Select Icon**. Allows you to browse to an icon file and select an icon for your application. By default, this setting uses the application executable's icon but you can select any valid icon. Icons are stored in the database as text.
  - **High Resolution Icons Only**. Displays only HD icons in the selection box.

- **Application State**. Controls whether the application shortcut is enabled. When disabled, the agent does not process it even if it is assigned to a user.
- **Maintenance Mode**. When active, this setting prevents the user from running the application shortcut. The shortcut icon is modified to include a warning sign to denote that the icon is not available, and the user receives a short message informing them the application is unavailable if they try to launch it. This allows you to proactively manage scenarios where published applications are in maintenance without having to disable or delete application shortcut resources.
- **Display Name**. The name of the shortcut as it appears in the user's environment.
- **Hotkey**. Allows you to specify a hotkey for the user to launch the application with. Hotkeys are case sensitive and are entered in the following format (for example): Ctrl + Alt + S.
- **Action Type**. Describes what type of action this resource is.

Advanced Settings

- **Enable Automatic Self-Healing**. When selected, the agent automatically recreates application shortcuts on refresh if the user has moved or deleted them.
- **Enforce Icon Location**. Allows you to specify the exact location of the application shortcut on the user's desktop. Values are in pixels.
- **Windows Style**. Controls whether the application opens in a minimized, normal, or maximized window on endpoints.
- **Do Not Show in Self Services**. Hides the application from the self-service interface accessible from a status bar icon available to end-users when the session agent is running in UI mode. This includes hiding it in the context menu "My Applications" icon list, and in the Manage Applications form.
- **Create Shortcut in User Favorites Folder**. Creates an application shortcut in the end-user Favorites folder.

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

Start Menu View

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

Refresh. Refreshes the application list.

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

Edit. Opens up the application edition wizard.

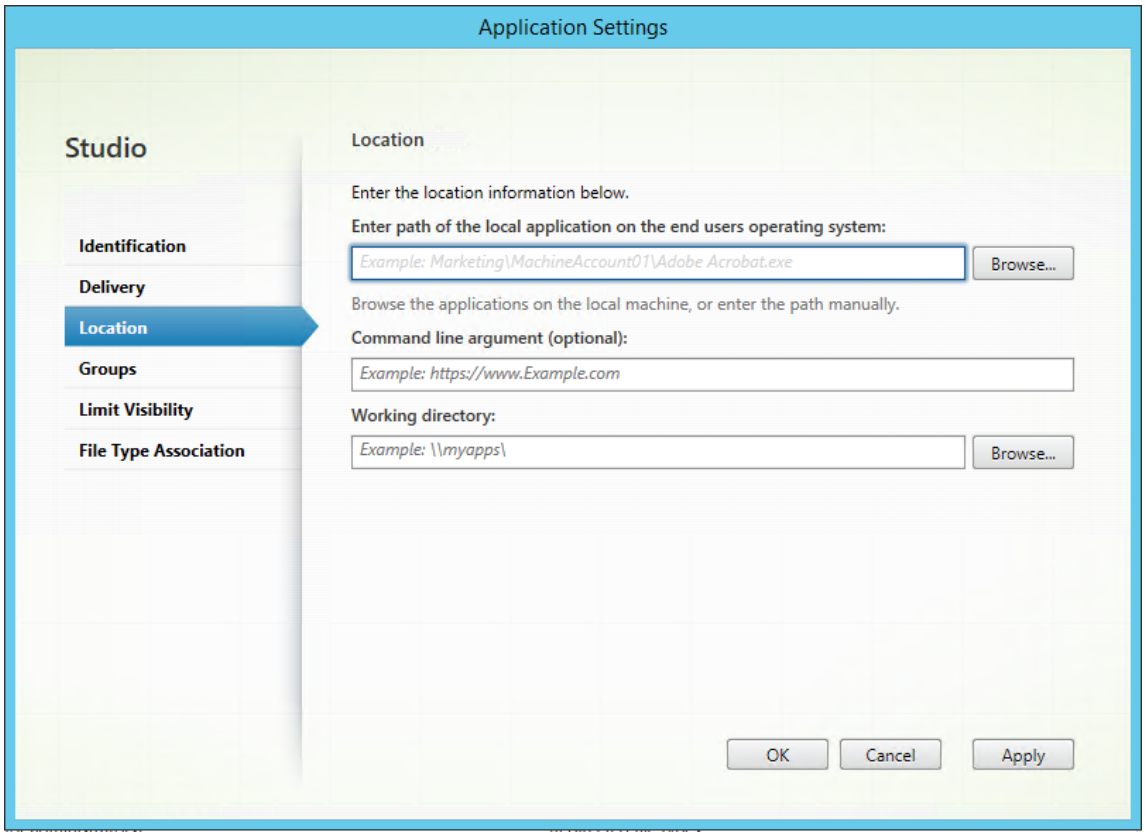
Delete. Deletes the selected application shortcut resource.

Editing application settings using Citrix Studio

Workspace Environment Management (WEM) provides you with client-side tools to troubleshoot issues you experience. The VUEMAppCMD tool (**VUEMAppCmd.exe**) ensures that the WEM agent finishes processing an environment before Citrix Virtual Apps and Desktops published applications are started. It is located in the agent installation folder: `%ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMAppCmd.exe`.

You can use Citrix Studio to edit the application settings and then add an executable file path that points to **VUEMAppCmd.exe**. To do so, complete the following steps:

1. Navigate to the **Application Settings > Location** page of Citrix Studio.



2. Type the path of the local application on the end-user operating system.
   - Type the following: `%ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMAppCmd.exe`.
3. Type the command-line argument to specify an application to open.
   - Type the full path to the application that you want to launch through **VUEMAppCmd.exe**. Make sure that you wrap the command line for the application in double quotes if the path contains blank spaces.
   - For example, suppose you want to launch **iexplore.exe** through **VUEMAppCmd.exe**. You

can do so by typing the following: `" %ProgramFiles(x86)%\Internet Explorer\iexplore.exe"` .

Printers

August 13, 2019

This tab controls the mapping of printers.

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

Network Printer List

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

To add a printer

1. On the **Network Printer List** tab, click **Add** or right-click the blank area and then select **Add** in the context menu.
2. In the **New Network Printer** window, type the required information and then click **OK**.

Fields and controls

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

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

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

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

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

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

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

October 22, 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.

Import registry files

1. In the administration console, navigate to **Actions** > **Registry Entries**.
2. In the ribbon, click **Import Registry File**.
3. In the **Import from Registry File** window, click **Browse** to navigate to the applicable registry file.
4. Click **Scan** to start scanning the registry file. After the scan completes successfully, a list of registry settings appears.
5. Select the registry settings you want to import and then click **Import Selected** to start the importing process.
6. Click **OK** to exit the **Import from Registry File** window.

Fields and controls

Registry File Name. Populates automatically after you navigate to a **.reg** file and click **Open**. The **.reg** file contains registry settings you want to import into WEM. The **.reg** file must be generated from a clean environment to which only the registry settings you want to import are applied.

Scan. Scans the **.reg** file and then displays a list of registry settings that the file contains.

Registry Values List. Lists all registry values that the **.reg** file you want to import contains.

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

Prefix Imported Item Names. If selected, adds a prefix to the name of all registry items imported through this wizard (for example, “XP ONLY” or “finance”). Doing so makes it easier to identify and organize your registry entries.

> **Note:**
>
> The wizard cannot import registry entries with the same names. If your **.reg** file contains more than one registry entry that has the same name (as displayed in the Registry Values List), select one of these entries for import. If you want to import the others, rename them.

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.

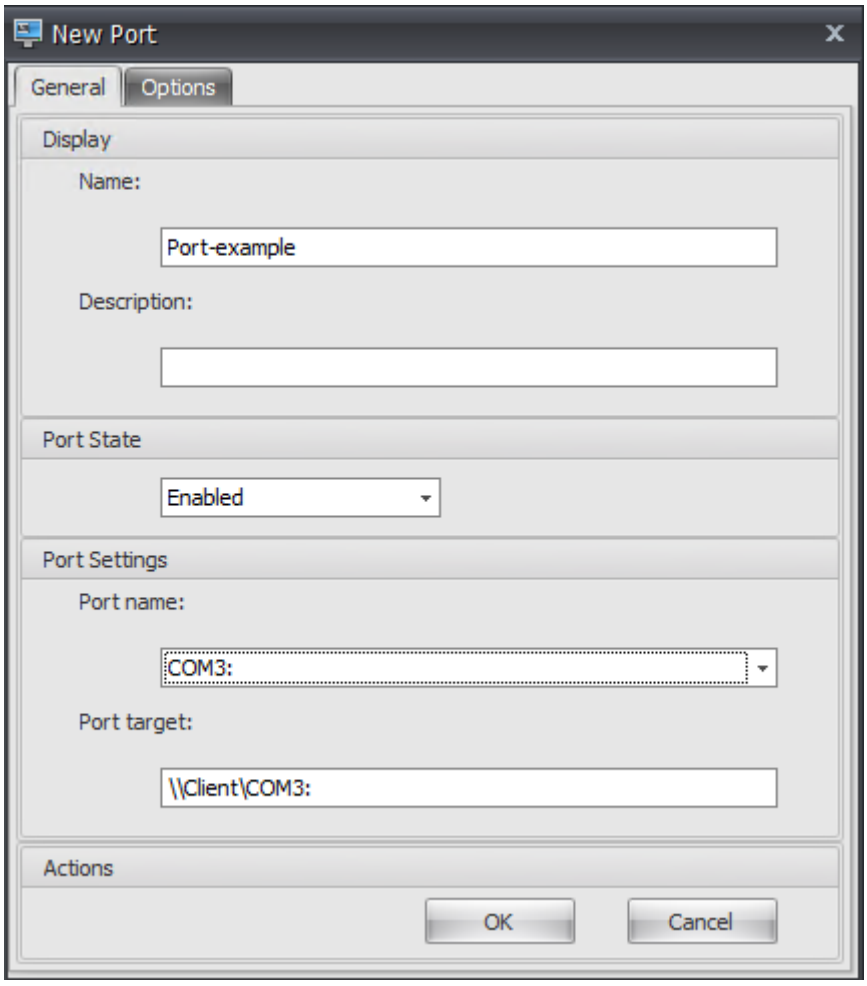
Port Target. The target port.

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:`



Ini Files

July 9, 2020

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

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

Ini files operation list

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

To add an .ini files operation

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

Fields and controls

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

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

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

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

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

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

Target Value. This specifies the value itself.

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

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

External Tasks

July 16, 2020

Controls the execution of external tasks. External tasks include running scripts and applications as long as the agent host has the corresponding programs to run them. Commonly used scripts include: **.vbs** and **.cmd** scripts.

With the external tasks feature, you can specify when to run an external task. Doing so lets you more effectively manage user environments.

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

External task list

A list of your existing external tasks. You can use **Find** to filter the list 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. Lets you specify the display name of the external task, which appears in the external task list.

Description. Lets you specify additional information about the external task.

Path. Lets you specify the path to the external task. The path resolves in the user environment. Make sure that:

- The path you specified here is consistent with the agent host.
- The agent host has the corresponding program to run the task.

Arguments. Lets you specify launch parameters or arguments. You can type a string. The string contains arguments to pass to the target script or application. For examples to use the **Path** and **Arguments** fields, see External task examples.

External Task State. Controls whether the external task is enabled or disabled. When disabled, the agent does not process the task even if the task is assigned to users.

Process on

- **Refresh**. Controls whether to run the external task when users refresh the agent. By default, the option is selected.
- **Reconnect**. Controls whether to run the external task when a user reconnects to a machine on which the agent is running. By default, the option is selected. If the WEM agent is installed on a physical Windows device, this option is not applicable.
- **Logon**. Controls whether to run the external task when users log on. By default, the option is selected.
- **Logoff**. Controls whether to run the external task when users log off. This option does not work unless Citrix User Logon Service is running. By default, the option is not selected.

Run Hidden. If selected, the task runs in the background and is not displayed to users.

Run Once. If selected, WEM runs the task only once regardless of which options you select in the **Process On** section and regardless of whether agents restart. By default, this option is selected.

Execution Order. Lets you specify the order of execution for each task. The option can be useful when you have multiple tasks assigned to users and some tasks rely on others to run successfully. By default, the value is 0.

Wait for Task Completion. Lets you specify how long the agent waits for the task to complete. By default, the **Wait Timeout** value is 30 seconds.

Action Type. Describes what type of action the external task is.

Troubleshooting

After you enable the feature, the WEM agent creates a log file named `Citrix WEM Agent Logoff.log` the first time a user logs off. The log file is located in a user's profile root folder. The WEM agent writes information to the log file every time the user logs off. The information helps you monitor and troubleshoot issues related to external tasks.

External task examples

For a script (for example, PowerShell script):

- If neither the folder path nor the script name contains blank spaces:
  - In the **Path** field, type the following: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.
  - In the **Arguments** field, type the following: `C:\<folder path>\<script name>.ps1`.

  Alternatively, you can type the path to the script file directly in the **Path** field. For example: `C:\<folder path>\<script name>.ps1`. In the **Arguments** field, specify arguments if needed. However, whether the script file is run or opens with a different program depends on file type

associations configured in the user environment. For information about file type associations, see File Associations.

- If the folder path or the script name contains blank spaces:
  - In the **Path** field, type the following: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.
  - In the **Arguments** field, type the following: `-file C:\<folder path>\<script name>.ps1`.

For an application (for example, iexplore.exe):

- In the **Path** field, type the following: `C:\Program Files\internet explorer\iexplore.exe`.
- In the **Arguments** field, type the URL of the website to open: `https://docs.citrix.com/`.

File System Operations

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

July 9, 2020

> **Important:**
>
> File type associations that you configure become default associations automatically. However, when you open an applicable file, the "How do you want to open this file?" window might still appear, prompting you to select an application to open the file. Click **OK** to dismiss the window. If you do not want to see a similar window again, do the following: Open the Group Policy Editor and enable the **Do not show the 'new application installed' notification** policy (**Computer Configuration > Administrative Templates > Windows Components > File Explorer**).

Controls the creation of file type associations in the user environment.

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

File association list

A list of your existing file associations. You can use **Find** to filter the list by name or ID.

To add a file association

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

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

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

File Association State. Toggles whether the file association is Enabled or Disabled. When disabled, it is not processed by the agent even if assigned to a user.

File Extension. The extension used for this file type association. If you select a file name extension from the list, the **ProgID** field automatically populates (if the file type is present on the machine where the administration console is running). You can also type the extension directly. However, for browser associations, you *must* type the extension directly. For more information, see Browser association.

ProgID. The programmatic identifier associated with an application (COM). This value automatically populates when you select a file extension from the list. You can also type the ProgID directly. To discover the ProgID of an installed application, you can use the OLE/COM Object Viewer (oleview.exe), and look in Object Classes/Ole 1.0 Objects. For more information about ProgID, see Programmatic identifier (ProgID).

Action. Lets you select the action type: open, edit, or print.

Target application. Lets you specify the executable used with this file name extension. Type the full path of the executable. For example, for UltraEdit Text Editor: `C:\Program Files\IDM Computer Solutions\UltraEdit\uedit64.exe`

Command. Lets you specify action types that you want to associate with the executable. For example:

- For an open action, type `"%1"`.
- For a print action, type `/p"%1"`.

Set as Default Action. Toggles whether the association is set as a default for that file name extension.

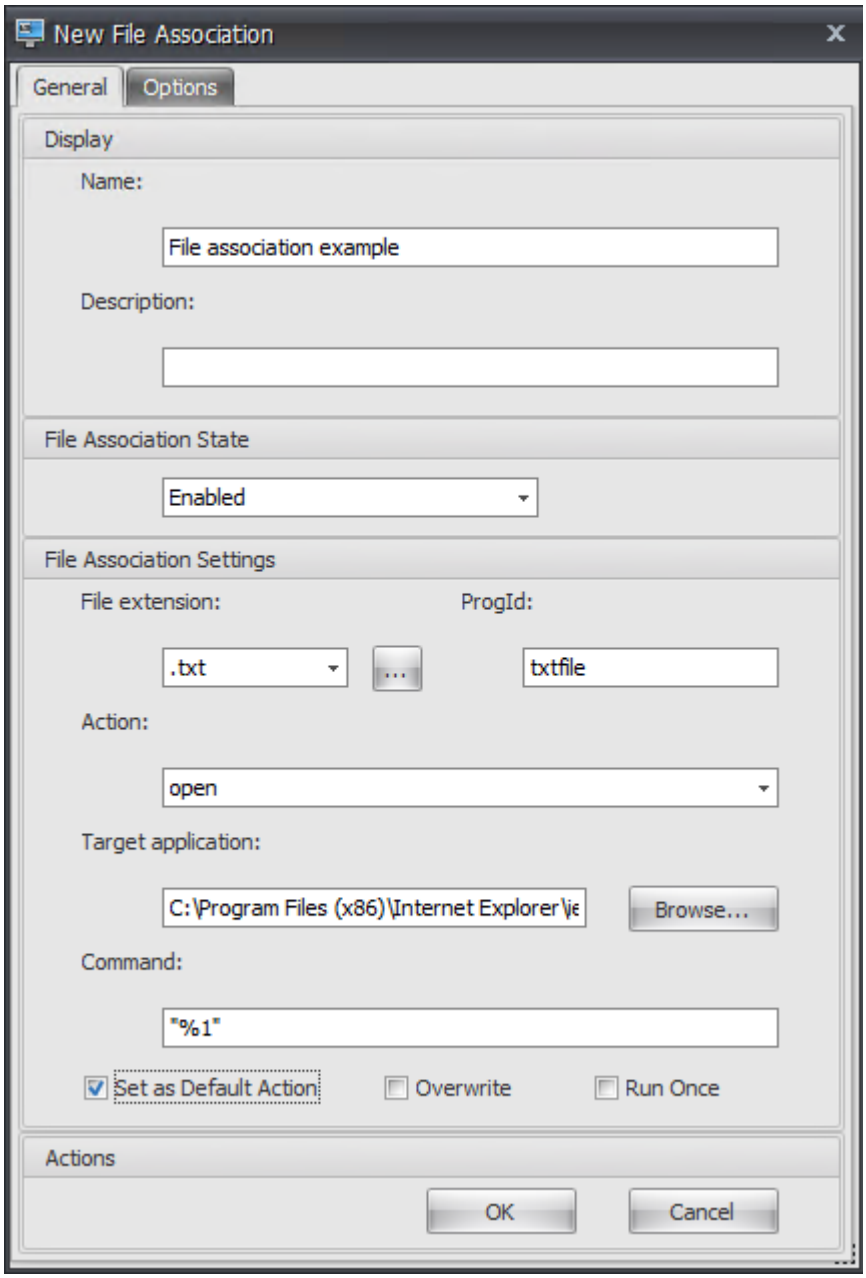
Overwrite. Toggles whether this file association overwrites any existing associations for the specified extension.

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

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

For example, to add a new file type association for text (.txt) files for users to automatically open text files with the program you selected (here, iexplore.exe), complete the following steps.

1. On the **Administration Console > Actions > File Associations > File Association List** tab, click **Add**.
2. In the **New File Association** window, type the information and then click **OK**.



- **File Association State**. Select **Enabled**.
- **File extension**. Type the file name extension. In this example, type .txt.
- **Action**. Select **Open**.
- **Target application**. Click **Browse** to navigate to the applicable executable (.exe file). In this example, browse to iexplore.exe located in the C:\Program Files (x86)\Internet Explorer folder.

- **Command**. Type “%1” and make sure to wrap %1 in double quotes.
- Select **Set as Default Action**.

3. Go to the **Administration Console > Assignments > Action Assignment** tab.
4. Double-click the user or user group to which you want to assign the action.
5. Go to the **Administration Console > Administration > Agents > Statistics** tab and then click **Refresh**.
6. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.
7. Go to the machine on which the agent is running (user environment) to verify that the created file type association works.

In this example, if you double-click a file with a .txt extension in the end-user environment, that file automatically opens in Internet Explorer.

Good to know

Browser association

WEM supports creating an association for these browsers:

- Google Chrome
- Firefox
- Opera
- Internet Explorer (IE)
- Microsoft Edge

When creating browser associations, keep the following in mind:

- In the **File extension** field, type `http` or `https`.
- In the **ProgID** field, type the following (case sensitive) based on your choice:
  - `ChromeHTML` for Google Chrome
  - `firefox` for Firefox
  - `OperaStable` for Opera
  - `IE` for Internet Explorer (IE)
  - `edge` for Microsoft Edge

Programmatic identifier (ProgID)

You no longer have to fill out the following fields: **Action**, **Target application**, and **Command**. You can leave the fields empty as long as you can provide the correct **ProgID**. See below a list of ProgIDs for popular applications:

- Acrobat Reader DC: `AcroExch.Document.DC`

- Opera browser: `OperaStable`
- Google Chrome browser: `ChromeHTML`
- Internet Explorer: `htmlfile`
- Wordpad: `textfile`
- Notepad: `txtfile`
- Microsoft Word 2016: `Word.Document.12`
- Microsoft PowerPoint 2016: `PowerPoint.Show.12`
- Microsoft Excel 2016: `Excel.Sheet.12`
- Microsoft Visio 2016: `Visio.Drawing.15`
- Microsoft Publisher 2016: `Publisher.Document.16`

However, you must fill out the fields (**Action**, **Target application**, and **Command**) if:

- You cannot provide the correct **ProgID**.
- The target application (for example, UltraEdit Text Editor) does not register its own ProgID in the registry during installation.

Filters

July 31, 2020

Filters contain rules and conditions that let you make actions available (assign actions) to users. Set up rules and conditions before assigning actions to users.

Rules

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

Filter rule list

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

To add a filter rule

1. Use the context menu **Add** command.
2. Enter details in the **New Filter Rule** dialog.
3. Move conditions you want configured in this rule from the **Available** list to the **Configured** list.
4. Click **OK**.

Fields and controls

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

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

Filter Rule State. Toggles whether the rule is enabled or disabled. When disabled, the agent does not process actions using this rule even if they are assigned.

Available Conditions. These are the filter conditions available to be added to the rule. Note. The **DateTime** filter expects results in the format: `YYYY/MM/DD HH:mm`

Multiple values can be separated with semicolons (;) and ranges can be separated with hyphens. When specifying a range between two times on the same date, the date must be included in both ends of the range, for example: 1969/12/31 09:00-1969/12/31 17:00

Configured Conditions. These are the conditions already added to the rule.

> **Note:**
>
> These conditions are **AND** statements, not **OR** statements. Adding multiple conditions requires them all to trigger for the filter to be considered triggered.

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 (for example **192.168.10.1-192.168.10.5**). Separate multiple ranges or addresses using the semicolon character (;) . For example, **192.168.10.1-192.168.10.5;192.168.10.8-192.168.10;192.168.10.17** is a valid value which includes the ranges **.1-.5** and **.8-.10**, plus the individual address **.17**.

Assignments

September 21, 2020

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

Use assignments to make actions available to your users. This lets you replace a portion of your users' logon scripts.

Action Assignment

Users

This is your list of configured users and groups (see Users in Active Directory Objects). Double-click a user or group to populate the assignments menu. Use **Find** to filter the list by name or ID.

> **Tip:**
>
> To simplify assigning actions for all users in Active Directory, use the "Everyone" default group to assign the actions. The actions that you assign to the "Everyone" default group do not appear on the **Resultant Actions** tab in the **Actions Modeling Wizard** for an individual user. For example, after you assign action1 to the "Everyone" default group, you might find that action1 does not appear on the **Resultant Actions** tab.

Assignments

Lets you assign actions to the selected user or group. Use **Find** to filter the list by name or ID.

Available. Displays actions available for you to assign to this user or group.

Double-click an action or click the arrow buttons to assign or unassign it. When you assign an action, you are prompted to select a rule to contextualize it.

Assigned. Displays actions already assigned to this user or group. You can expand individual actions to configure them (application shortcut locations, default printers, drive letter, and so on).

To assign actions to users/groups

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

> **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 want to model.

Resultant Actions. The actions assigned to the user or to groups the user belongs to.

User Groups. The groups the user belongs to.

System Optimization

November 3, 2020

Workspace Environment Management system optimization consists of the following:

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

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

While system optimization settings are machine-based and apply to all user sessions, process optimization is user centric. This means that when a process triggers CPU Spike Protection in user A's session, the event is recorded only for user A. When user B starts the same process, process optimization behavior is determined only by process triggers in user B's session.

CPU Management

September 17, 2020

These settings let you optimize CPU usage.

CPU Management Settings

Processes can run across all cores and can use up as much CPU as they want. In Workspace Environment Management (WEM), **CPU Management Settings** lets you limit how much CPU capacity individual processes can use. CPU spike protection is not designed to reduce overall CPU usage. It is designed to reduce the impact on user experience by processes that consume an excessive percentage of CPU Usage.

When CPU spike protection is enabled, if a process reaches a specified threshold, WEM automatically lowers the priority of the process for a certain time. Then, when a new application is launched, it has a higher priority than the lower-priority process and the system will continue to run smoothly.

CPU spike protection examines each process in quick "snapshot." If the average load of a process exceeds the specified usage limit for a specified sample time, its priority reduces immediately. After a specified time, the process' CPU priority returns to its previous value. The process is not "throttled." Like in **CPU Clamping**, only its priority is reduced.

CPU spike protection is not triggered until at least one instance of an individual process exceeds the threshold. In other words, even if total CPU consumption exceeds the specified threshold, CPU spike protection is not triggered unless at least one process instance exceeds the threshold. But when that process instance triggers CPU spike protection, new instances of the same process are (CPU) optimized when the option "Enable Intelligent CPU Optimization" is enabled.

Whenever a specific process triggers CPU spike protection, the event is recorded in the agent's local database. The agent records trigger events for each user separately. This means that CPU optimization for a specific process for user1 does not affect the behavior of the same process for user2.

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

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

CPU Spike Protection

> **Note:**
>
> - "CPU usage" in the following settings is based on "logical processors" in the physical or virtual machine. Each core in a CPU is considered as a logical processor, in the same way that Windows does. For example, a physical machine with one 6-core CPU is considered to have 12 logical processors (Hyper-Threading Technology means cores are doubled). A physical machine with 8 x CPUs, each with 12 cores, has 96 logical processors. A VM configured with two 4-core CPUs has 8 logical processors.

> - The same applies to virtual machines. For example, suppose you have a physical machine with 8 x CPUs, each with 12 cores (96 logical processors), supporting four multi-session OS VDA VMs. Each VM is configured with two 4-core CPUs (8 logical processors). To restrict processes that trigger CPU spike protection on a VM, to use half of its cores, set **Limit CPU Core Usage** to 4 (half of the VM's logical processors), not to 48 (half of the physical machine's logical processors).

Enable CPU Spike Protection. Lowers the CPU priority of processes for a period of time (specified in the **Idle Priority Time** field) if they exceed the specified percentage of CPU usage for a period of time (specified in the **Limit Sample Time** field).

- **Auto Prevent CPU Spikes**. Use this option to automatically reduce the CPU priority of processes that overload your CPU. This option automatically calculates the threshold value at which to trigger CPU spike protection based on the number of logical processors (CPU cores). For example, suppose there are 4 cores. With this option enabled, if the overall CPU usage exceeds 23%, the CPU priority of processes that consume more than 15% of the overall CPU resources reduces automatically. Similarly, in the case of 8 cores, if the overall CPU usage exceeds 11%, the CPU priority of processes that consume more than 8% of the CPU resources reduces automatically.
- **Customize CPU Spike Protection.** Lets you customize settings for CPU spike protection.
  - **CPU Usage Limit**. The percentage of CPU usage that any process instance must reach to trigger CPU spike protection. This limit is global across all logical processors in the server, and is determined on an instance-by-process basis. Multiple instances of the same process do not have their CPU usage percentages added when determining CPU spike protection triggers. If a process instance never reaches this limit, CPU spike protection is not triggered. For example, on a Server VDA, in multiple concurrent sessions, suppose there are many iexplore.exe instances. Each instance peaks at around 35% CPU usage for periods of time, so that cumulatively, iexplore.exe is consistently consuming a high percentage of CPU usage. However, CPU spike protection is never triggered unless you set CPU Usage Limit at or below 35%.
  - **Limit Sample Time**. The length of time for which a process must exceed the CPU usage limit before its CPU priority is lowered.
  - **Idle Priority Time**. The length of time for which the CPU priority of the process is lowered. After that time, the priority returns to one of the following:
    * The default level (**Normal**) if the process priority is not specified on the **CPU Priority** tab and the **Enable Intelligent CPU Optimization** option is not selected.
    * The specified level if the process priority is specified on the **CPU Priority** tab, regardless of whether the **Enable Intelligent CPU Optimization** option is selected.
    * A random level depending on the behavior of the process. This case occurs if the process priority is not specified on the **CPU Priority** tab and the **Enable Intelligent CPU Optimization** option is selected. The more frequent the process triggers CPU spike

protection, the lower its CPU priority is.

Enable CPU Core Usage Limit. Limits processes that trigger CPU spike protection to a specified number of logical processors on the machine. Type an integer in the range of 1 through X, where X is the total number of cores. If you type an integer greater than X, WEM limits the maximum consumption of isolated processes to X by default.

- **Limit CPU Core Usage**. Specifies the number of logical processors to which processes that trigger CPU spike protection are limited. In the case of VMs, the value you type limits the processes to the number of logical processors in the VMs rather than in the underlying physical hardware.

Enable Intelligent CPU Optimization. When enabled, the agent intelligently optimizes the CPU priority of processes that trigger CPU spike protection. Processes that repeatedly trigger CPU spike protection are assigned progressively lower CPU priority at launch than processes that behave correctly. Note that WEM does not perform CPU optimization for the following system processes:

- Taskmgr
- System Idle Process
- System
- Svchost
- LSASS
- Wininit
- services
- csrss
- audiodg
- MsMpEng
- NisSrv
- mscorsvw
- vmwareresolutionset

Enable Intelligent I/O Optimization. When enabled, the agent intelligently optimizes the process I/O priority of processes that trigger CPU spike protection. Processes that repeatedly trigger CPU spike protection are assigned progressively lower I/O priority at launch than processes that behave correctly.

Exclude Specified Processes. By default, WEM CPU management excludes all of the most common Citrix and Windows core service processes. You can, however, use this option to **Add** or **Remove** processes from an exclusion list for CPU spike protection by executable name (for example notepad.exe). Typically, antivirus processes would be excluded.

> **Tip:**
>
> - To stop antivirus scanning taking over disk I/O in the session, you can also set a static I/O Priority of Low for antivirus processes, see I/O Management.

> - When processes trigger CPU spike protection, and process CPU priority is lowered, WEM logs a warning each time it lowers the CPU priority of a process. In the Event Log, in Application and Services Logs, 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 let you optimize the CPU priority level of specific processes, so that processes that are contending for CPU processor time do not cause performance bottlenecks. When processes compete with each other, processes with lower priority are served after other process with a higher priority. They are therefore less likely to consume such a large share of the overall CPU consumption.

The process priority you set here establishes the "base priority" for all of the threads in the process. The actual, or "current," priority of a thread might be higher (but is never lower than the base). When a number of processes are running on a computer, the processor time is shared between them based on their CPU priority level. The higher the CPU priority level of a process is, the more the processor time is assigned to it.

> **Note:**
>
> The overall CPU consumption does not necessarily decrease if you set lower CPU priority levels on specific processes. There might be other processes (with higher CPU priority) still affecting percentage CPU usage.

Enable Process Priority. When selected, lets you set CPU priority for processes manually.

To add a process to the CPU priority process list

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

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

   CPU Priority. The "base" priority of all threads in the process. The higher the priority level of a process is, the more the processor time it gets. Select from Realtime, High, Above Normal, Normal, Below Normal, and Low.

To edit a process 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, lets you define how many "logical processors" a process uses. For example, you can restrict every instance of Notepad launched on the VDA to the number of cores defined.

CPU Clamping

CPU clamping prevents processes using more than a specified percentage of the CPU's processing power. WEM "throttles" (or "clamps") that process when it reaches the specified CPU percentage you set. This lets you prevent processes from consuming large amounts of CPU.

> **Note:**
>
> - CPU clamping is a brute force approach that is computationally expensive. To keep the CPU usage of a troublesome process artificially low, it is better to use CPU spike protection, at the same time as assigning static CPU priorities and CPU affinities to such processes. CPU clamping is best reserved for controlling processes that are notoriously bad at resource management, but that cannot stand to be dropped in priority.
> - After you apply a percentage of the CPU's processing power for a process and configure a different percentage for the same process later, select **Refresh Agent Host Settings** for the change to take effect.

The clamping percentage you configure is applied to the total power of any individual CPU in the server, not to any individual core it contains. (In other words, 10% on a quad-core CPU is 10% of the entire CPU, not 10% of one core).

Enable Process Clamping. Enable process clamping.

Add. Add the process by executable name (for example, notepad.exe).

Remove. Remove the highlighted process from the clamping list.

Edit. Edit the values typed for a given process.

> **Tip:**
>
> - When WEM is clamping a process, it adds the process to its watchlist the WEM client initializes. You can verify that a process is clamped by viewing this.
> - You can also verify that CPU clamping is working by looking at process monitor and confirming that CPU consumption never rises above the clamping percentage.

Memory Management

July 9, 2020

These settings allow you to optimize application RAM usage through Workspace Environment Management (WEM).

If these settings are enabled, 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, WEM releases the process's excess RAM to the page file, and optimizes the process for subsequent launches. Usually, an application becomes idle when it is minimized to the task bar.

When applications are restored from the task bar, they initially run in their optimized state but can still go on to consume more 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 RAMs that are freed up are 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 the 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).

WEM does not optimize application RAM usage for the following system processes:

- rdpshell

- wfshell
- rdpclip
- wmiprvse
- dllhost
- audiodg
- msdtc
- mscorsvw
- spoolsv
- smss
- winlogon
- svchost
- taskmgr
- System Idle Process
- System
- LSASS
- wininit
- msiexec
- services
- csrss
- MsMpEng
- NisSrv
- Memory Compression

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.

Citrix Optimizer

November 3, 2020

Citrix optimizer optimizes user environments for better performance. It runs a quick scan of user environments and then applies template-based optimization recommendations. You can optimize user environments in two ways:

- Use built-in templates to perform optimizations. To do so, select a template applicable to the operating system.
- Alternatively, create your own customized templates with specific optimizations you want and then add the templates to Workspace Environment Management (WEM).

Settings

Enable Citrix Optimizer. Controls whether to enable or disable Citrix optimizer.

Run Weekly. If selected, WEM runs optimizations on a weekly basis.

The **Citrix Optimizer** tab displays a list of templates you can use to perform system optimizations. The **Actions** section displays the actions available to you:

- **Add**. Lets you add a custom template.
- **Remove**. Lets you delete an existing custom template. You cannot delete built-in templates.
- **Edit**. Lets you edit an existing template.
- **Preview**. Lets you have an itemized view of the optimization entries that the selected template contains.

To add a custom template:

1. On the **Administration Console > System Optimization > Citrix Optimizer > Citrix Optimizer** tab, click **Add**.
2. In the **New Custom Template** window, click **Browse** to select the applicable template, select the applicable OS from the dropdown, configure groups contained in the template, and then click **OK**.

To edit a template, select the applicable template and then click **Edit**.

To remove a template, select the applicable template and then click **Remove**.

To view details of a template, select the applicable template and then click **Preview**.

Fields and controls

Template Name. The display name of the selected template.

Applicable OSs. A list of operating systems. Select one or more operating systems to which the template applies.

> **Important:**
>
> - You can apply only one template to the same OS.

Groups. The **Available** pane displays a list of grouped optimization entries. The entries are grouped by category. Double-click a group or click the arrow buttons to move the group around.

State. Toggles the template between enabled and disabled states. If disabled, the agent does not process the template, and WEM does not run optimizations associated with the template.

Changes to Citrix optimizer settings take some time to take effect, depending on the value that you specified for the **SQL Settings Refresh Delay** option on the **Advanced Settings > Configuration > Service Options** tab.

For the changes to take effect immediately, navigate to the context menu of the **Administration > Agents > Statistics** tab and then select **Process Citrix Optimizer**.

> **Tip:**
>
> - New changes might fail to take effect immediately. We recommend that you select **Refresh Agent Host Settings** before you select **Process Citrix Optimizer**.

Policies and Profiles

July 31, 2020

These settings let you replace user GPOs and configure user profiles.

- Environmental Settings
- Microsoft USV Settings
- Citrix Profile Management Settings

Environmental Settings

October 21, 2020

These options modify the user's environmental settings. Some of the options are processed at logon, while some others can be refreshed in session with the agent refresh feature.

Start menu

These options modify the user's Start menu.

Process Environmental Settings. This check box toggles whether the agent processes environmental settings. If it is cleared, no environmental settings are processed.

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

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

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

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

Desktop

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

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

Windows Explorer

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

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

Hide Specified Drives from Explorer. If enabled, the listed drives are hidden from the user's My Computer menu. They are still accessible if browsed to directly.

Restrict Specified Drives from Explorer. If enabled, the listed drives are blocked. Neither the users nor their applications can access them.

Control Panel

Hide Control Panel. This option is enabled by default to secure the user environment. If disabled, the users have access to their Windows control panel.

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

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

See Common Control Panel applets along with their canonical names.

Known Folders Management

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

SBC/HVD Tuning

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

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

Disable Drag Full Windows. Disables dragging maximized windows.

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

Disable Cursor Blink. Disables the cursor flickering effect.

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

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

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

Set Cursor Blink Rate. Changes the cursor blink rate.

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

August 11, 2020

> **Note:**
>
> Some options work only with specific versions of Profile Management. Consult the Profile Management documentation for details.

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

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

Main Citrix Profile Management Settings

These settings control the main Citrix Profile Management parameters.

Enable Profile Management Configuration. Toggles whether the agent processes Citrix Profile Management settings. If cleared, none of the Profile Management settings are processed.

Enable Profile Management. Toggles whether 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. Lets you 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. Lets you 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. Lets you specify the path to the user store directory.

Migrate user store. Lets you specify the path to the folder where the user settings (registry changes and synchronized files) were saved. Type the user store path that you previously used. Use this option along with the **Set path to user store** option.

Enable active write back. If enabled, profiles are written back to the user store during the user's session. 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 Container Settings

These options control Profile Management profile container settings.

Enable Profile Container. If enabled, Profile Management maps the listed folders to the profile disk stored on the network, thus eliminating the need to save a copy of the folders to the local profile. Specify at least one folder to include in the profile container.

Enable Folder Exclusions for Profile Container. If enabled, Profile Management excludes the listed folders from the profile container. Specify at least one folder to exclude from the profile container.

Enable Folder Inclusions for Profile Container. If enabled, Profile Management keeps the listed folders in the profile container when their parent folders are excluded. Folders on this list must be subfolders of the excluded folders. This means that you must use this option in combination with the **Enable Folder Exclusions for Profile Container** option. Specify at least one folder to include in the profile container.

Profile Handling

These settings control Profile Management profile handling.

Delete local cached profiles on logoff. If enabled, locally cached profiles are deleted when the user logs off.

Set delay before deleting cached profiles. Lets you specify a delay (in seconds) before cached profiles are deleted at log-off.

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

Automatic migration of existing application profiles. If enabled, existing application profiles are migrated automatically. Profile Management performs the migration when a user logs on and there are no user profiles in the user store.

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

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

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

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

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

Advanced Settings

These options control advanced Profile Management settings.

Set number of retries when accessing locked files. Configures the number of times the Agent retries 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, deletes local copies of redirected folders.

Disable automatic configuration. If enabled, dynamic configuration is disabled.

Log off user if a problem is encountered. If enabled, users are logged off rather than switched to a temporary profile if a problem is encountered.

Customer experience improvement program. If enabled, Profile Management uses the Customer Experience Improvement Program (CEIP) to help improve the quality and performance of Citrix products by collecting anonymous statistics and usage information. For more information on the CEIP, see About the Citrix Customer Experience Improvement Program (CEIP).

Enable search index roaming for Microsoft Outlook users. If enabled, the user-specific Microsoft Outlook offline folder file (*.ost) and Microsoft search database are roamed along with the user profile. This improves the user experience when searching mail in Microsoft Outlook.

Outlook search index database – backup and restore. If enabled, Profile Management automatically saves a backup of the last known good copy of the search index database. When there is a cor-

ruption, Profile Management reverts to that copy. As a result, you no longer need to manually reindex the database when the search index database becomes corrupted.

Enable multi-session write-back for FSLogix Profile Container. If enabled, Profile Management saves changes in multi-session scenarios for FSLogix Profile Container. If the same user launches multiple sessions on different machines, changes made in each session are synchronized and saved to FSLogix Profile Container.

Log Settings

These options control Profile Management logging.

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

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

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

Set Path to Log File. Lets you specify the location at which the log file is created.

Registry

These options control Profile Management registry settings.

NTUSER.DAT Backup. If selected, Profile Management maintains a last known good backup of the NTUSER.DAT file. If Profile Management detects corruption, it uses the last known good backup copy to recover the profile.

Enable Default Exclusion List. Default list of registry keys in the HKCU hive that are not synchronized to the user's profile. If selected, registry settings which are selected in this list are forcibly excluded from Profile Management profiles.

Enable Registry Exclusions. Registry settings in this list are forcibly excluded from Profile Management profiles.

Enable Registry Inclusions. Registry settings in this list are forcibly included in Profile Management profiles.

File System

These options control file system exclusions for Profile Management.

Enable Logon Exclusion Check. If enabled, configures what Profile Management does when a user logs on when a profile in the user store contains excluded files or folders. (If disabled, the default behavior is **Synchronize excluded files or folders**). You can select one of the following behaviors in the list:

Synchronize excluded files or folders (default). Profile Management synchronizes these excluded files or folders from the user store to local profile when a user logs on.

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

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

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

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

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

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

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

Cleanse Profiles. Cleans the selected profiles per the folder exclusion settings.

Scan Profiles Folder. Scans the specified folder with the specified recursion settings to find user profiles and then displays all profiles found.

Profiles Root Folder. The root folder of your user profiles. You can also browse to this folder if you like.

Search Recursivity. Controls how many levels of recursion the user profile search goes through.

Synchronization

These options control Profile Management synchronization settings.

Enable Directory Synchronization. If enabled, the listed folders are synchronized to the user store.

Enable File Synchronization. If enabled, the listed files are synchronized to the user store, ensuring that users always get the most up-to-date versions of the files. If files have been modified in more than one session, the most up-to-date files are kept in the user store.

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

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

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

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

Streamed User Profiles

These options control streamed user profile settings.

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

Always cache. If enabled, files of the specified size (in MB) or larger will always be cached.

Set timeout for pending area lock files: Frees up files so they are written back to the user store from the pending area after the specified time if the user store remains locked when a server becomes unresponsive.

Set streamed user profile groups. This list determines which user groups streamed profiles are used for.

Enable Profile Streaming Exclusion List - Directories. If selected, Profile Management does not stream folders in this list, and all the folders are fetched immediately from the user store to the local computer when users log on.

Cross-Platform Settings

These options control cross-platform settings.

Enable cross-platform settings. If disabled, none of the settings in this section are processed.

Set cross-platform settings groups. Lets you specify the user groups for which cross-platform profiles are used.

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

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

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

Security

September 21, 2020

These settings let you control user activities within Workspace Environment Management.

Application Security

> **Important:**
>
> To control which applications 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. When a user runs an app that violates an AppLocker rule, the app is allowed to run and the information about the app is added to the AppLocker event log.

To import AppLocker rules

You can import rules 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 is added to the list.

To edit rules

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

To delete rules

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

To back up application security rules

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

To restore application security rules

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

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

1. In the ribbon, click **Restore** to start the restore wizard.
2. Select Security settings, then click **Next** twice.
3. In **Restore from folder**, browse to the folder containing the backup file.
4. Select **AppLocker Rule Settings**, then click **Next**.
5. Confirm whether you want to restore rule assignments or not:

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

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 BlackLists

These settings allow you to blacklist specific processes.

Enable Process Blacklist. This enables process blacklisting. You must add processes by using their 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. You must add processes by using their 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

July 31, 2020

Use these pages to specify the users, computers, groups, and organizational units you want Workspace Environment Management to manage.

> **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

October 12, 2020

These options let you configure the Transformer feature. Transformer lets agents connect as web or application launchers that redirect users to the configured remote desktop interface. Use Transformer to convert any Windows PC into a high performance thin client using a fully reversible “kiosk” mode.

General

General Settings

These settings control the appearance and basic settings for Transformer.

Enable Transformer. If enabled, Agent Hosts connected to this site automatically goes into *kiosk mode*. While in kiosk mode, the Agent Host becomes a web or application launcher that redirects the user to the configured remote desktop interface. The user environment is locked down and the user is only allowed to interact with the agent. If you disable this option, none of the settings in either the **General** or **Advanced** pages are processed.

Web Interface URL. This URL is used as the web front end for the user’s virtual desktop. This is the access URL for your Citrix Virtual Apps or Citrix Virtual Desktops environment.

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

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

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

Show Navigation Buttons. If enabled, the “Forward”, “Back”, and “Home” web navigation buttons appear in the Agent kiosk window. “Home” sends users back to the web interface URL defined above.

Display Clock. If enabled, displays a clock in the Transformer UI.

Show 12 Hour Clock. If enabled, displays a 12-hour clock (AM/PM). By default, the Transformer clock is a 24-hour clock.

Enable Application Panel. If enabled, displays a panel with the user’s applications as assigned in Workspace Environment Management.

Auto-Hide Application Panel. If enabled, the application panel auto-hides itself when not in use.

Change Unlock Password. Allows you to specify the password that can be used to unlock the user’s environment by pressing **Ctrl+Alt+U**. This is designed to allow administrators and to support agents to troubleshoot the user environment without restrictions.

Site Settings

Enable Site List. If enabled, adds a list of URLs to the kiosk interface.

Tool Settings

Enable Tool List. If enabled, adds a list of tools to the kiosk interface.

Advanced

Process Launcher

These options allow you to turn the Workspace Environment Management Agent kiosk mode into a process launcher rather than presenting a web interface.

Enable Process Launcher. If enabled, puts the Workspace Environment Management agent into process launcher mode. While in process launcher mode, the Workspace Environment Management agent launches the process specified in **Process Command Line**. If terminated, the process is relaunched.

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

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

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

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

Enable Microsoft RDS Mode. If enabled, allows the process launcher to monitor the virtual applications or desktops running on a user's machine in Microsoft Remote Desktop Services (RDS) mode and to run **End of Session Options** when they are all closed.

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

Advanced & Administration Settings

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

this forces the kiosk window to run in IE7 compatibility mode.

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

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

Fix SSL Sites. If enabled, hides SSL warnings entirely.

Hide Kiosk While in Citrix Session. If enabled, hides the Citrix Workspace Environment Management Agent kiosk while the users are connected to their Citrix sessions.

Always Show Admin Menu. If enabled, always displays the kiosk admin menu – this gives all users access to the kiosk admin menu.

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

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

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

Lock Citrix Desktop Viewer. If enabled, switches the desktop viewer to a locked down mode. This is equivalent to the lockdown that happens when Citrix Workspace app for Windows Desktop Lock is installed. This allows better integration with local applications. This option works only when all of the following conditions are met:

- The user logging on to the agent host is not a member of the administrators group.
- The **Enable Transformer** option on the **General Settings** tab is enabled.
- The **Enable Autologon Mode** option on the **Logon/Logoff & Power Settings** tab is enabled.

Hide Display Settings. If enabled, hides **Display** under **Settings** in the Transformer UI.

Hide Keyboard Settings. If enabled, hides **Keyboard** under **Settings** in the Transformer UI.

Hide Mouse Settings. If enabled, hides **Mouse** under **Settings** in the Transformer UI.

Hide Volume Settings. If enabled, hides **Volume** under **Settings** in the Transformer UI.

Hide Client Details. If enabled, hides **Client Details** under the exclamation mark icon in the Transformer UI. From **Client Details**, you can see information such as the version number.

Disable Progress Bar. If enabled, hides the embedded web browser progress bar.

Hide Windows Version. If enabled, hides **Windows Version** under the exclamation mark icon in the Transformer UI.

Hide Home Button. If enabled, hides the Home icon in the menu in the Transformer UI.

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 front end specified in the General Settings page is logged off when the user's desktop session is launched.

End of Session Options. Allows you to specify which action the agent takes with the environment that it is running in when the user ends their session.

Shut Down at Specified Time. If enabled, the agent automatically shuts off the environment that it is running in at the specified local time.

Shut Down When Idle. If enabled, the agent automatically shuts off the environment that it is running in after running idle (no user input) for the specified length of time.

Don't Check Battery Status. In Transformer use cases, the agent checks battery status and alerts the user if the battery is running low. If enabled, the agent does not perform this check.

Advanced settings

October 29, 2020

These settings modify how and when the agent processes actions.

Configuration

These options control basic agent behavior.

Main Configuration

Agent Actions. These settings determine whether the agent processes actions configured in the Actions tab. These settings apply 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 control how the agent service behaves on endpoints.

Launch Agent on Logon. Controls whether the agent runs on logon.

Launch Agent on Reconnect. Controls whether the agent runs when a user reconnects to a machine where the agent is running.

Launch Agent for Admins. Controls whether the agent runs when a user is an administrator.

Agent Type. Controls whether a user is presented with a user interface (UI) or a command-line prompt (CMD) when interacting with the agent.

Enable (Virtual) Desktop Compatibility. Ensures that the agent is compatible with desktops where it is running. This setting is necessary for the agent to launch when the user logs on to a session. If you have users on physical or VDI desktops, select this option.

Execute Only CMD Agent in Published Applications. If enabled, the agent launches in CMD mode rather than in UI mode in published applications. CMD mode displays a command prompt instead of an agent splash screen.

Cleanup Actions

Options present on this tab control whether the agent deletes the shortcuts or other items (network drives and printers) when the agent refreshes. If you assign actions to a user or user group, you might find that you can also control the creation of the shortcuts or items. You can do so by configuring the options for the actions in the **Assigned** pane of the **Assignments > Action Assignment > Action Assignment** tab. Workspace Environment Management processes these options according to a specific priority:

1. The options present on the **Cleanup Actions** tab
2. The options configured for the assigned actions in the **Assigned** pane

For example, suppose you have enabled the **Create Desktop** option for the assigned application in the **Assigned** pane, and the application shortcut is already created on the desktop. The shortcut is still on the desktop when the agent refreshes, even though you enabled the **Delete Desktop Shortcuts** option on the **Cleanup Actions** tab.

Shortcut Deletion at Startup. The agent deletes all shortcuts of the selected types when it refreshes.

Delete Network Drives at Startup. If enabled, the agent deletes all network drives whenever it refreshes.

Delete Network Printers at Startup. If enabled, the agent deletes all network printers whenever it refreshes.

Preserve Auto-created Printers. If enabled, the agent does not delete auto-created printers.

Preserve Specific Printers. If enabled, the agent does not delete any of the printers in this list.

Agent Options

These options control the agent settings.

Enable Agent Logging. Enables the agent log file.

Log File. The log file location. By default, this is the profile root of the logged-in user.

Debug Mode. This enables verbose logging for the agent.

Enable Offline Mode. If disabled, the agent does not fall back on its cache when it fails to connect to the infrastructure service.

Use Cache Even When Online. If enabled, the agent always reads its settings and actions from its cache (which is built whenever the agent service cycles).

Use Cache to Accelerate Actions Processing. If enabled, the agent processes actions by retrieving relevant settings from the agent local cache instead of from the infrastructure services. Doing so speeds up the processing of actions. By default, this option is enabled. Disable this option if you want to revert to the previous behavior.

> **Important:**
>
> - The agent local cache is synchronized with the infrastructure services on a periodic basis. Therefore, changes to action settings take some time to take effect, depending on the value that you specified for the **Agent Cache Refresh Delay** option (on the **Advanced Settings > Configuration > Service Options** tab).
> - To reduce delays, specify a lower value. For the changes to take effect immediately, navigate to the **Administration > Agents > Statistics** tab, right-click the applicable agent, and then select **Refresh Cache** in the context menu.

Refresh Environmental Settings. If enabled, the agent triggers a refresh of user environment settings when an agent refresh occurs. For information about environment settings, see Environmental Settings.

Refresh System Settings. If enabled, the agent triggers a refresh of Windows system settings (for example, Windows Explorer and Control Panel) when an agent refresh occurs.

Refresh When Environmental Settings Change. If enabled, the agent triggers a Windows refresh on endpoints when any environment setting changes.

Refresh Desktop. If enabled, the agent triggers a refresh of desktop settings when an agent refresh occurs. For information about desktop settings, see Desktop.

Refresh Appearance. If enabled, the agent triggers a refresh of Windows theme and desktop wallpaper when an agent refresh occurs.

Asynchronous Printer Processing. If enabled, the agent processes printers asynchronously 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 15000 milliseconds.

Directory Services Timeout. The timeout value for directory services on the Agent Host machine, after which the agent uses its own internal cache of user group associations. The default value is 15000 milliseconds.

Network Resources Timeout. The timeout value for resolving network resources (network drives or file/folder resources located on the network), after which the agent considers the action has failed. The default value is 500 milliseconds.

Agent Max Degree of Parallelism. The maximum number of threads the agent can use. Default value is 0 (as many threads as physically allowed by the processor), 1 is single-threaded, 2 is dual-threaded, and so on. Usually, this value does not need changing.

Enable Notifications. If enabled, the agent displays notification messages on the agent host when the connection to the infrastructure service is lost or restored. Citrix recommends that you do not enable this option on poor-quality network connections. Otherwise, connection state change notifications might appear frequently on the endpoint (agent host).

Advanced Options

Enforce Execution of Agent Actions. If these settings are enabled, the Agent Host always refreshes those actions, even if no changes have been made.

Revert Unassigned Actions. If these settings are enabled, the Agent Host deletes any unassigned actions when it next refreshes.

Automatic Refresh. If enabled, the Agent Host refreshes automatically. By default, the refresh delay is 30 minutes.

Reconnection Actions

Action Processing on Reconnection. These settings control what actions the Agent Host processes upon reconnection to the user environment.

Advanced Processing

Filter Processing Enforcement. If enabled, these options force the Agent Host to reprocess filters at every refresh.

Service Options

These settings configure the Agent Host service.

Agent Cache Refresh Delay. This setting controls how long the Citrix WEM Agent Host Service waits to refresh its cache. The refresh keeps the cache in sync with the WEM service database. The default is 30 minutes.

SQL Settings Refresh Delay. This setting controls how long the Citrix WEM Agent Host Service waits to refresh its SQL connection settings. The default is 15 minutes.

Agent Extra Launch Delay. This setting controls how long the Citrix WEM Agent Host Service waits to launch the agent host executable.

> **Tip:**
>
> In scenarios where you want the agent host to complete the necessary work first, you can specify how long the agent application launcher (VUEMAppCmd.exe) waits. VUEMAppCmd.exe ensures that the agent host finishes processing an environment before Citrix Virtual Apps and Desktops published applications are started. To specify the wait time, configure the VUEMAppCmd extra sync delay setting, available in the Agent Host Configuration group policy. For more information, see Install and configure the WEM agent.

Enable Debug Mode. This enables verbose logging for all Agent Hosts connecting to this site.

Bypass ie4uinit Check. By default, the Citrix WEM Agent Host Service awaits ie4uinit to run before launching the Agent Host executable. This setting forces the Agent Host service to not wait for ie4uinit.

Agent Launch Exclusions. If enabled, the Citrix WEM Agent Host is not launched for any user belonging to the specified user groups.

Console Settings

Forbidden Drives. Any drive letter added to this list is excluded from the drive letter selection when assigning a drive resource.

StoreFront

Use this tab to add a StoreFront store to Workspace Environment Management. You can then navigate to the **Actions > Applications > Application List** tab to add applications available in those stores. Doing so lets you assign published applications as application shortcuts to endpoints. For more information, see Applications. In Transformer (kiosk) mode, assigned StoreFront application actions appear on the **Applications** tab. For more information about StoreFront stores, see StoreFront documentation.

To add a store

1. Click **Add**.
2. Enter details in the **Add Store** dialog, then click **OK**. The store is saved in your configuration set.

Store URL. The URL of the store on which you want to access resources using Workspace Environment Management. The URL must be specified in the form http[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.

> **Important:**
>
> - The store URL you use must be directly accessible from external networks, and must not be behind any solutions such as Citrix ADC.
> - This feature does not work with StoreFront using multifactor authentication.

Description. Optional text describing the store.

To edit a store

Select a store in the list and click **Edit** to change the store URL or description.

To remove a store

Select a store in the list and click **Remove** to remove a store from your configuration set.

To apply changes

Click **Apply** to apply store settings immediately to your agents.

Agent Switch

Options present on this tab let you switch from the on-premises agent to the service agent.

> **Important:**
>
> Agent switch works at a configuration set level. The switch operation you perform affects only the agents in the configuration set.

Switch to Service Agent. If enabled, the agent switches from the on-premises agent to the service agent. You can then specify Citrix Cloud Connectors to which the agent connects. This is useful when you want to migrate your existing on-premises deployment to the WEM service.

> **Warning:**
>
> Enable this option only if you want to move your on-premises deployment to the WEM service.

> This move cannot be reversed through the WEM administration console.

Configure Citrix Cloud Connectors. Lets you configure the Citrix Cloud Connectors by typing the FQDN or IP address of the Cloud Connector. Click **Add** to add one Cloud Connector at a time. To ensure high service availability, Citrix recommends that you install at least two Cloud Connectors in each resource location. Therefore, you need to configure at least two Citrix Cloud Connectors.

Skip Citrix Cloud Connector Configuration. Select this option if you want to configure Citrix Cloud Connectors using Group Policy.

> **Important:**
>
> It might take some time for the agent switch settings to take effect, depending on the **SQL Settings Refresh Delay** setting you configured on the **Advanced Settings > Configuration > Service Options** tab.

The agent might fail to connect to the WEM service after you switch from the on-premises agent to the service agent, and you might want to roll back. To do so, use the AgentConfigurationUtility.exe command line; for example:

- `<WEM agent installation folder path>AgentConfigurationUtility.exe switch -o --server <server name> --agentport <port number> --syncport <port number>`
- `<WEM agent installation folder path>AgentConfigurationUtility.exe switch -o --server <server name>`
- `<WEM agent installation folder path>AgentConfigurationUtility.exe switch --usegpo -o`

UI Agent Personalization

These options let you personalize the look and feel of the agent in UI mode. These options determine how the UI agent appears in the user environment.

> **Note:**
>
> These options apply only to the agent in UI mode. They do not apply to the agent in CMD mode.

UI Agent Options

These settings let you customize the appearance of the session agent (in UI mode only) in the user's environment.

Custom Background Image Path. If specified, displays a custom splash screen instead of the Citrix Workspace Environment Management logo when the agent launches or refreshes. The image must be

accessible from the user environment. We recommend that you use a 400*200 px .bmp file.

Loading Circle Color. Lets you modify the color of the loading circle to fit your custom background.

Text Label Color. Lets you modify the color of the loading text to fit your custom background.

UI Agent Skin. Lets you select a preconfigured skin you want to use for dialogs that open from the UI agent. For example, the **Manage applications** dialog and the **Manage Printers** dialog. **Note**: This setting does not change the splash screen.

Hide Agent Splashscreen. If enabled, hides the splash screen when the agent is loading or refreshing. This setting does not take effect the first time the agent refreshes.

Hide Agent Icon in Published Applications. If enabled, published applications do not display the agent icon.

Hide Agent Splashscreen in Published Applications. If enabled, hides the agent splash screen for published applications where the agent is running.

Only Admins Can Close Agent. If enabled, only administrators can exit the agent. As a result, the **Exit** option in the agent menu is disabled on endpoints for non-administrators.

Allow Users to Manage Printers. If enabled, the **Manage Printers** option in the agent menu is available to users on endpoints. Users can click the option to open the **Manage printers** dialog to configure a default printer and to modify print preferences. By default, the option is enabled.

Allow Users to Manage Applications. If enabled, the **Manage Applications** option in the agent menu is available to users on endpoints. Users can click the option to open the **Manage applications** dialog and configure the following options. By default, the option is enabled.

- **Desktop**. Adds the application shortcut to the desktop.
- **Start Menu**. Creates the application shortcut in the Start menu folder.
- **QuickLaunch**. Adds the application to the quick launch toolbar.
- **Taskbar (P)**. Creates the application shortcut in the taskbar.
- **Start Menu (P)**. Pins the application to the Start menu.

> **Note:**
>
> Shortcuts created in self-healing mode cannot be deleted using this menu.
> The QuickLaunch option is available only in Windows XP and Windows Vista.

Prevent Admins From Closing Agent. If enabled, administrators cannot exit the agent.

Enable Applications Shortcuts. If enabled, controls whether to display the **My Applications** option in the agent menu. Users can run applications from the **My Applications** menu. By default, the option is enabled.

Disable Administrative Refresh Feedback. If enabled, this option does not display a notification in the user environment when an administrator forces an agent refresh through the administration console.

Allow Users to Reset Actions. Controls whether to display the **Reset Actions** option in the agent menu. By default, the option is disabled. The **Reset Actions** option lets current users specify what actions to reset in their environment. After a user selects **Reset Actions**, the **Reset actions** dialog appears. In the dialog, the user can have granular control over what to reset. The user can select applicable actions and then click **Reset**. Doing so purges the corresponding action-related registry entries.

> **Note:**
>
> - The following two options are always available in the agent menu: **Refresh** and **About**. The **Refresh** option triggers an immediate update of the WEM agent settings. As a result, settings configured in the administration console take effect immediately. The **About** option opens a dialog displaying version details about the agent in use.

Helpdesk Options

These options control help desk functionalities available to users on endpoints.

Help Link Action. Controls whether the **Help** option is available to users on endpoints and what happens when a user clicks it. Type a website link through which users can ask for help.

Custom Link Action. Controls whether to display the **Support** option in the agent menu and what happens when a user clicks it. Type a website link through which users can access support-related information.

Enable Screen Capture. Controls whether to display the **Capture** option in the agent menu. Users can use the option to open a screen capture tool. The tool provides the following options:

- **New capture**. Takes a screenshot of errors in the user environment.
- **Save**. Saves the screenshot.
- **Send to support**. Sends the screenshot to support staff.

Enable Send to Support Option. Controls whether to display the **Send to support** option in the screen capture tool. If enabled, users can use the option to send screenshots and log files directly to the specified support email address, in the specified format. This setting requires a working, configured email client.

Custom Subject. If enabled, lets you specify an email subject template that the screen capture tool uses to send support emails.

Email Template. Lets you specify an email content template that the screen capture tool uses to send support emails. This field cannot be empty.

> **Note:**
>
> For a list of hash-tags that you can use in the email template, see Dynamic tokens.
> Users are only presented with the option to enter a comment if the **##UserScreenCaptureComment## hash-tag** is included in the email template.

Use SMTP to Send Email. If enabled, sends a support email using SMTP instead of MAPI.

Test SMTP. Tests the SMTP settings as typed above to verify that they are correct.

Power Saving

Shut Down At Specified Time. If enabled, lets the agent automatically shuts down the machine where it is running at the specified time. The time is based on the agent time zone.

Shut Down When Idle. If enabled, lets the agent automatically shut down the machine where it is running after the machine remains idle (no user input) for the specified length of time.

Administration

October 15, 2020

The **Administration** pane consists of the following:

- **Administrators**. Lets you define Workspace Environment Management administrators (users or groups) and give them permissions to access configuration sets through the administration console.
- **Users**. Lets you view user statistics.
- **Agents**. Lets you view agent statistics and perform administrative tasks such as refreshing cache, resetting settings, and uploading statistics.
- **Logging**. Lets you view administrative activities in Workspace Environment Management. You can use the logs to:
  - Diagnose and troubleshoot problems after configuration changes are made.
  - Assist change management and track configurations.
  - Report administrative activities.

Administrators

These options let you define Workspace Environment Management administrators (users or groups) and give them permissions to access configuration sets through the administration console.

Configured Administrators List

A list of configured administrators showing their permission level (**Full Access**, **Read Only** or **Granular Access**, see details below). You can use **Find** to filter the list by name or ID against a text string.

To add an administrator

1. Use the context menu **Add** command.
2. Enter details in the Select Users or Groups dialog, then click **OK**.

Name. The name of the user or group you are currently editing.

Description. Additional information about the user or group.

Global Administrator. Select to specify that the selected user/group is a Global Administrator. Clear to specify that the selected user/group is a Site Administrator. Global Administrators have their permissions applied to all sites (configuration sets). Site Administrators have their permissions configured on a per-site basis.

Permissions. This allows you to specify one of the following levels of access to the selected user/-group. **Note**: Administrators can only view settings which they have access to.

Full Access administrators have full control over every aspect of the specified sites (configuration sets). Only Global Administrators with Full Access can add/delete Workspace Environment Management administrators. Only Global Full Access and Global Read Only administrators can see the **Administration** tab.

Read Only administrators can view the entire console, but cannot modify any settings at all. Only Global Full Access and Global Read Only administrators can see the **Administration** tab.

Granular Access indicates that the administrator has one or more of the following permission sets:

Action Creators can create and manage actions.

Action Managers can create, manage, and assign actions. They cannot edit or delete actions.

Filter Managers can create and manage conditions and rules. Rules that are in use on assigned applications cannot be edited or deleted by Filter Managers.

Assignment Managers can assign resources to users or groups.

System Utilities Managers can manage the System Utilities settings (CPU, RAM and process management).

Policies and Profiles Managers can manage Policies and Profiles settings.

Configured Users Managers can add, edit, and remove users or groups from the configured users list. Users or groups with assigned actions cannot be edited or deleted by Configured Users Managers.

Transformer Managers can manage Transformer settings.

Advanced Settings Managers can manage advanced settings (enabling or disabling action processing, cleanup actions, and so on).

Security Managers can access all controls in the Security tab.

State. This controls whether the selected user/group is enabled or disabled. When disabled, the user/-group is not considered to be a Workspace Environment Management administrator and cannot use the administration console.

Type. This field is read only and indicates whether the selected entity is a user or a group.

If the **Global Administrator** is cleared, the following controls are enabled:

Site Name. All Workspace Environment Management sites (configuration sets) belonging to the database this infrastructure service is connected to.

Enabled. Select to enable this administrator for the specified Workspace Environment Management site (configuration set). When disabled, the user/group is not considered to be an administrator for that site and cannot access it.

Permissions. Select a permission level for the selected user/group for each Workspace Environment Management site (configuration set) attached to this infrastructure service.

Users

This page displays statistics about your Workspace Environment Management deployment.

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.

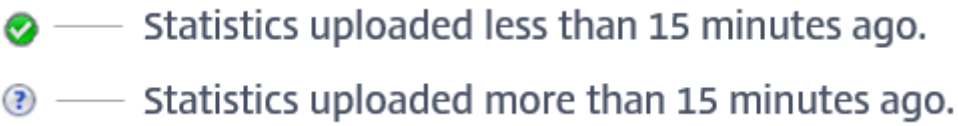
Statistics

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.



> **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.

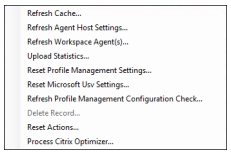
If the status checks do not reflect your experience or if they do not detect the issues you are having, contact Citrix Technical Support.

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 local cache (an agent-side replica of the WEM configuration database). Refreshing the cache synchronizes the agent local cache with the infrastructure services.

Refresh Agent Host Settings. Applies the agent service settings. Those settings include advanced settings, optimization settings, transformer settings, and other non-user assigned settings.

Refresh Workspace Agents. Applies the user-assigned actions to the WEM agents. Those actions include network drives, printers, applications, and more.

> **Important:**
>
> - The **Refresh Workspace Agents** option works only with the agents in UI mode that are automatically launched (not launched by end users or by using scripts). The option does not work with the agents in CMD mode.
> - Not all settings can be refreshed. Some settings (for example, environment settings and group policy settings) are applied only on startup or logon.

Upload Statistics. Uploads statistics to the infrastructure service.

Reset Profile Management Settings. Clears the registry cache and updates the associated configuration settings. If Profile Management Settings are not applied to your agent, click **Reset Profile Management Settings**. You might need to click **Refresh** for this option to become available.

> **Note:**
>
> If the settings are not applied to the agent after configuring **Reset Profile Management Settings** from the WEM administration console, see CTX219086 for a workaround.

Reset Microsoft USV Settings. Clears the registry cache and updates the associated configuration settings. If Microsoft USV Settings are not applied to your agent, click **Reset Microsoft Usv Settings**, and then click **Refresh**.

Refresh Profile Management Configuration Check. Performs status checks on your agent host(s) to determine whether Profile Management is configured optimally.

Delete Record. Enables deletion of the agent record from the database. If the agent is still active, this option is grayed out.

Reset Actions. Lets you reset all actions you assigned by purging all action-related registry entries on the applicable machine.

Process Citrix Optimizer. Applies the settings to the agents so that changes to Citrix optimizer settings take effect immediately.

Registrations

This page shows the registration status of the Workspace Environment Management agents recorded in the database.

> **Important:**
>
> Agents must register only with one configuration set.

The following information is reported:

Machine Name. Name of computer on which the agent is running.

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.

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

Dynamic tokens

July 9, 2020

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)!

#Mod(string,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 used in the processing of Workspace Environment Management items. The following example illustrates how you use hash-tags:

To write to an **.ini** file, you can use **%UserName%** in the **.ini** file's path and Workspace Environment Management processes it and expands the final directory. However, assessing the value which Workspace Environment Management writes in the **.ini** itself is more complicated: you may want to write **%UserName%** literally, or write the expanded value.

To increase flexibility, **##UserName##** exists as a hash-tag, so that using **%UserName%** for a value writes it literally and **##UserName##** writes the expanded value.

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 organizational unit (OU) structures, WEM replaces the **[UserParentOU:level]** value with the related Active Directory OU name. The Active Directory path is the complete user path (LDAP) in Active Directory and [UserParentOU:level] is a subset of it.

For example, suppose you want to build a network drive for an OU to which the users belong. You can use the dynamic token [UserParentOU:level] in the network drive path to resolve the users' OU dynamically. There are two ways to use the dynamic token:

- Use the [UserParentOU:level] dynamic token directly in the network drive path. For example, you can use the following path: `\\Server\Share\[UserParentOU:0]\`.
- Set an environment variable called OU, and then set its value to [UserParentOU:0]. You can then map the drive as `\\Server\Share\\%OU%\`.

> **Note:**
>
> - 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

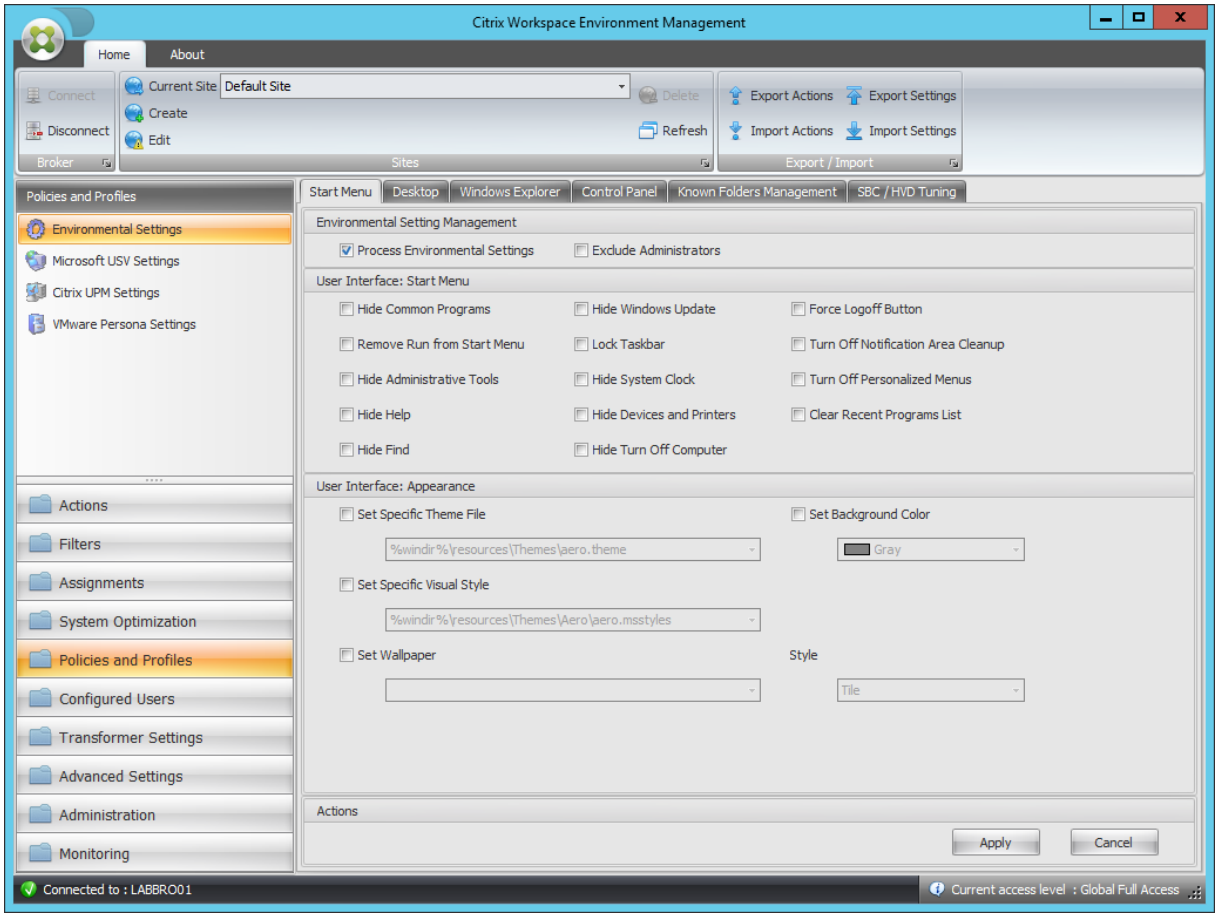
For Active Directory Attribute Match, the dynamic token is [ADAttribute:attrName].
There is no dynamic token available for Active Directory Group Match because that condition type is used to check a group membership.

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##.

Environmental Settings registry values

June 2, 2020

This article describes the registry values associated with Environmental Settings in Workspace Environment Management.



Hide Common Programs	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoCommonGroups
Value Type	DWORD
Enabled Value	1
Disabled Value	0

Hide Common Programs	
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
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

Hide System Clock	
Enabled Value	1
Disabled Value	0
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

Force Logoff Button	
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

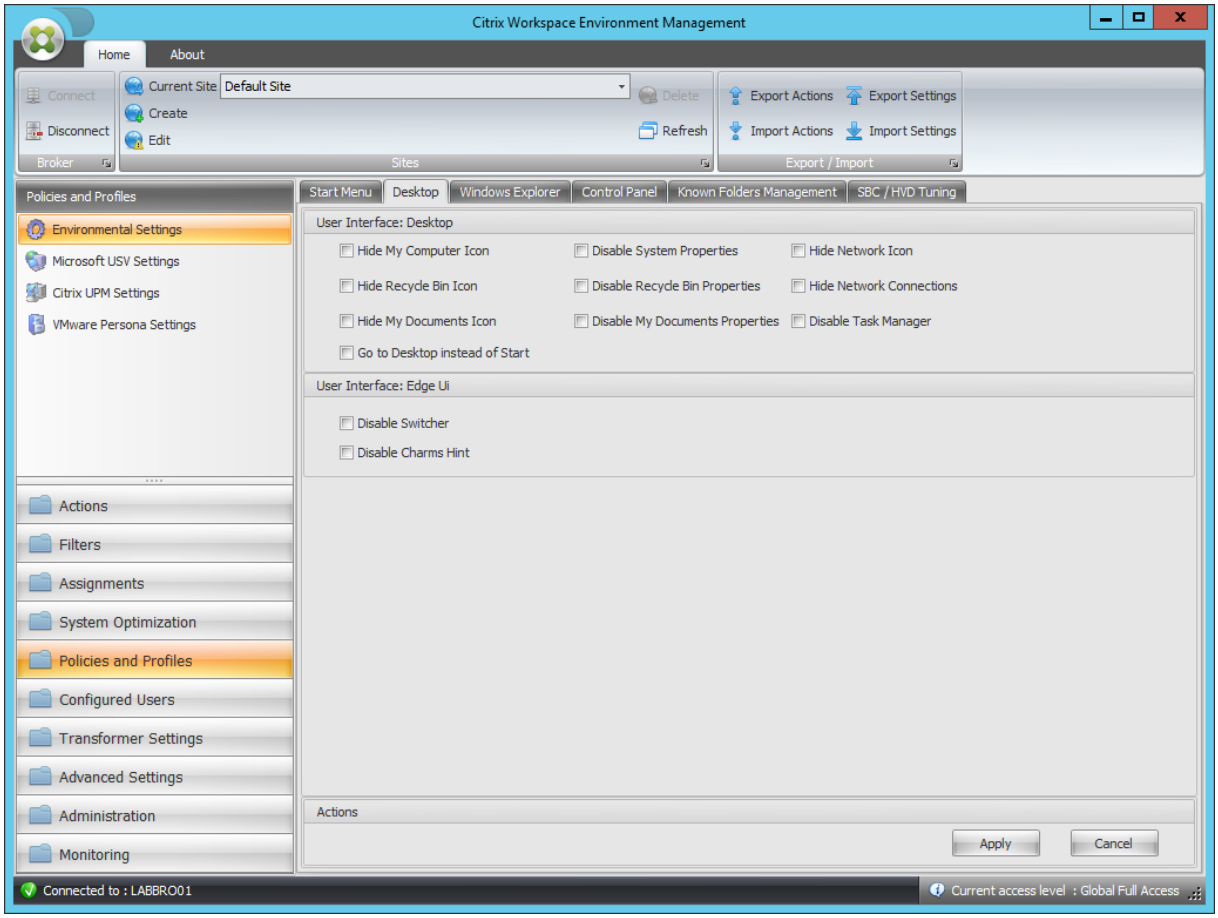
Set Specific Theme File	
Parent Key	HKCU\Software\Policies\Microsoft\Windows\Personalization
Value Name	ThemeFile
Value Type	REG_SZ
Enabled Value	Path specified in console
Disabled Value	Value is absent
Processing	Service at logon

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

Set Wallpaper	
Value Type	REG_SZ
Enabled Value	Path specified in console
Disabled Value	Value is absent
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



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

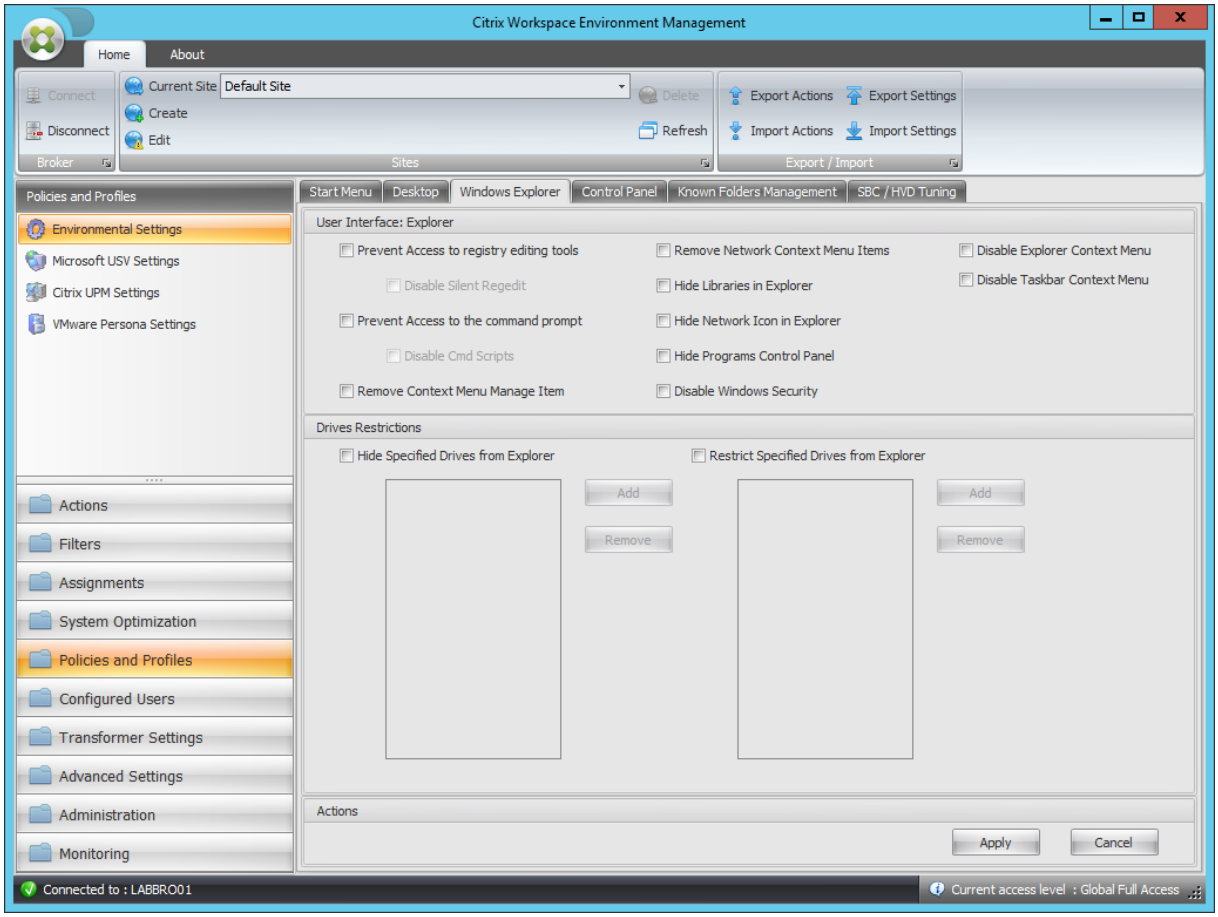
Hide Network Connections	
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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



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

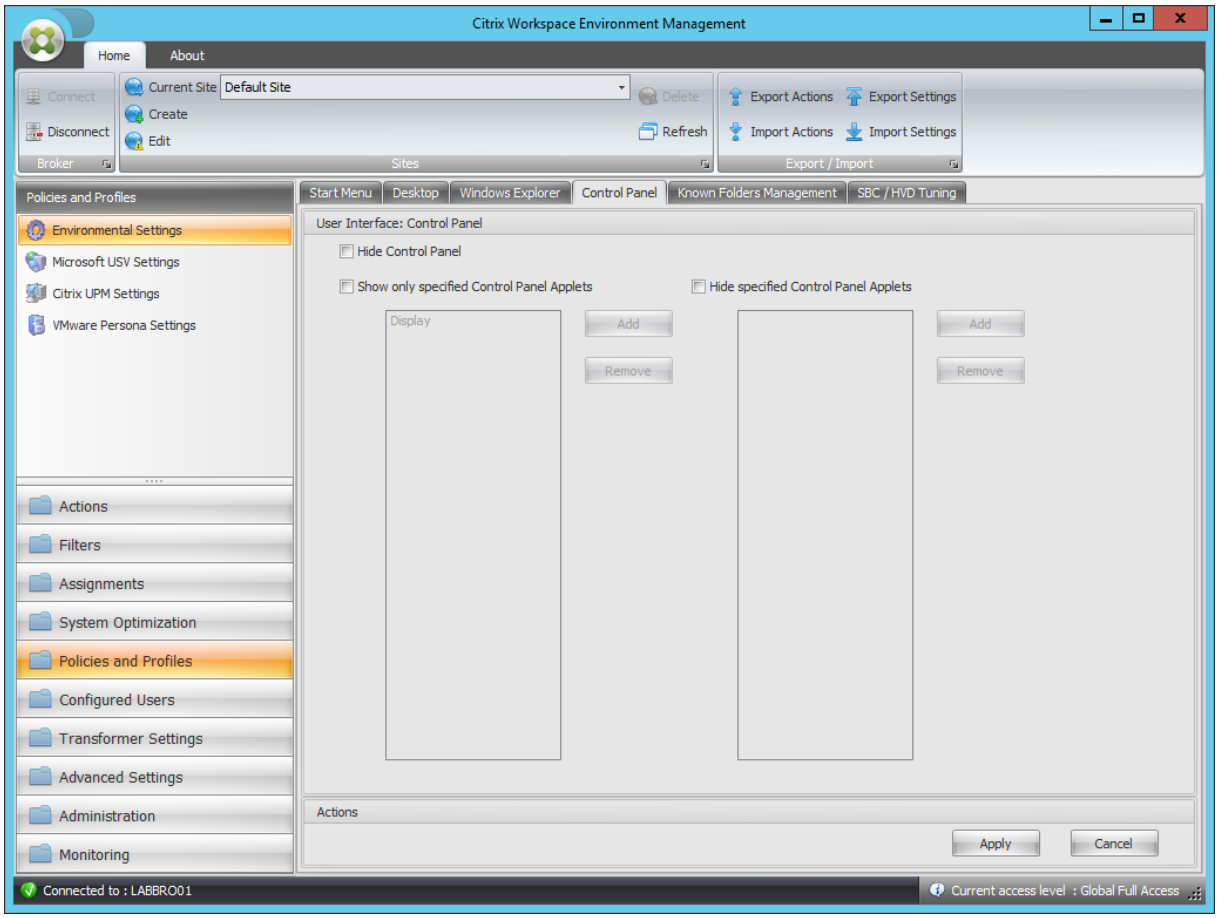
Disable Windows Security	
Processing	Service called by agent

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



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

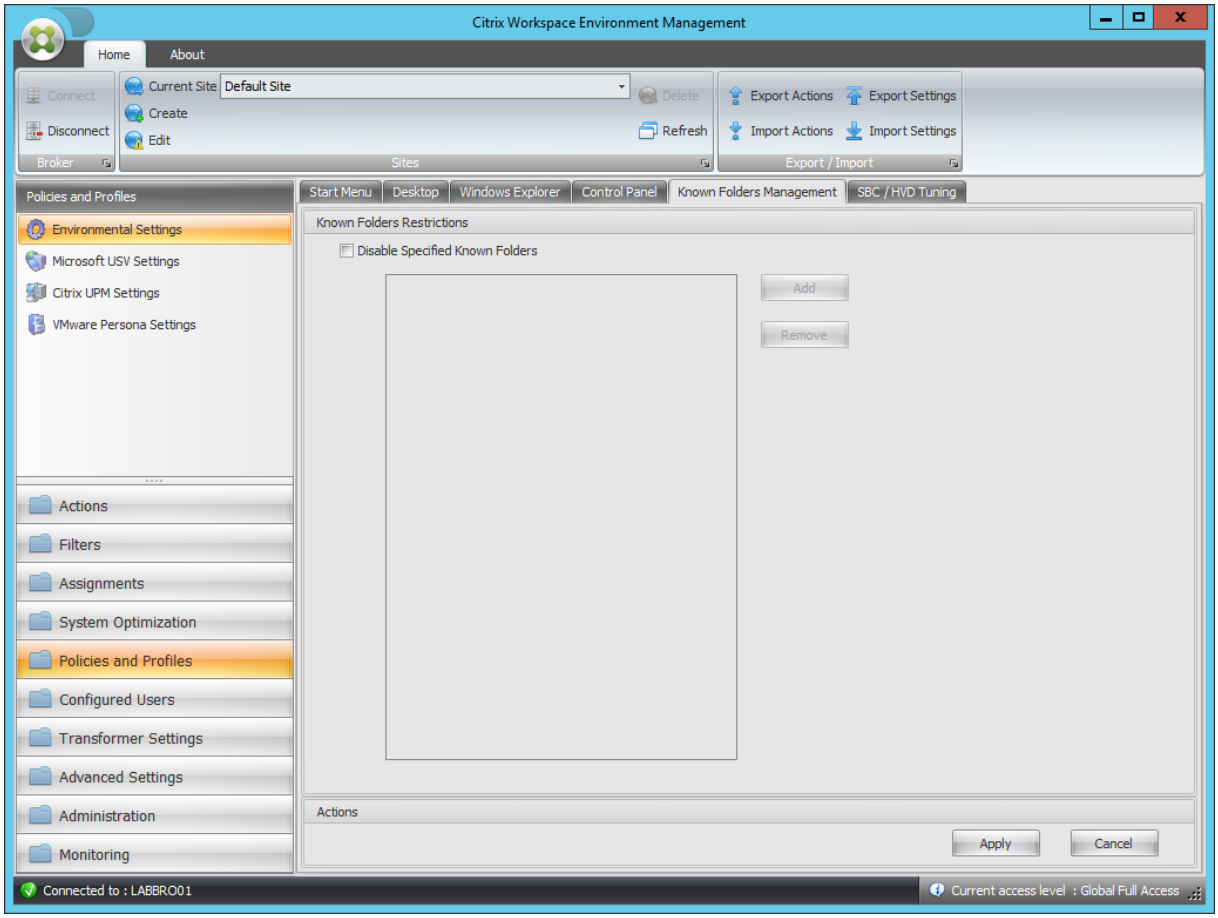
Show only specified Control Panel Applets	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	RestrictCpl
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

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

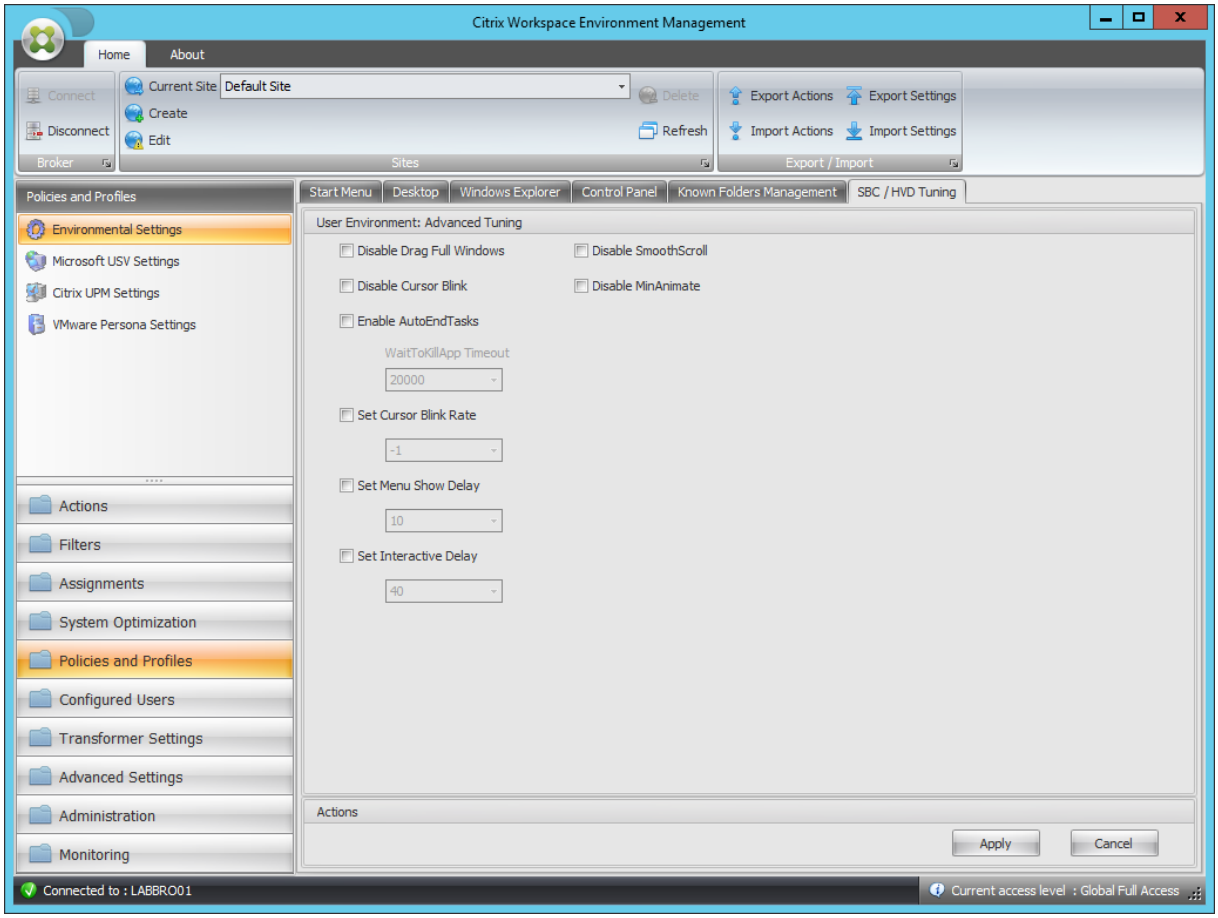
Hide specified Control Panel Applets	
Processing	Service called by agent

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	
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



Disable Drag Full Windows	
Parent Key	HKCU\Control Panel\Desktop
Value Name	DragFullWindows
Value Type	REG_SZ
Enabled Value	0
Disabled Value	1
Processing	Service at logon

Disable Cursor Blink	
Parent Key	HKCU\Control Panel\Desktop
Value Name	DisableCursorBlink
Value Type	DWORD
Enabled Value	1

Disable Cursor Blink	
Disabled Value	0
Processing	Service at logon

Enable AutoEndTasks	
Parent Key	HKCU\Control Panel\Desktop
Value Name	AutoEndTasks
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

WaitToKillApp Timeout	
Parent Key	HKCU\Control Panel\Desktop
Value Name	WaitToKillAppTimeout
Value Type	DWORD
Enabled Value	Configured value
Disabled Value	20000 (decimal)
Processing	Service at logon

Set Cursor Blink Rate	
Parent Key	HKCU\Control Panel\Desktop
Value Name	CursorBlinkRate
Value Type	DWORD
Enabled Value	Configured value
Disabled Value	500 (decimal)
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

Filter conditions

July 9, 2020

Workspace Environment Management includes the following filter conditions that you use to configure the circumstances under which the agent assigns resources to users. For more information about using these conditions in the administration console, see Filters.

When using the following filter conditions, be aware of these two scenarios:

- If the agent is installed on a single-session or multi-session OS:
  - "Client" refers to a client device connecting to the agent host.
  - "Computer" and "Client Remote" refer to the agent host.
- If the agent is installed on a physical endpoint, conditions that contain "client" in the condition names are not applicable.

Condition Name	**Always True**
Expected value type	N/A
Expected result type	N/A
Expected syntax	N/A
Returns	True.

Condition Name	**ComputerName Match**
Expected value type	N/A
Expected result type	String.
Expected syntax	Single name test: Computername Multiple tests (OR): Computername1;Computername2 Wildcard (also works with multiples): ComputerName*

Condition Name	**ComputerName Match**
Returns	True if the current computer name matches the tested value, false otherwise.

Condition Name	**ClientName Match**
Expected value type	N/A
Expected value type	String.
Expected syntax	Single name test: Clientname Multiple tests (OR): Clientname1;Clientname2 Wildcard (also works with multiples): ClientName*
Returns	True if the current client name matches the tested value, false otherwise.

Condition Name	**IP Address Match**
Expected value type	N/A
Expected result type	IP address.
Expected syntax	Single name test: IpAddress Multiple tests (OR): IpAddress1;IpAddress2 Wildcard (also works with multiples): IpAddress* Range (also works with multiples): IpAddress1-IpAddress2
Returns	True if the current computer IP address matches the tested value, false otherwise.

Condition Name	**Client IP Address Match**
Expected value type	N/A
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

Condition Name	**Client IP Address Match**
Returns	True if the current client IP address matches the tested value, false otherwise.

Condition Name	**Active Directory Site Match**
Expected value type	N/A
Expected result type	Exact name of the Active Directory site to test.
Expected syntax	Active directory site name.
Returns	True if the specified site matches the current site, false otherwise.

Condition Name	**Scheduling**
Expected value type	N/A
Expected result type	Day of week (example: Monday).
Expected syntax	Single name test: DayOfWeek Multiple tests (OR): DayOfWeek1; DayOfWeek2
Returns	True if today matches the tested value, false otherwise.

Condition Name	**Environment Variable Match**
Expected value type	String. Name of the tested variable.
Expected result type	String. Expected value of the tested variable.
Expected syntax	Single name test: value Not null test: ?
Returns	True if environment variable exists and value matches, false otherwise.

Condition Name	**Registry Value Match**
Expected value type	String. Full path and name of the registry value to test. Example: Registry Key **HKCU\Software\Citrix\TestValueName**
Expected result type	String. Expected value of the tested registry entry.
Expected syntax	Single name test: value Not null test: ?
Returns	True if registry value exists and value matches, false otherwise.

Condition Name	**WMI Query result Match**
Expected value type	N/A
Expected result type	String.
Expected syntax	Valid WMI query. For more information, see https://docs.microsoft.com/en-us/windows/win32/wmisdk/querying-with-wql.
Returns	True if query is successful and has a result, false otherwise.

Condition Name	**User Country Match**
Expected value type	N/A
Expected result type	String.
Expected syntax	Two letter ISO language name.
Returns	True if user ISO language name matches the specified value, false otherwise.

Condition Name	**User UI Language Match**
Expected value type	N/A
Expected result type	String. Two letter ISO language name. Example FR.

Condition Name	**User UI Language Match**
Expected syntax	Two letter ISO language name. Example FR.
Returns	True if user UI ISO language name matches the specified value, false otherwise.

Condition Name	**User SBC Resource Type**
Expected value type	N/A
Expected result type	Select from list.
Expected syntax	N/A
Returns	True if user context (published desktop or application) matches the selected value, false otherwise.

Condition Name	**OS Platform Type**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if machine platform type (x64 or x86) matches the selected value, false otherwise.

Condition Name	**Connection State**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if connection state (online or offline) matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Apps Version Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Version. Example: 6.5
Expected syntax	N/A
Returns	True if version matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Apps Farm Name Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Farm Name (up to version 6.5). Example: Farm.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Apps Zone Name Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Zone Name (up to version 6.5). Example: Zone.
Expected syntax	N/A
Returns	True if name matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Desktops Farm Name Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Desktops Farm Name (up to version 5). Example: Farm.
Expected syntax	N/A

Condition Name	**Citrix Virtual Desktops Farm Name Match**
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
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

Condition Name	**Active Directory Path Match**
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	Runs **ComputerName Match** and returns the opposite result (true if false, false if true). See condition **ComputerName Match** for more information.

Condition Name	**No ClientName Match**
Negative condition behavior	Runs ClientName Match and returns the opposite result (true if false, false if true). See condition **ClientName Match** for more information.

Condition Name	**No IP Address Match**
Negative condition behavior	Runs IP Address Match and returns the opposite result (true if false, false if true). See condition **IP Address Match** for more information.

Condition Name	**No Client IP Address Match**
Negative condition behavior	Runs Client IP Address Match and returns the opposite result (true if false, false if true). See condition **Client IP Address Match** for more information.

Condition Name	**No Active Directory Site Match**
Negative condition behavior	Runs Active Directory Site Match and returns the opposite result (true if false, false if true). See condition **Active Directory Site Match** for more information.

Condition Name	**No Environment Variable Match**
Negative condition behavior	Runs Environment Variable Match and returns the opposite result (true if false, false if true). See condition **Environment Variable Match** for more information.

Condition Name	**No Registry Value Match**
Negative condition behavior	Runs Registry Value Match and returns the opposite result (true if false, false if true). See condition **Registry Value Match** for more information.

Condition Name	**No WMI Query result Match**
Negative condition behavior	Runs WMI Query result Match and returns the opposite result (true if false, false if true). See condition **WMI Query result Match** for more information.

Condition Name	**No User Country Match**
Negative condition behavior	Runs User Country Match and returns the opposite result (true if false, false if true). See condition **User Country Match** for more information.

Condition Name	**No User UI Language Match**
Negative condition behavior	Runs User UI Language Match and returns the opposite result (true if false, false if true). See condition **User UI Language Match** for more information.

Condition Name	**No Citrix Virtual Apps Version Match**
Negative condition behavior	Runs Citrix Virtual Apps Version Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Apps Version Match** for more information.

Condition Name	**No Citrix Virtual Apps Farm Name Match**
Negative condition behavior	Runs Citrix Virtual Apps Farm Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Apps Farm Name Match** for more information.

Condition Name	**No Citrix Virtual Apps Zone Name Match**
Negative condition behavior	Runs Citrix Virtual Apps Zone Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Apps Zone Name Match** for more information.

Condition Name	**No Citrix Virtual Desktops Farm Name Match**
Negative condition behavior	Runs Citrix Virtual Desktops Farm Name Match and returns the opposite result (true if false, false if true). See condition **Citrix Virtual Desktops Farm Name Match** for more information.

Condition Name	**No Citrix Virtual Desktops Desktop Group Name Match**
Negative condition behavior	Runs 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	Runs Active Directory Path Match and returns the opposite result (true if false, false if true). See condition **Active Directory Path Match** for more information.

Condition Name	**No Active Directory Attribute Match**
Negative condition behavior	Runs Active Attribute Path Match and returns the opposite result (true if false, false if true). See condition **Active Attribute Path Match** for more information.

Condition Name	**Name or Value is not in List**
Negative condition behavior	Runs Name or Value is in List and returns the opposite result (true if false, false if true). See condition **Name or Value is in List** for more information.

Condition Name	**Client Remote OS Match**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A

Condition Name	**Client Remote OS Match**
Returns	True if current remote client operating system matches selected value, false otherwise.

Condition Name	**No Client Remote OS Match**
Negative condition behavior	Runs Client Remote OS Match and returns the opposite result (true if false, false if true). See condition **Client Remote OS Match** for more information.

Condition Name	**Dynamic Value Match**
Expected value type	String. Any dynamic expression using environment variables or Dynamic Tokens.
Expected result type	String. Expected value of the tested expression.
Expected syntax	Single name test: value Not null test: ?
Returns	True if dynamic expression result value exists and value matches, false otherwise.

Condition Name	**No Dynamic Value Match**
Negative condition behavior	Runs Dynamic Value Match and returns the opposite result (true if false, false if true). See condition **Dynamic Value Match** for more information.

Condition Name	**Transformer Mode State**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A

Condition Name	**Transformer Mode State**
Returns	True if current Transformer state matches selected value, false otherwise.

Condition Name	**No Client OS Match**
Negative condition behavior	Runs Client OS Match and returns the opposite result (true if false, false if true). See condition **Client OS Match** for more information.

Condition Name	**Active Directory Group Match**
Expected value type	N/A
Expected result type	String.
Expected syntax	Single name test: group NetBIOS name (DOMAIN\Groupname) Multiple tests (OR): Groupname1;Groupname2
Returns	True if any of the current user groups matches the tested value, false otherwise.

Condition Name	**No Active Directory Group Match**
Negative condition behavior	Runs Active Directory Group Match and returns the opposite result (true if false, false if true). See condition **Active Directory Group Match** for more information.

Condition Name	**File Version Match**
Expected value type	String. Full path and name of the file to test. Example: **C:\Test\TestFile.dll**
Expected result type	String. Expected file version value of the tested file.
Expected syntax	Single name test: value Not null test: ?

Condition Name	**File Version Match**
Returns	True if registry value exists and value matches, false otherwise.

Condition Name	**No File Version Match**
Negative condition behavior	Runs File Version Match and returns the opposite result (true if false, false if true). See condition **File Version Match** for more information.

Condition Name	**Network Connection State**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current network connection state matches selected value, false otherwise.

> **Important:**
>
> Before you use Published Resource Name as the filter condition type, keep the following in mind: If the published resource is a published application, type the browser name of the application in the **Matching Result** field. If the published resource is a published desktop, type the published name of the desktop in the **Matching Result** field.

Condition Name	**Published Resource Name**
Expected value type	N/A
Expected result type	String. Name of the published resource (Citrix Virtual Apps/Citrix Virtual Desktops/RDS).
Expected syntax	Single name test: published resource name Multiple tests (OR): Name1;Name2 Wildcard test: Name*

Condition Name	**Published Resource 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	Runs Name is in List and returns the opposite result (true if false, false if true). See condition **Name is in List** for more information.

Condition Name	**File/Folder exists**
Expected value type	N/A
Expected result type	String.
Expected syntax	Full path of the file system entry (file or folder) to test.
Returns	True if the specified file system entry exists, false otherwise.

Condition Name	**File/Folder does not exist**
Negative condition behavior	Runs File/Folder exists and returns the opposite result (true if false, false if true). See condition **File/Folder exists** for more information.

Condition Name	**DateTime Match**
Expected value type	N/A
Expected result type	DateTime as String. Date/time to test.
Expected syntax	Single Date: 06/01/2016 Date Range: 06/01/2016-08/01/2016 Multiple entries: entry1;entry2 Ranges and single dates can be mixed
Returns	True if execution date/time matches any of the specified entries, false otherwise.

Condition Name	**No DateTime Match**
Negative condition behavior	Runs DateTime Match and returns the opposite result (true if false, false if true). See condition **DateTime Match** for more information.

Load balancing with Citrix ADC

January 3, 2020

This article guides you through the deployment of a Workspace Environment Management (WEM) server group containing two or more infrastructure servers in all active load balanced configurations. The article provides details of how to configure a Citrix ADC appliance to load balance incoming requests from the WEM administration console and the WEM agent.

You can listen on these WEM ports with Citrix ADC:

- Administration port (by default, 8284)
- Agent service port (by default, 8286)

- Cached data synchronization port (by default, 8288)

Suppose you want to deploy a WEM server group containing two infrastructure servers (infrastructure server 1 and infrastructure server 2). Perform the following steps:

1. Log on to the Citrix ADC management GUI and then click **Configuration**.
2. Navigate to **Traffic Management > Load Balancing > Servers > Add** and then click **Add** to add infrastructure server 1. Repeat to add infrastructure server 2.
3. Navigate to **Traffic Management > Load Balancing > Service Groups** and then click **Add** to create a service group for the *administration console service*.
    - **Protocol**. Select **TCP**.
    - **Cache Type**. Select **SERVER**.
4. On the Load Balancing Service Group page, click **No Service Group Member**.
5. On the Create Service Group Member page, select **Server Based**, click the right arrow, and then select infrastructure server 1. Repeat steps 3 through 5 for infrastructure server 2.
    - **Port**. For example, type 8284 for the administration console.
6. Follow steps 3 through 5 to create service groups for the *agent service* and *cache synchronization service*.
    - **Port**. For the agent service port, type 8286. For the cached data synchronization port, type 8288.
7. Navigate to **Traffic Management > Load Balancing > Virtual Servers** and then click **Add** to add a virtual server for the *administration console service*.
    - **Protocol**. Select **TCP**.
    - **IP Address Type**. Select **IP Address**.
    - **IP Address**. Type the Virtual IP. For details, see Configuring Citrix ADC-owned IP addresses.
    - **Port**. For example, type 8284 for the administration console.
8. Click **No Load Balancing Virtual Server Service Group Binding**.
9. On the Service Group Binding page, click the right arrow, select the corresponding service group, and then click **Bind**.
10. Follow steps 7 through 9 to create virtual servers that listen on the agent service port and the cached data synchronization port.
    - **Port**. For the agent service port, type 8286. For the cached data synchronization port, type 8288.

If you want to enable persistence, follow these steps:

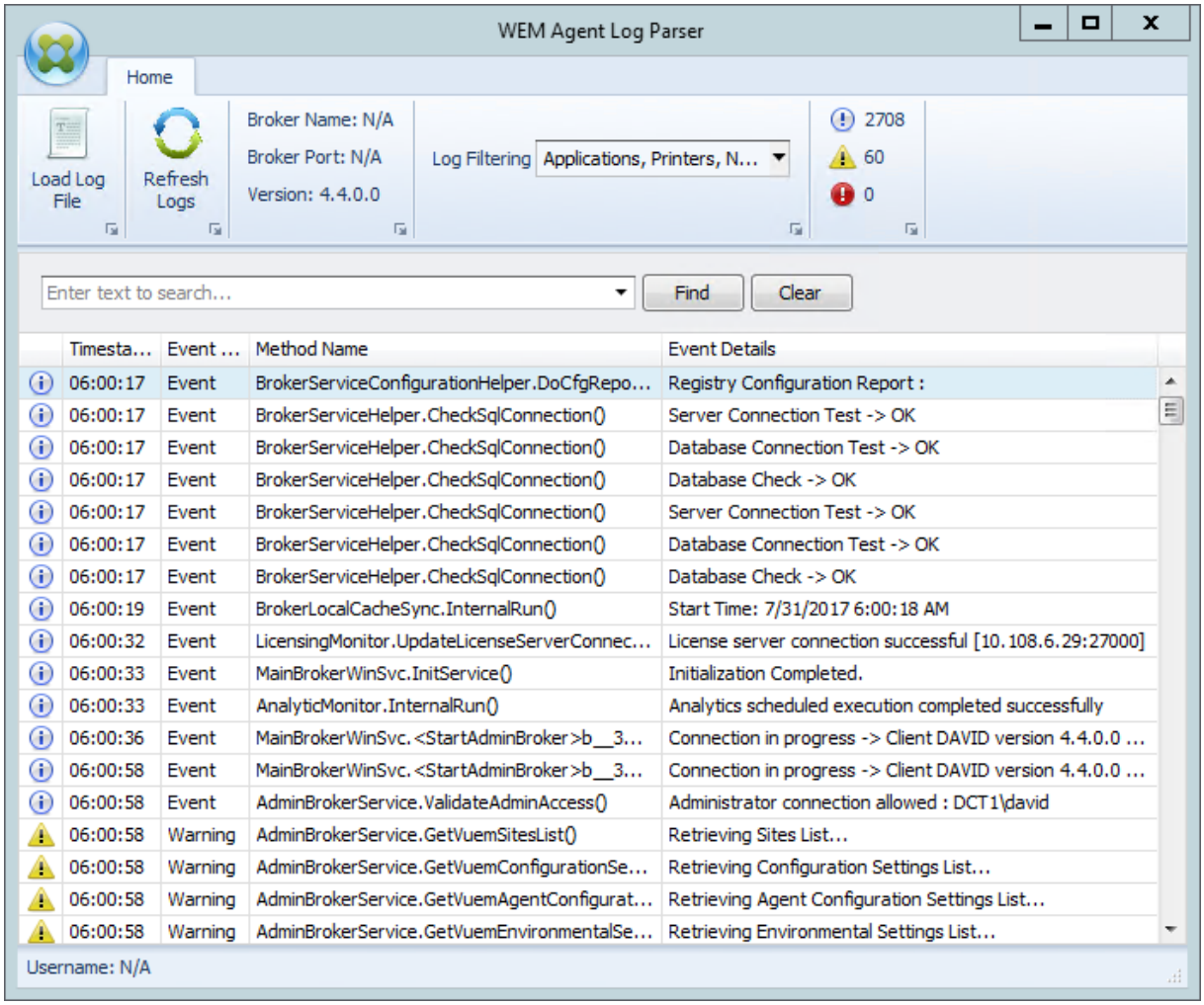
> **Note:**
>
> For more information about persistence, see Source IP address persistence.

1. Navigate to **Traffic Management > Load Balancing > Virtual Servers** and then click each listed virtual server.
2. In the **Help** pane of the Load Balancing Virtual Server page, click **Persistence**.
3. In the **Persistence** pane, configure the Persistence settings, click **OK**, and then click **Done**.
    - **Persistence**. Select **SOURCEIP**.
    - **Time-out (mins)**. Specify how long persistence times out.
    - **IPv4 Netmask**. Type the subnet mask that you used to configure Citrix ADC.

Log parser

July 9, 2020

Workspace Environment Management includes a log parser application, which is located in the agent installation directory:



The **WEM Agent Log Parser** allows you to open any Workspace Environment Management agent log file, making them searchable and filterable. The parser summarizes the total number of events, warnings, and exceptions (in the top right of the ribbon). It also includes details about the log file (the name and port of the infrastructure service it first connected to and the agent version and user name).

Port information

December 5, 2019

Workspace Environment Management uses the following ports.

Source	Destination	Type	Port	Details
Infrastructure service	Agent host	TCP	49752	“Agent port”. Listening port on the agent host that receives instructions from the infrastructure service.
Administration console	Infrastructure service	TCP	8284	“Administration port”. Port on which the administration console connects to the infrastructure service.
Agent	Infrastructure service	TCP	8286	“Agent service port”. Port on which the agent connects to the infrastructure server.

Source	Destination	Type	Port	Details
Agent cache synchronization process	Infrastructure service	TCP	8285	“Cache synchronization port”. Applicable to Workspace Environment Management 1909 and earlier; replaced by *Cached data synchronization port* in Workspace Environment Management 1912 and later. Port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server.

Source	Destination	Type	Port	Details
Agent cache synchronization process	Infrastructure service	TCP	8288	“Cached data synchronization port”. Applicable to Workspace Environment Management 1912 and later; replaces *Cache synchronization port* of Workspace Environment Management 1909 and earlier. Port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server.

Source	Destination	Type	Port	Details
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.
Monitoring service	Infrastructure service	TCP	8287	“WEM monitoring port”. Listening port on the infrastructure server used by the monitoring service. (Not yet implemented.)

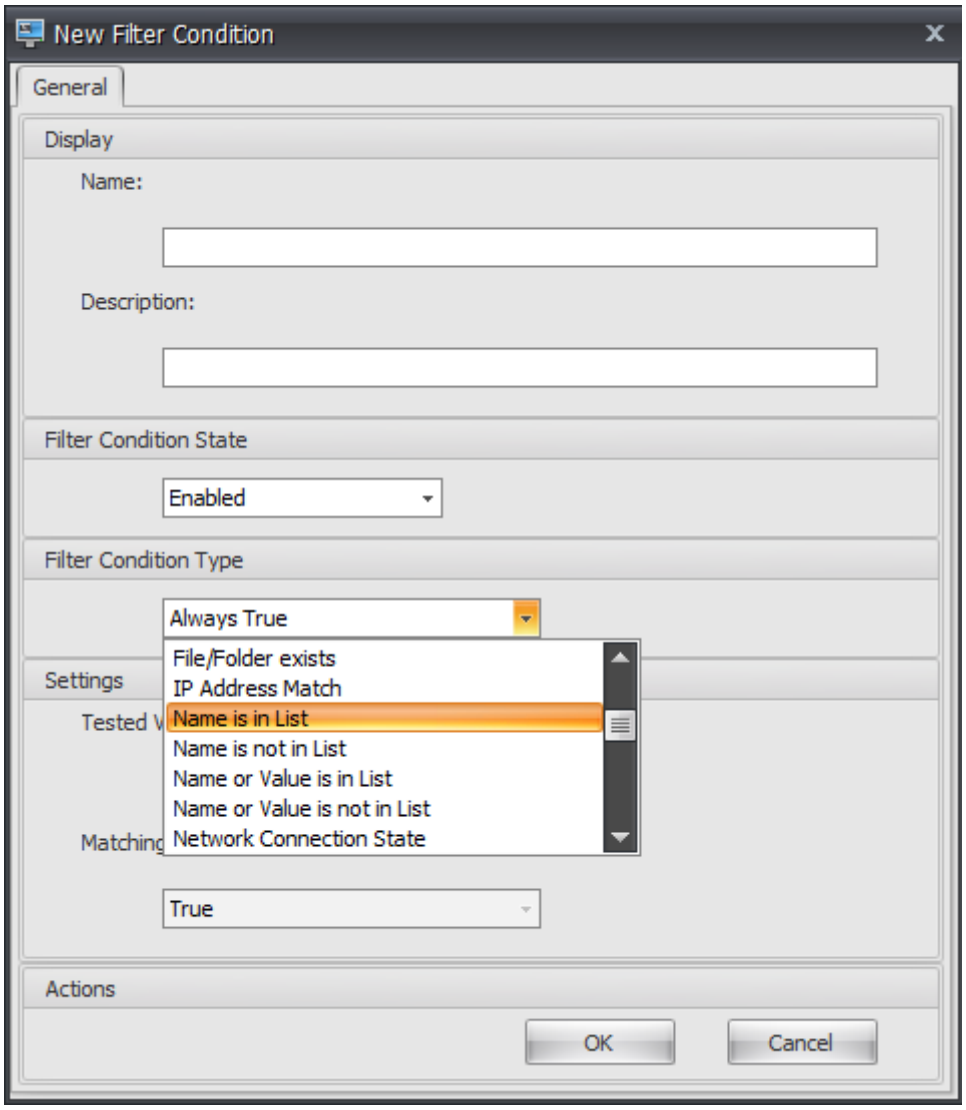
WEM Integrity Condition List Manager

July 4, 2019

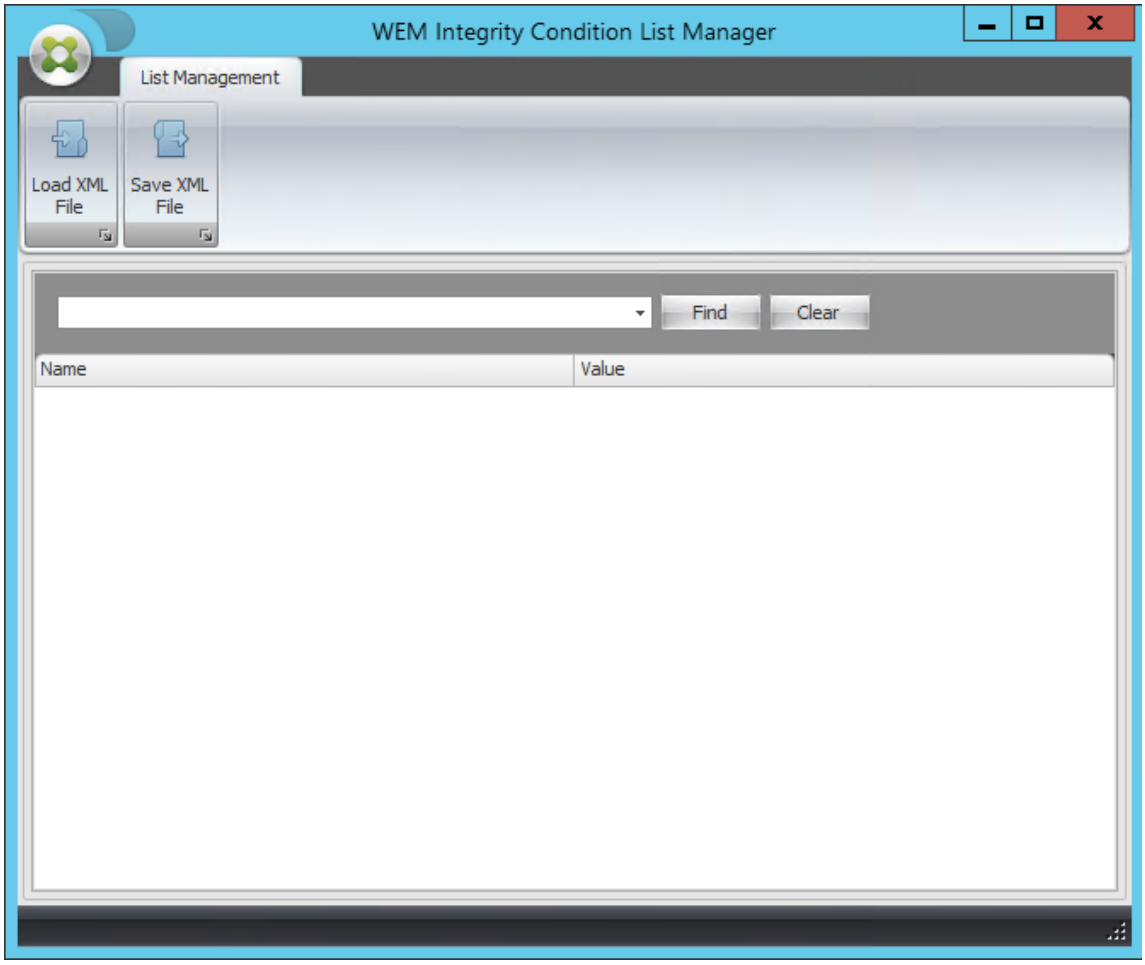
WEM Integrity Condition List Manager is a powerful tool that helps you create the XML file for filtering

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**.

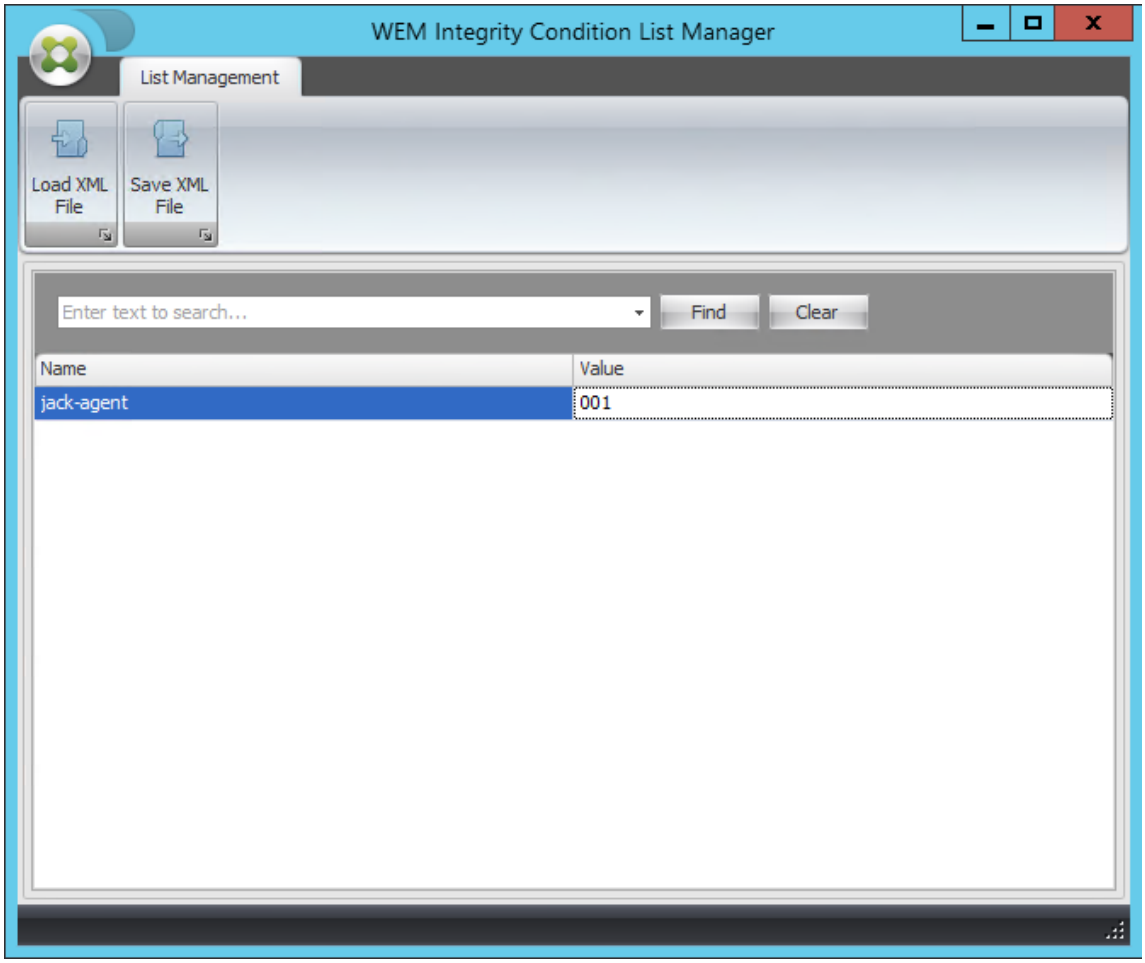


1. Open WEM Integrity Condition List Manager.

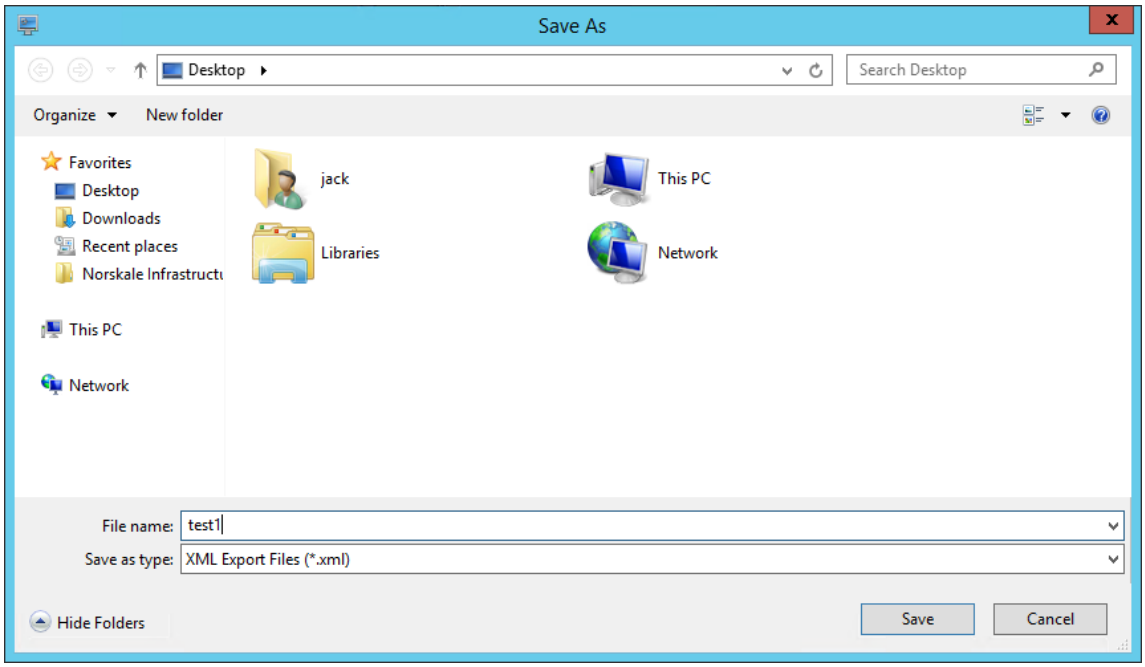


2. Right-click the blank area and then select **Add** in the context menu.
3. Type the name in the **Name** field.

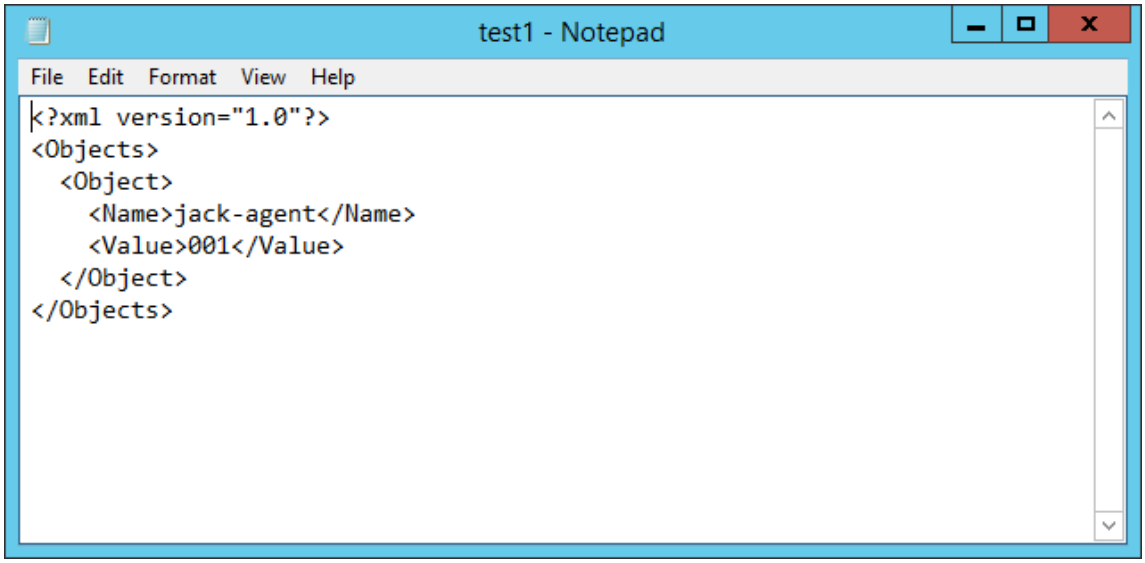
> **Note:**
>
> Type the name of the machine on which the WEM agent is running (agent host).



4. Click **Save XML File**, browse to the desired folder, and then click **Save**.



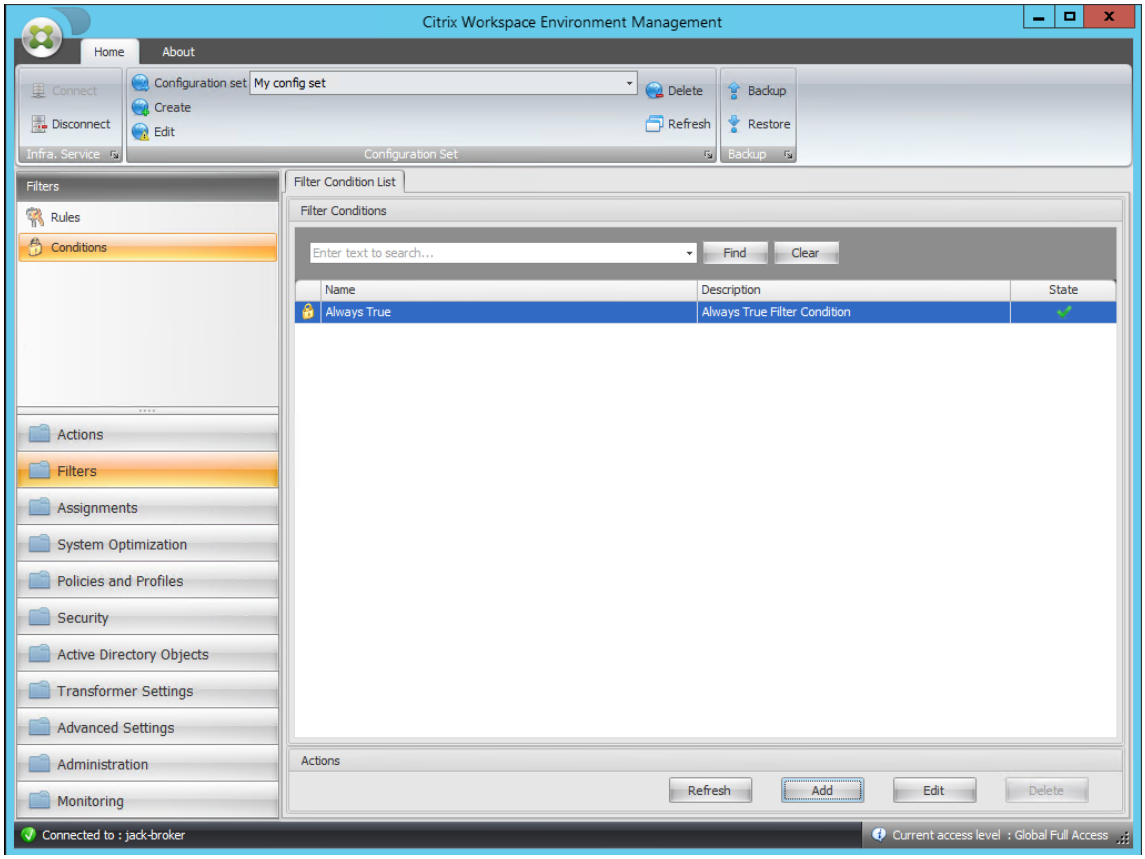
5. Open the saved XML file to verify that the information you provided was saved correctly.



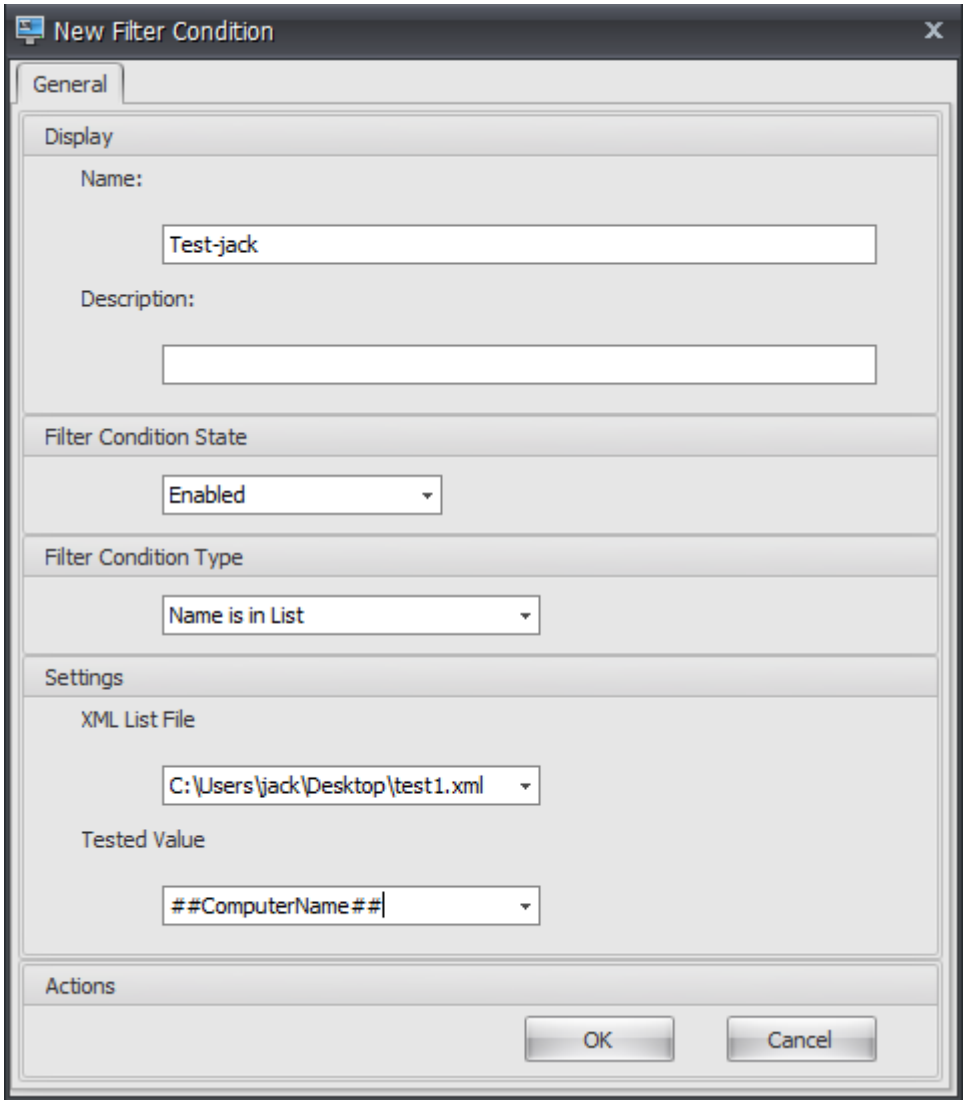
6. Copy the saved XML file to a folder on the agent host.

> **Note:**
>
> This feature does not work if you save the XML file on an administration console machine.

7. Go to the **Administration Console > Filters > Conditions > Filter Condition List** tab and then click **Add**.



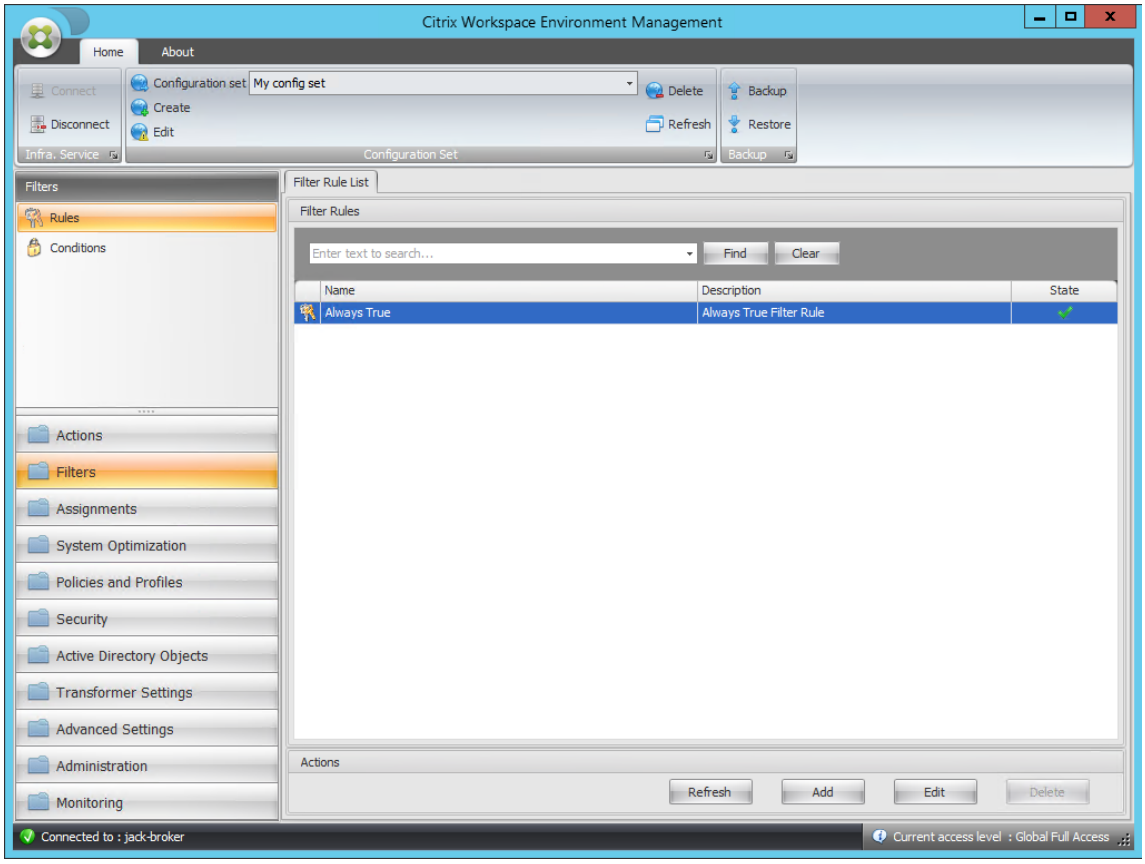
8. Type the information and then click **OK**.



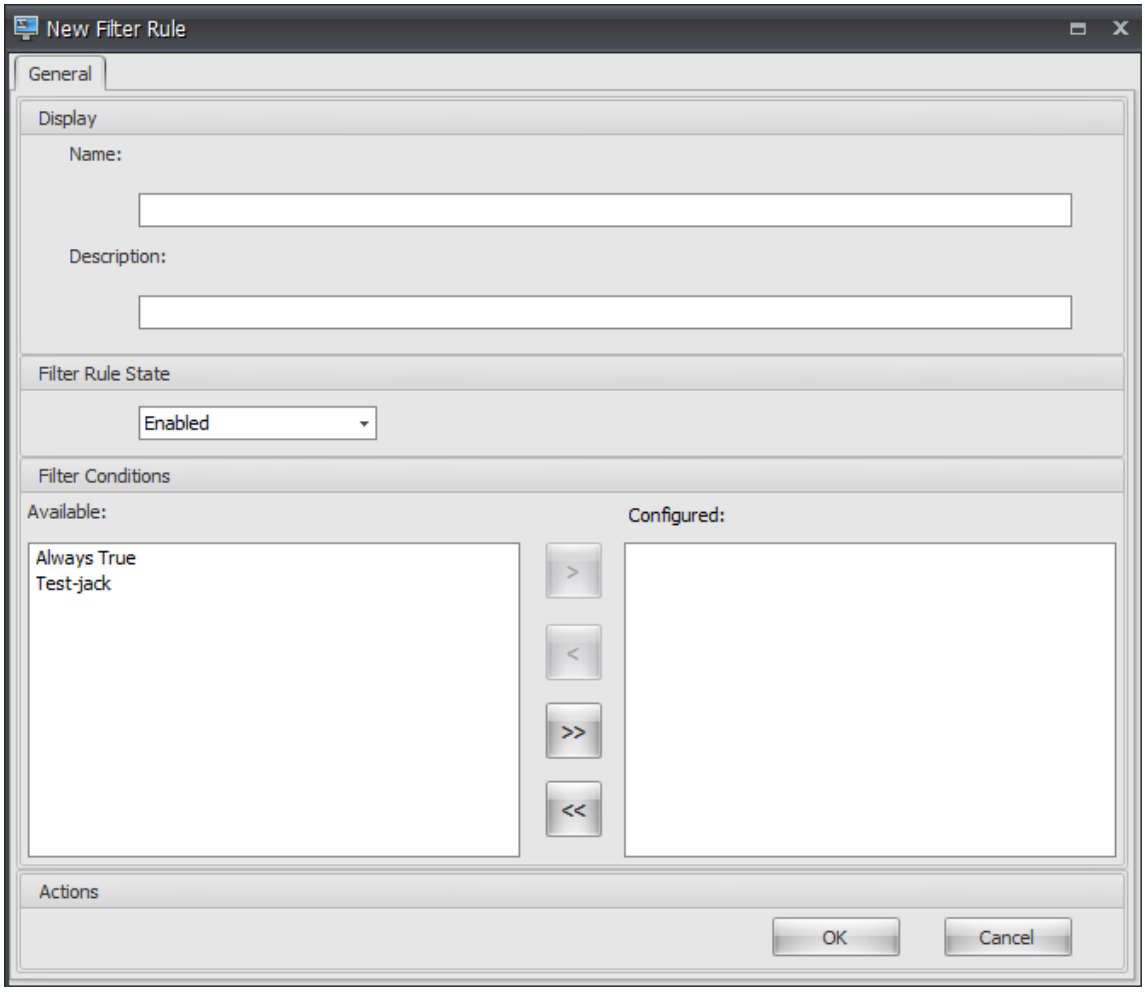
Note:

- **Filter Condition Type**. Select **Name is in List**.
- **XML List File**: C:\Users\<user1>\Desktop\test1.xml (file address on the agent host)
- **Tested Value**. Type the dynamic token that corresponds to the name you typed in the **Name** field in the WEM Integrity Condition List Manager. In this example, you typed the name of the machine on which the agent is running (agent host). Therefore, you must use the dynamic token "##ComputerName##." For more information about using dynamic tokens, see Dynamic tokens.

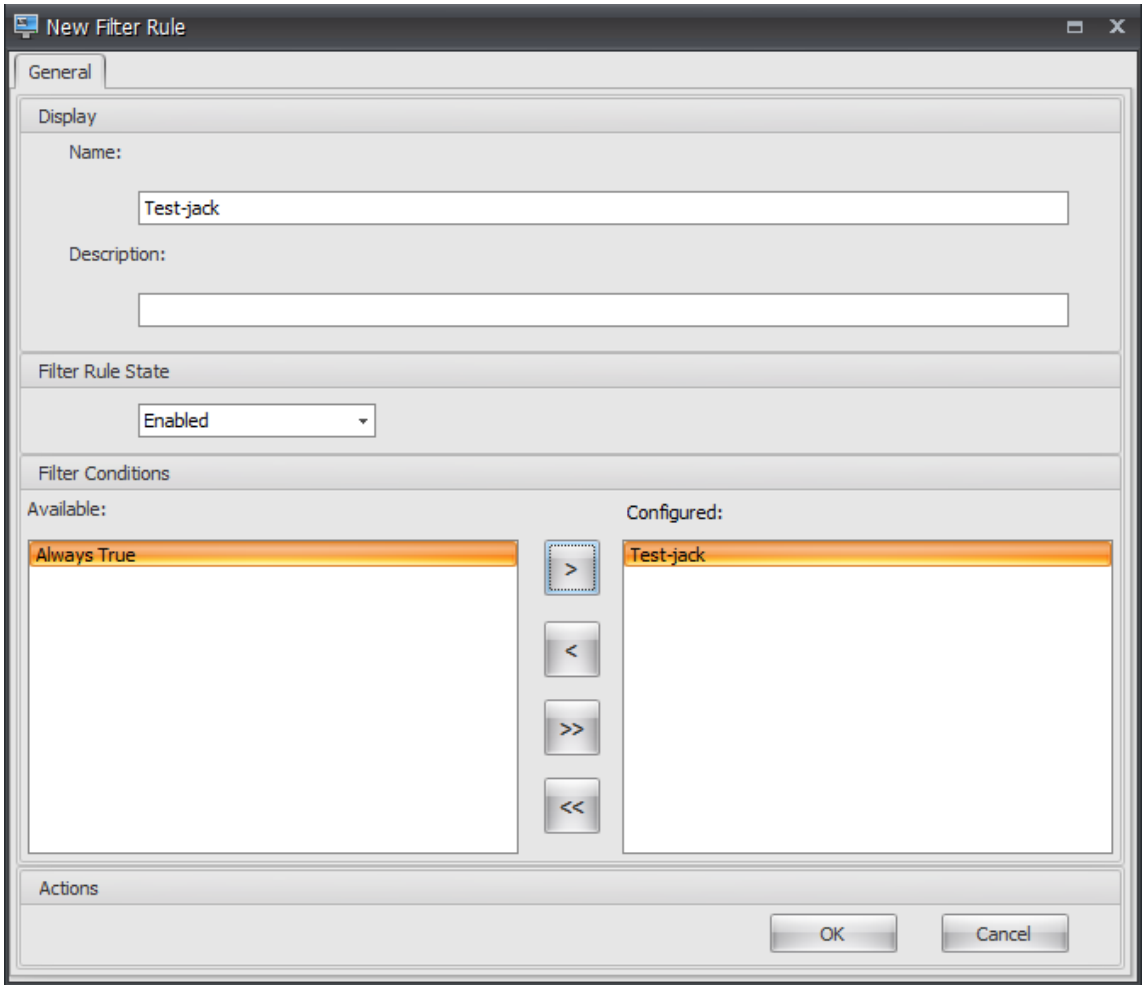
9. Go to the **Administration Console > Filters > Rules > Filter Rule List** tab and then click **Add**.



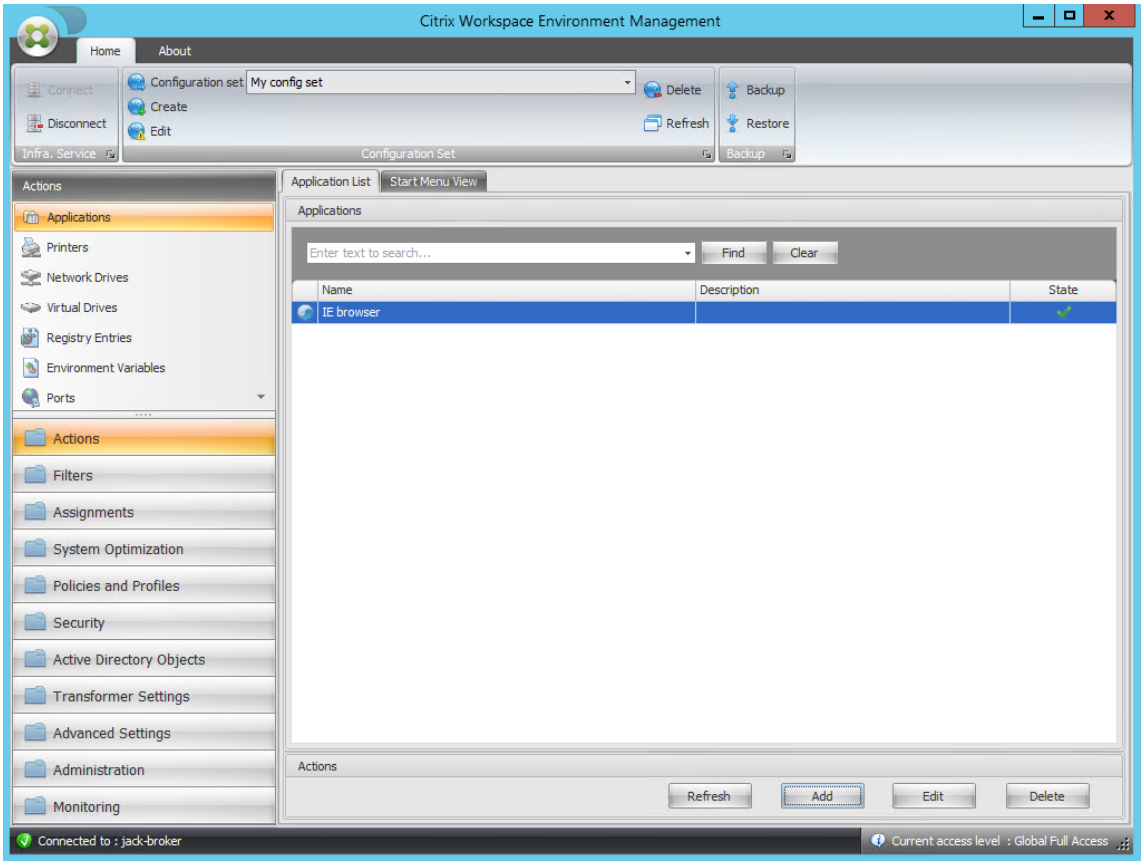
10. Type the filter name in the **Name** field.



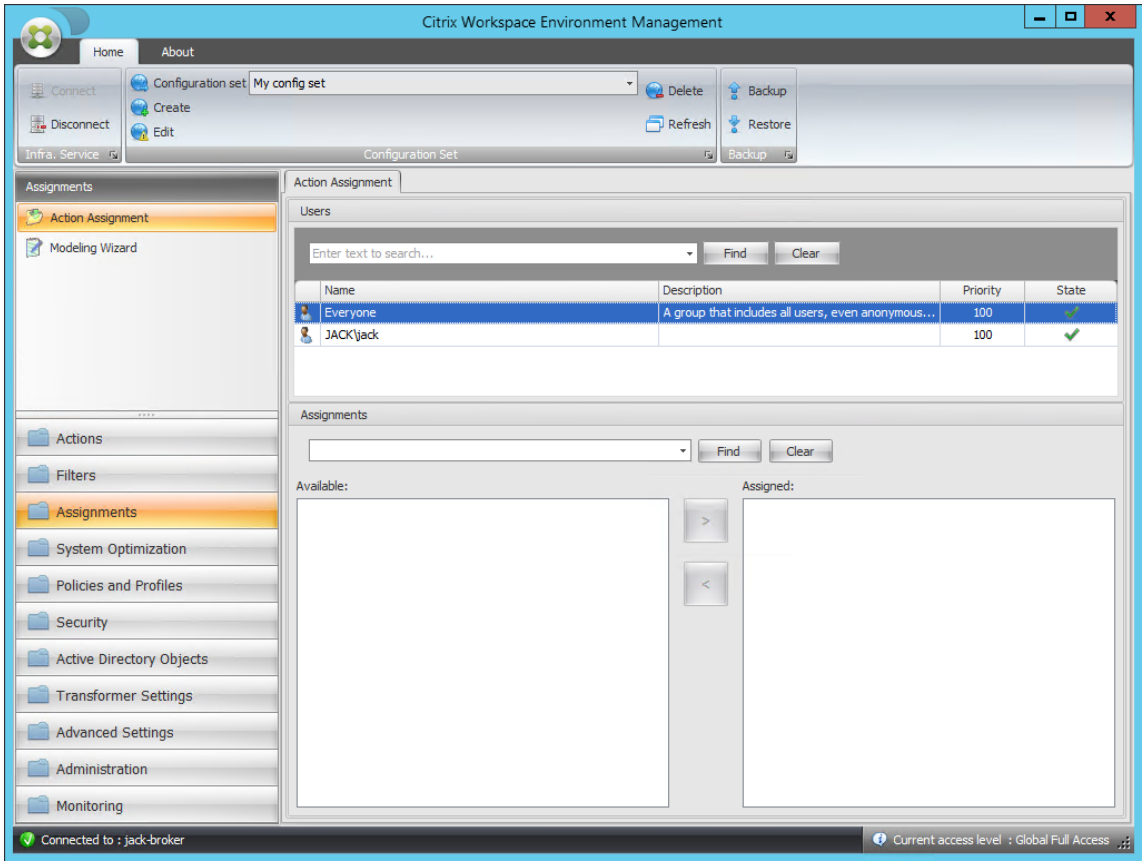
11. Move the configured condition from the **Available** pane to the **Configured** pane and then click **OK**.



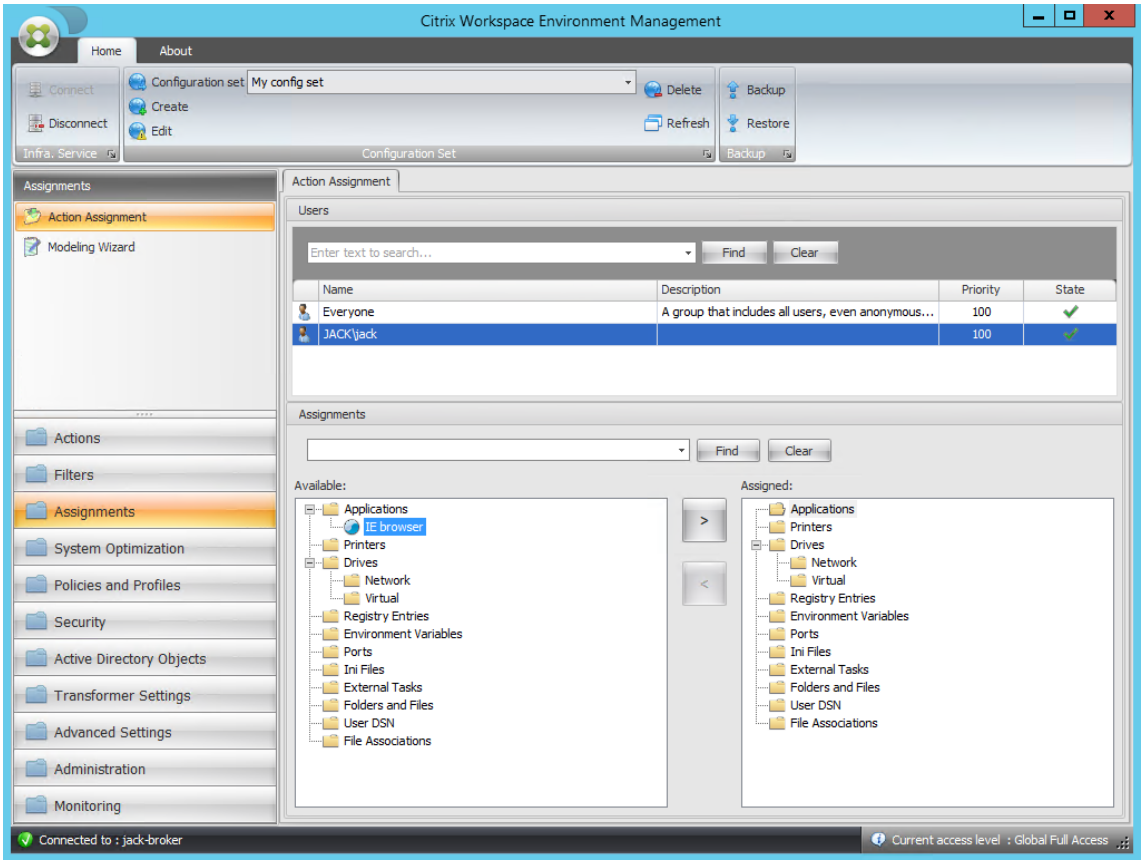
12. Go to the **Administration Console > Actions > Applications > Application List** tab and then add an application.



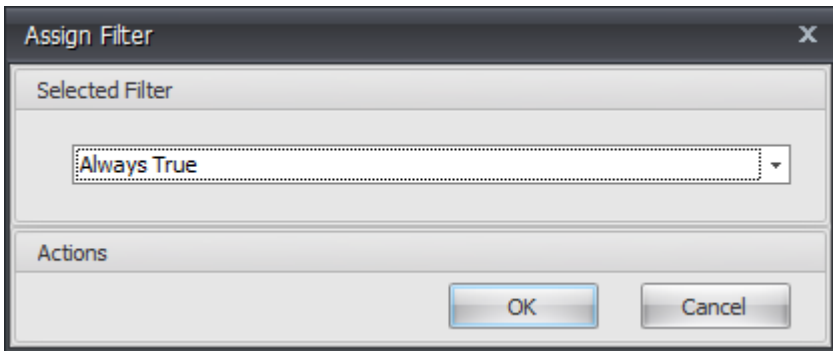
13. Go to the **Administration Console > Assignments > Action Assignment** tab.



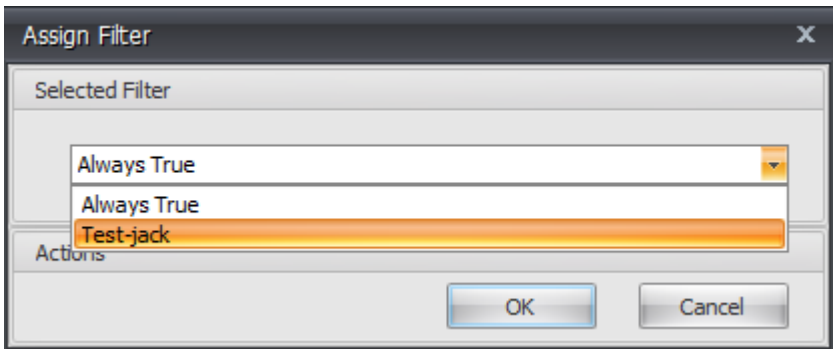
14. Double-click the desired user or user group (in this example, select the agent host).



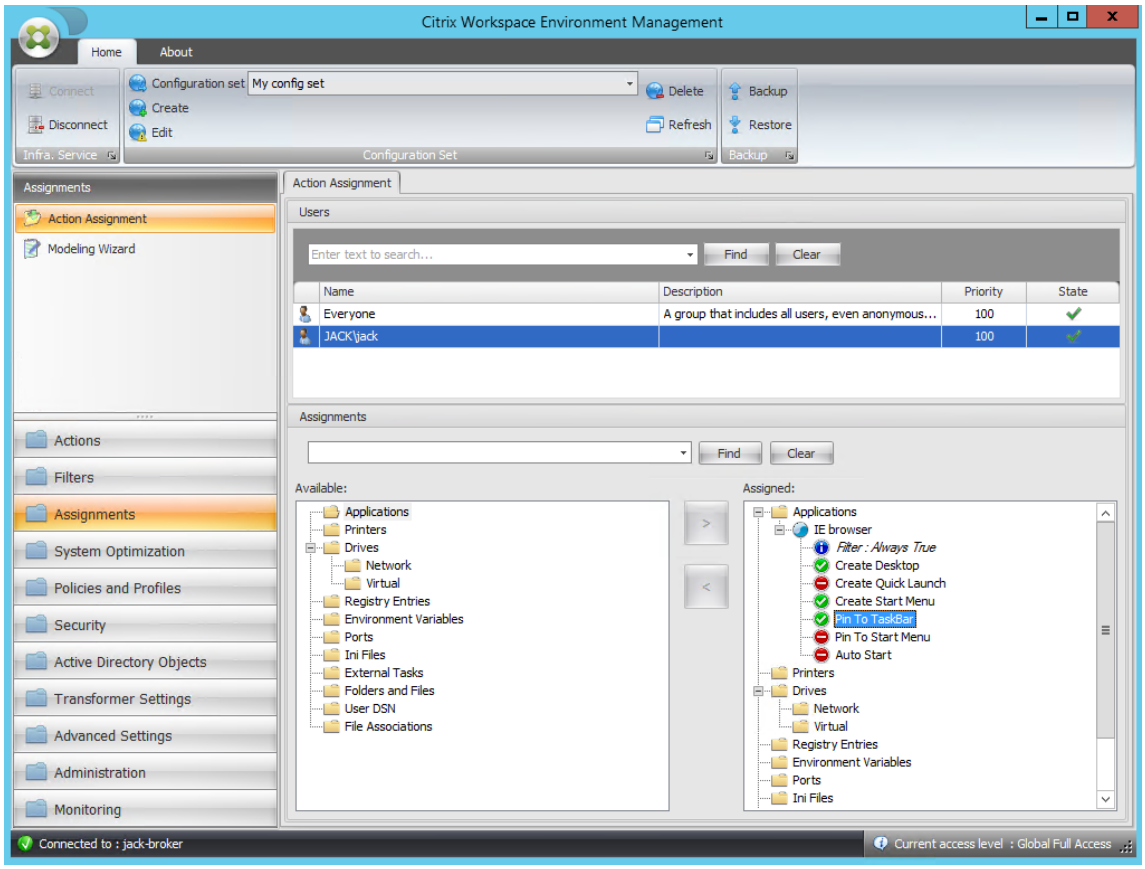
15. Move the application from the **Available** pane to the **Assigned** pane.



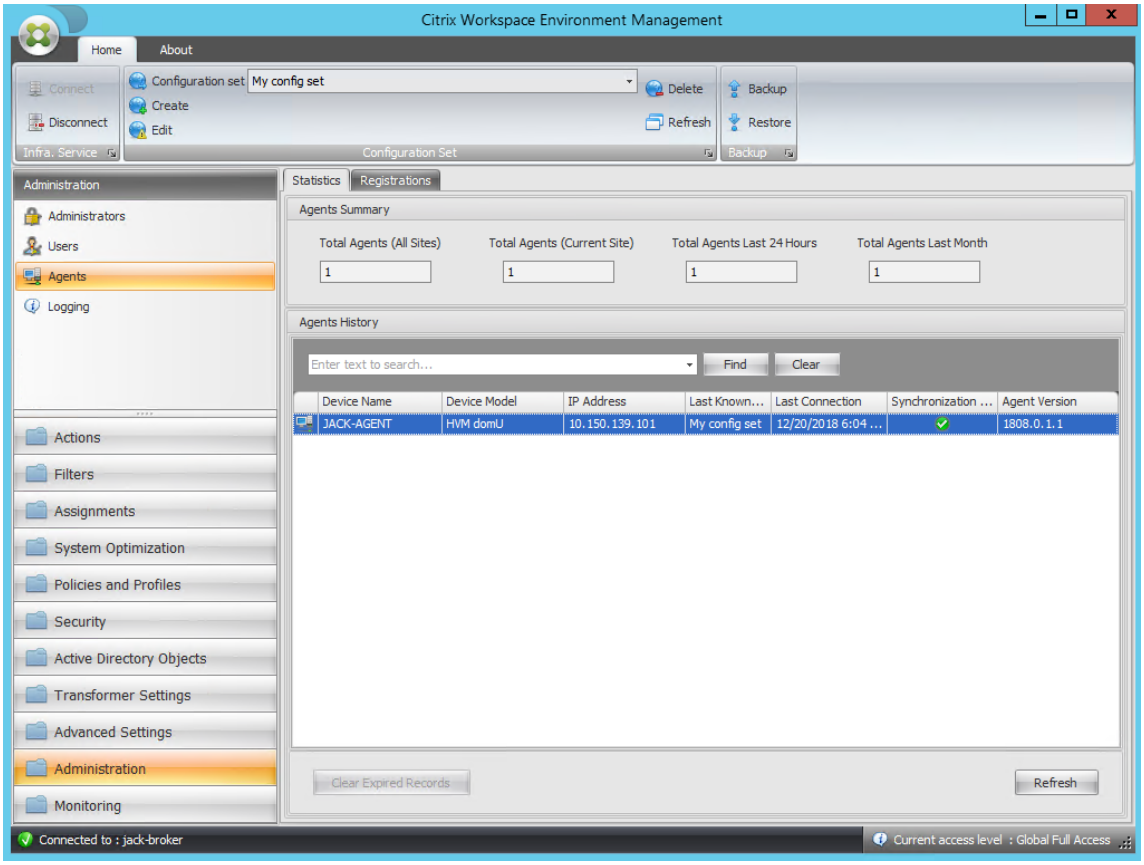
16. Select the filter and then click **OK**.



17. Enable the options for the assigned application (in this example, enable **Create Desktop** and **Pin To TaskBar**).

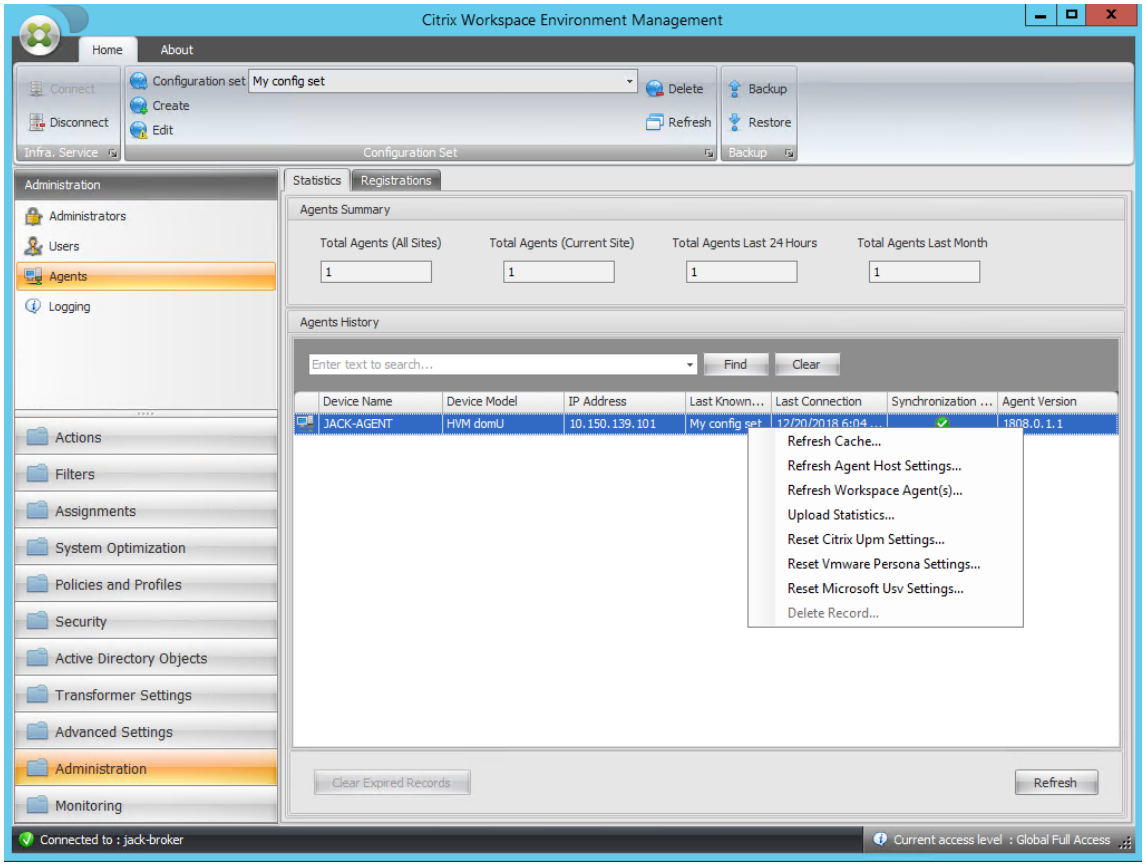


18. Go to the **Administration Console > Administration > Agents > Statistics** tab and then click **Refresh**.

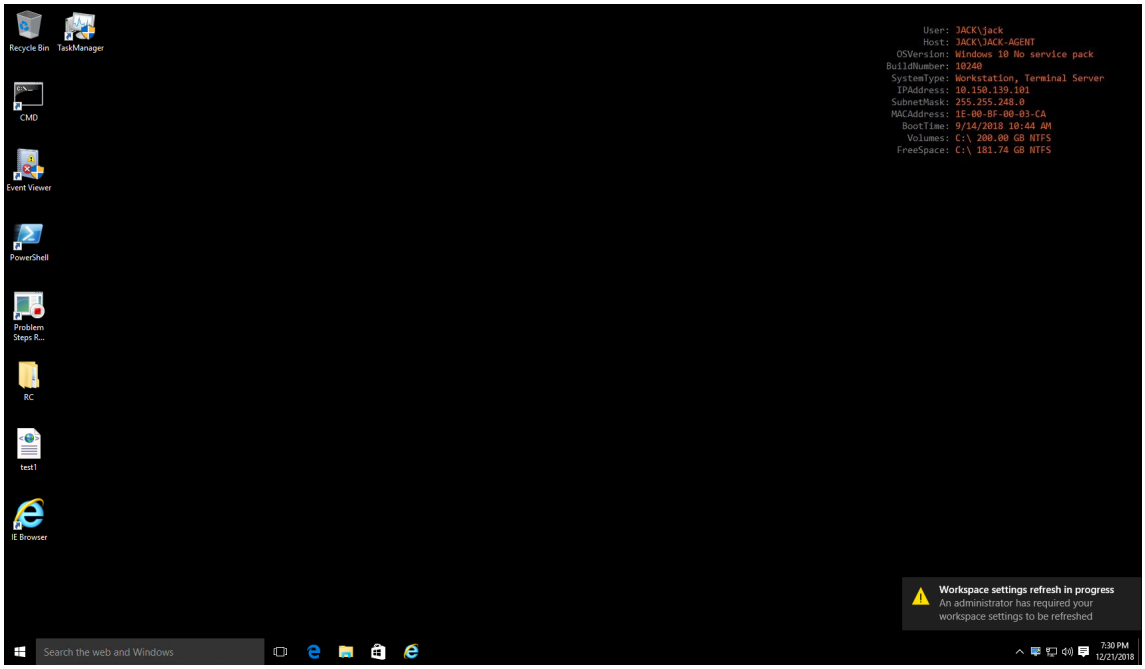


19. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.

> **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.



20. Go to the machine on which the agent is running (agent host) to verify that the configured condition works.



In this example, the application is successfully assigned to the agent host, which is created on the

desktop and pinned to the taskbar.

XML printer list configuration

July 8, 2020

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 later modified, increment this value by 1 to notify the Agent Host and ensure the printer action is reprocessed.

<Name>. This is the printer name as perceived by the Workspace Environment Management Agent Host. This field **cannot** be left blank.

<Description>. This is the printer description as perceived by the Workspace Environment Management Agent Host. This field can be blank.

<DisplayName>. This is unused and should be left blank.

<TargetPath>. This is the UNC path to the printer.

<ExtLogin>. Contains the name of the Windows account used when specifying Windows credentials for connection. [Currently unsupported. Leave this field blank.].

<ExtPassword>. Contains the password for the Windows account used when specifying Windows credentials for connection. [Currently unsupported. Leave this field blank.].

<Reserved01>. This contains advanced settings. **Do not** alter it in any way.

```
1 &gt;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;SelfHealingEnabled&lt;/
     Name&gt;&lt;Value&gt;0&lt;/Value&gt;&lt;/VUEMActionAdvancedOption
```

To activate self-healing for a given printer object, simply copy and paste the above contents, changing the highlight **0** value to **1**.

Example printer object

The following example assigns two active printers on the client or computer **DEVICE1**:

- **HP LaserJet 2200 Series** on UNC path **\\server.example.net\HP LaserJet 2200 Series** (default printer)
- **Canon C5531i Series** printer on UNC path **\\server.example.net\Canon C5531i Series**

It also assigns one active printer on the client or computer DEVICE2:

- **HP LaserJet 2200 Series** on UNC path **\\server.example.net\HP LaserJet 2200 Series**


```
<?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>
```

```
32                      <IdFilterRule>1</IdFilterRule>
33                      <RevisionId>1</RevisionId>
34                      <Name>Canon C5531i Series</Name>
35                      <Description />
36                      <DisplayName />
37                      <TargetPath>\\server.example.net\Canon C5531i
                           Series</TargetPath>
38                      <ExtLogin />
39                      <ExtPassword />
40                      <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>
41                  </VUEMUserAssignedPrinter>
42              </Value></
                   SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
                   >
43              <
                    SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
                    >
44              <Key>DEVICE2</Key>
45              <Value>
46                  <VUEMUserAssignedPrinter>
47                      <IdPrinter>1</IdPrinter>
48                      <IdSite>1</IdSite>
49                      <State>1</State>
50                      <ActionType>0</ActionType>
51                      <UseExtCredentials>0</UseExtCredentials>
52                      <isDefault>0</isDefault>
53                      <IdFilterRule>1</IdFilterRule>
54                      <RevisionId>1</RevisionId>
55                      <Name>HP LaserJet 2200 Series</Name>
56                      <Description />
57                      <DisplayName />
58                      <TargetPath>\\server.example.net\HP LaserJet 2200
                           Series</TargetPath>
59                      <ExtLogin />
60                      <ExtPassword />
61                      <Reserved01>&lt;?xml version=”1.0” encoding=”utf-8”
                           ?&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:
```



```
                                xsi=”http://www.w3.org/2001/XMLSchema-instance”
                                xmlns:xsd=”http://www.w3.org/2001/XMLSchema”&gt
                                ;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;
                                SelfHealingEnabled&lt;/Name&gt;&lt;Value&gt;0&lt
                                ;/Value&gt;&lt;/VUEMActionAdvancedOption&gt;&lt
                                ;/ArrayOfVUEMActionAdvancedOption&gt;</
                                Reserved01>
62                      </VUEMUserAssignedPrinter>
63                  </Value></
                        SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
                        >
64              </
                    ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
                    >
```

Glossary

November 21, 2019

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