Workspace Environment Management 2209

Contents

Workspace Environment Management 2209 4

What's new 4

Fixed issues 5

Known issues 6

Third party notices 6

Deprecation 6

Quick-start guide 9

System requirements 56

Install and configure 61

Infrastructure services 61

Administration console 77

Agent 81

Scale and size considerations for deployments 91

Upgrade a deployment 92

User experience 96

Ribbon 96

Actions 101

Action Groups 101

Group Policy Settings 113

Applications 119

Printers 123

Network Drives 125

Virtual Drives 126

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Registry Entries 127

Environment Variables 129

Ports 130

Ini Files 132

External Tasks 133

File System Operations 139

User DSN 141

File Associations 142

Filters 146

Assignments 148

System Optimization 150

CPU Management 151

Memory Management 156

I/O Management 159

Fast Logoff 160

Citrix Optimizer 160

Multi-session Optimization 163

Policies and Profiles 163

Environmental Settings 164

Microsoft USV Settings 166

Citrix Profile Management Settings 167

Security 175

Active Directory Objects 192

Transformer settings 195

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Advanced settings 199

Administration 209

Monitoring 216

Agent in CMD and UI mode 219

Common Control Panel applets 221

Dynamic tokens 223

Environmental Settings registry values 232

Filter conditions 255

FIPS support 270

Load balancing with Citrix ADC 274

Log parser 276

Port information 277

View log files 279

WEM Integrity Condition List Manager 286

XML printer list configuration 302

Glossary 306

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Workspace Environment Management 2209

November 16, 2022

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.

What's new

December 6, 2022

What's new in 2209

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

Ability to import Group Policy settings from registry files

Starting with this release, you can convert registry values that you export using the Windows Registry Editor into GPOs for management and assignment. If you are familiar with the **Import registry files** option available with Registry Entries, this feature:

- Lets you import registry values under both `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`.
- Lets you import registry values of the `REG_BINARY` and `REG_MULTI_SZ` types.
- Supports converting delete operations associated with registry keys and values that you define in .reg files.

For more information, see Group Policy Settings.

External task

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

For more information, see External Tasks.

Profile Management

Workspace Environment Management now supports all versions of Profile Management through 2209. The following new option is now available in the **Administration Console > Policies and Profiles > Citrix Profile Management Settings > Advanced Settings** interface.

- **Enable OneDrive container**. If enabled, Profile Management roams OneDrive folders with users by storing the folders on a VHDX disk. The disk is attached during logons and detached during logoffs.

For more information, see Citrix Profile Management Settings.

Fixed issues

December 6, 2022

Workspace Environment Management 2209 contains the following fixed issues compared with Workspace Environment Management 2206:

- When you use VUEMRSAV.exe to view results about actions applied through an action group for the current user, the **Applied Actions** tab might display the incorrect source of the actions. Example: Two action groups (`Group1` and `Group 2`) were assigned to the user and `Group1` contains `Application1`. The **Applied Actions** tab might also show that `Application1` is from `Group2` even if `Group2` does not contain `Application1`. (By default, VUEMRSAV.exe is located in the agent installation folder: %ProgramFiles%\Citrix\Workspace Environment Management Agent\VUEMRSAV.exe.) [WEM-20002]
- If you assign application security rules (AppLocker rules) to built-in administrators, the rules might not take effect on the agent machine even if the logged-on user belongs to the administrators group. [WEM-21133]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- When you view the health status of Profile Management in the management console, you might see errors even if Profile Management is configured correctly. The issue occurs when the local system account under which the agent is running does not have permission to the user store. [WEM-21247]

Known issues

December 15, 2022

- In **Administration Console > Policies and Profiles > Citrix Profile Management Settings**, there is no option to add user groups for which streamed profiles and cross-platform profiles are used. [WEM-23874, WEMHELP-256]

Third party notices

December 6, 2022

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

December 6, 2022

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 cache synchronization port (applicable to Workspace Environment Management 1909 and earlier; replaced by Cached data synchronization port in Workspace Environment Management 1912 and later).	2012	**2103**	Upgrade to Workspace Environment Management 1912 or later. Note: If you use Workspace Environment Management 2103 or later, be sure to upgrade your Workspace Environment Management agent to 1912 or later.
Support for VMware Persona settings.	1906	**1909**	
Support for WEM infrastructure services on the following OS platforms: Windows Server 2008 R2 SP1, and Windows Server 2012.	4.7	**1808**	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Item	Announced in	Removed in	Alternative
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	
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

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

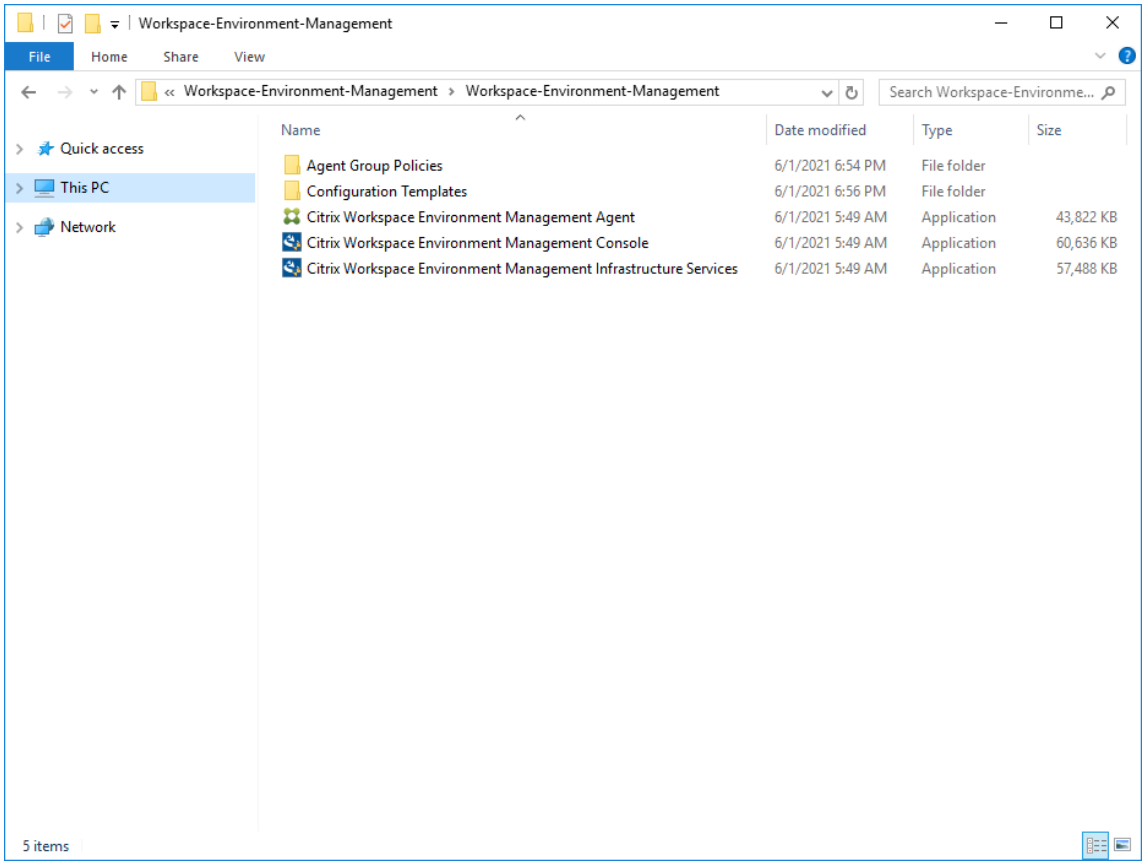
- Infrastructure services
- Administration console
- Agent

> **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 installed.

Step 1: Install the infrastructure services

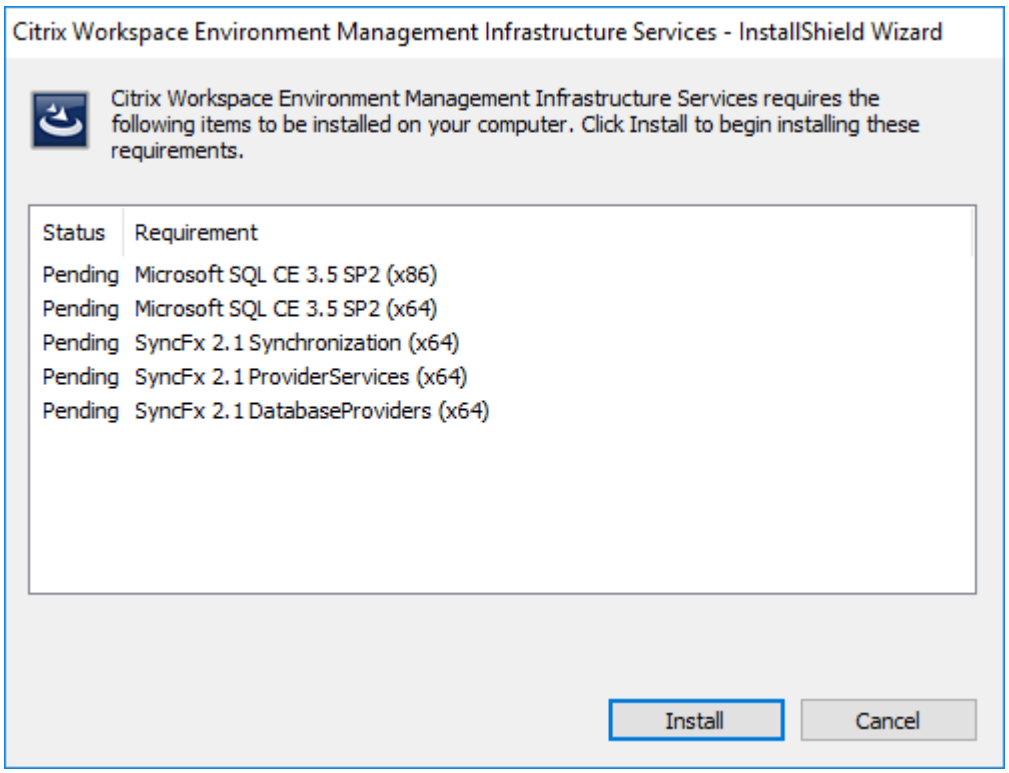
1. Download the latest WEM installer from the Citrix Virtual Apps and Desktops Advanced or Premium Edition Components downloads page https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/. Extract the zip file to a convenient folder.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

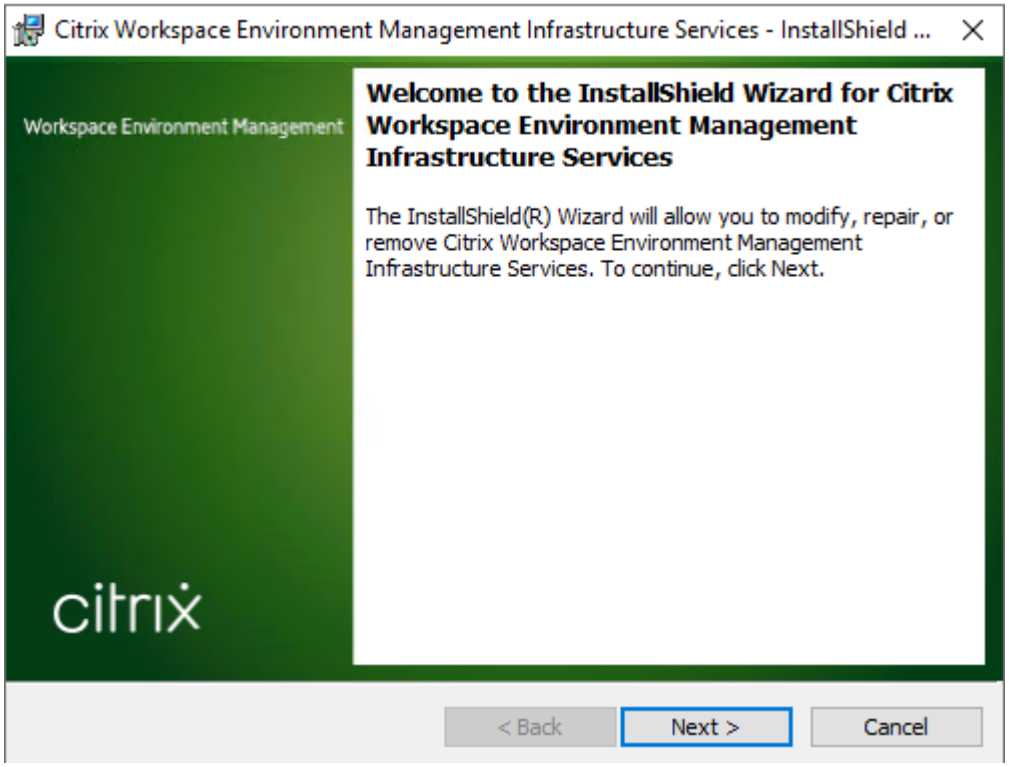


2. Run **Citrix Workspace Environment Management Infrastructure Services.exe** on your infrastructure server.
3. Click **Install**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

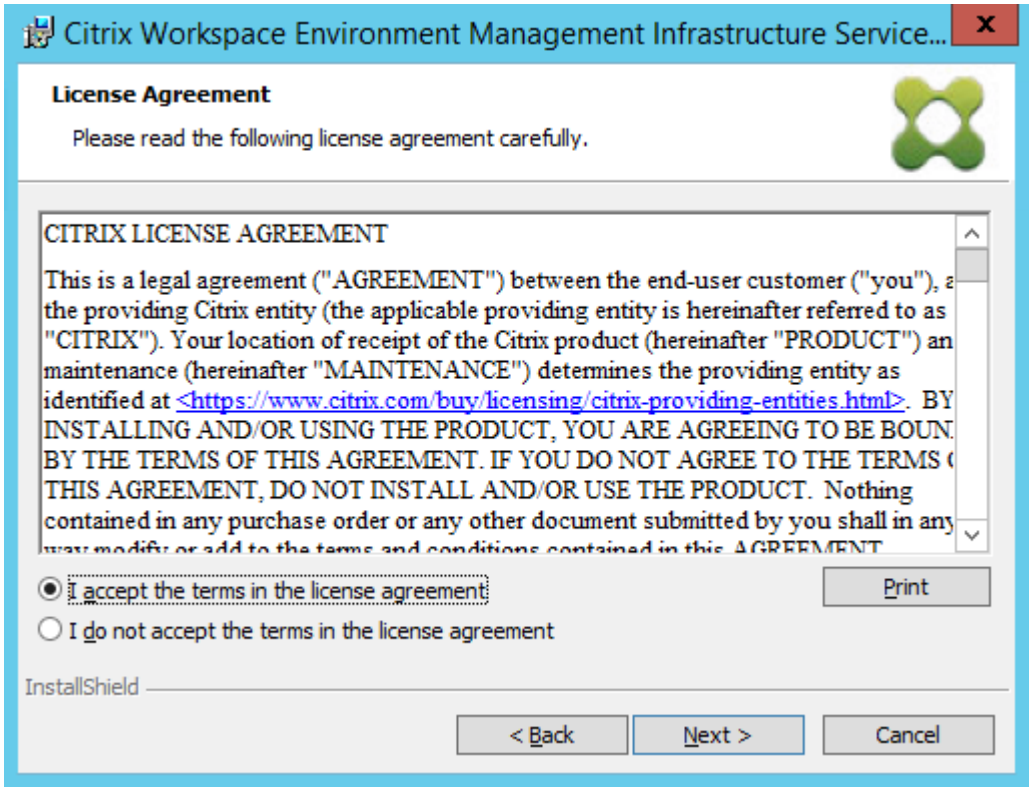


4. Click **Next**.

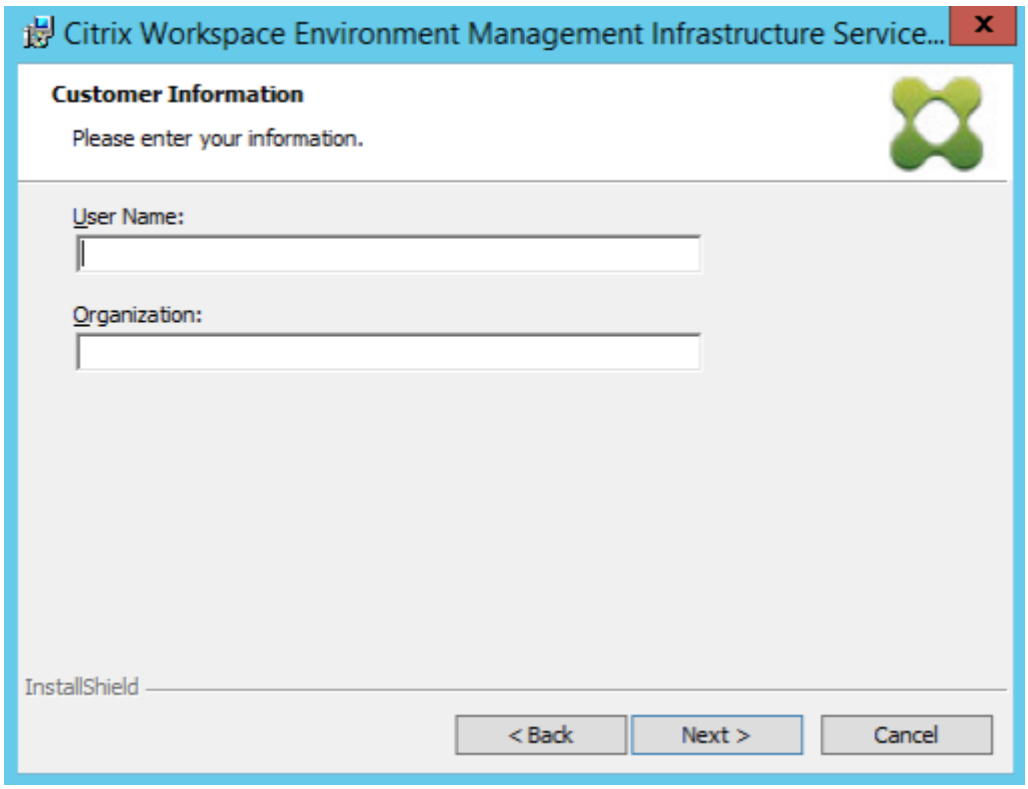


5. Select “I accept the terms in the license agreement”and then click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



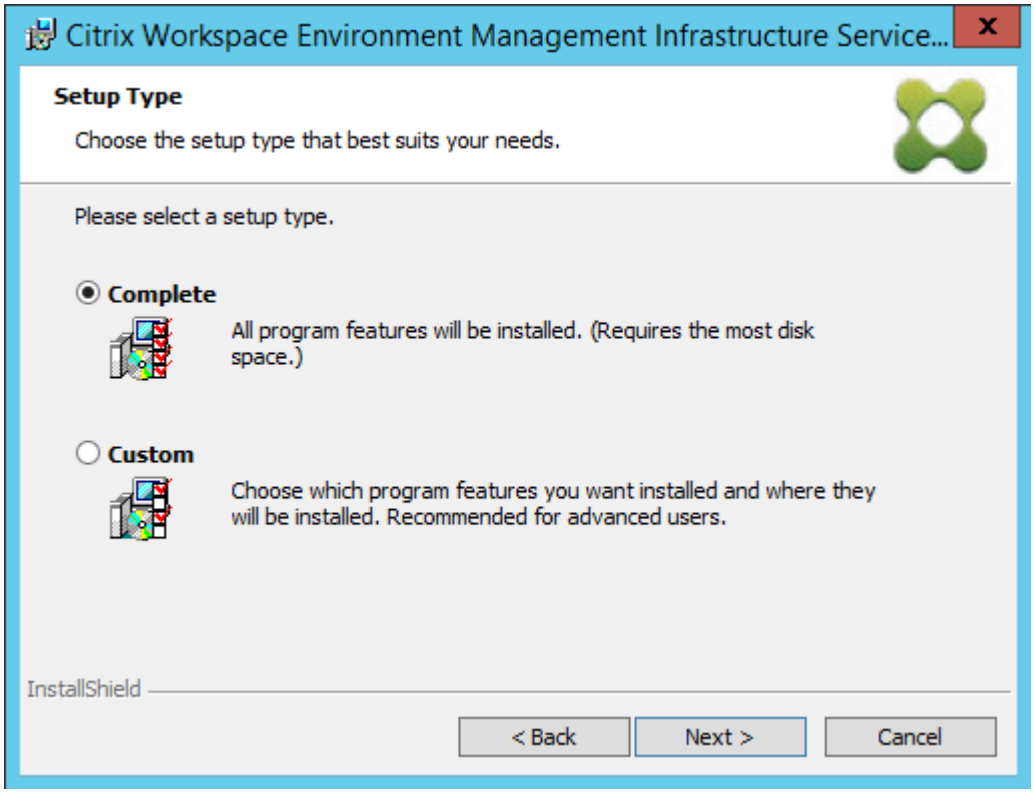
6. Type your user name and organization and then click **Next**.



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

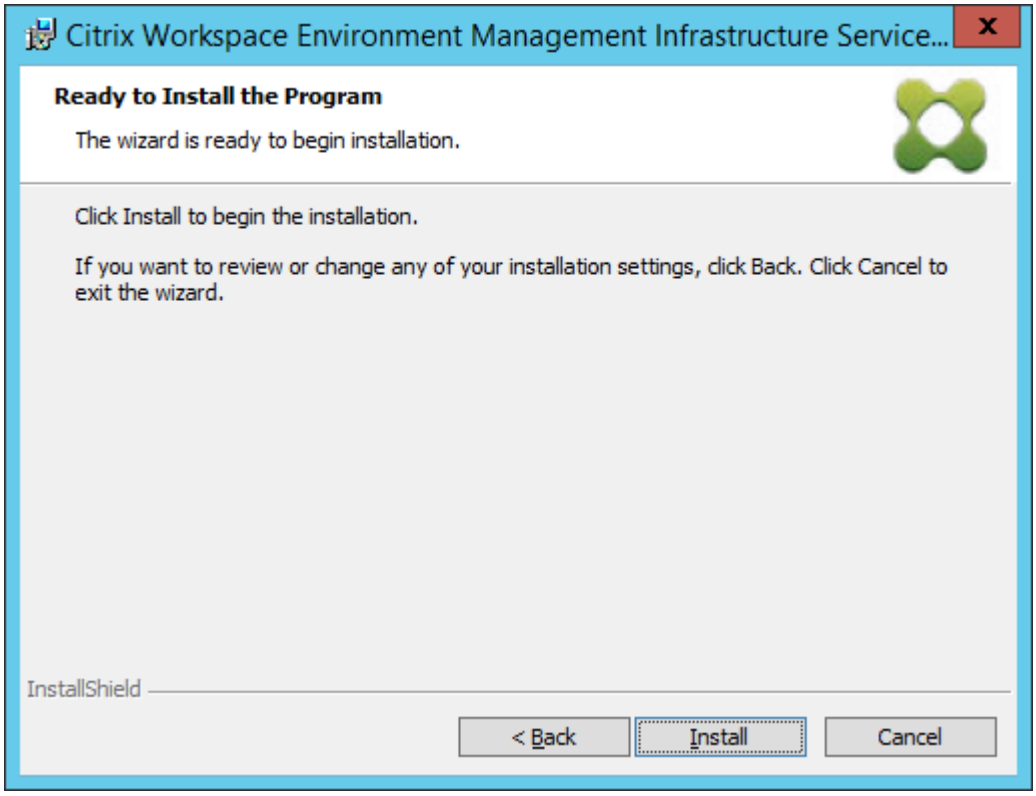
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



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

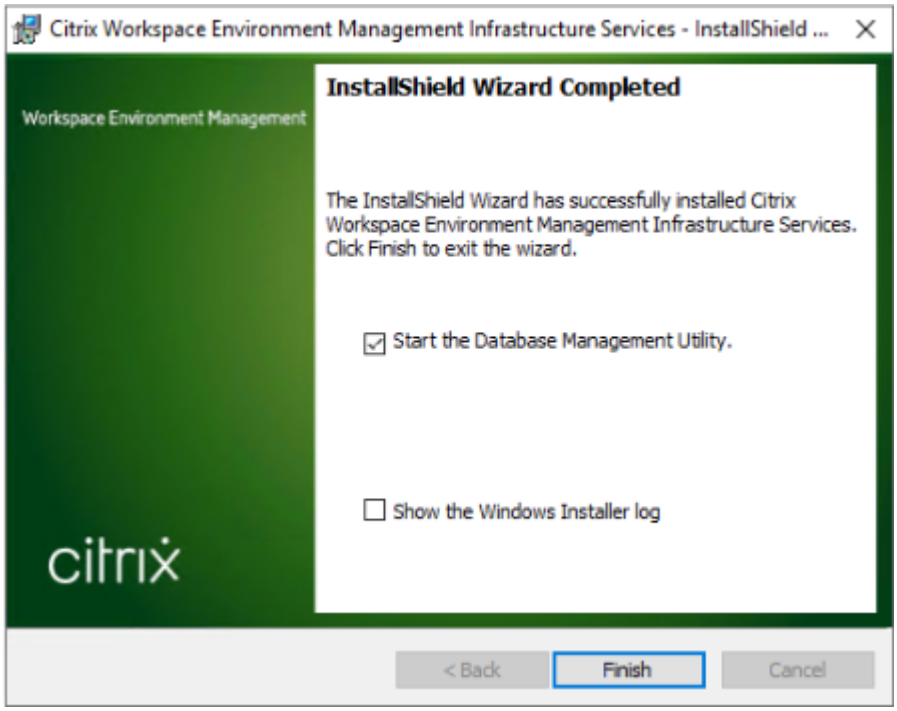
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

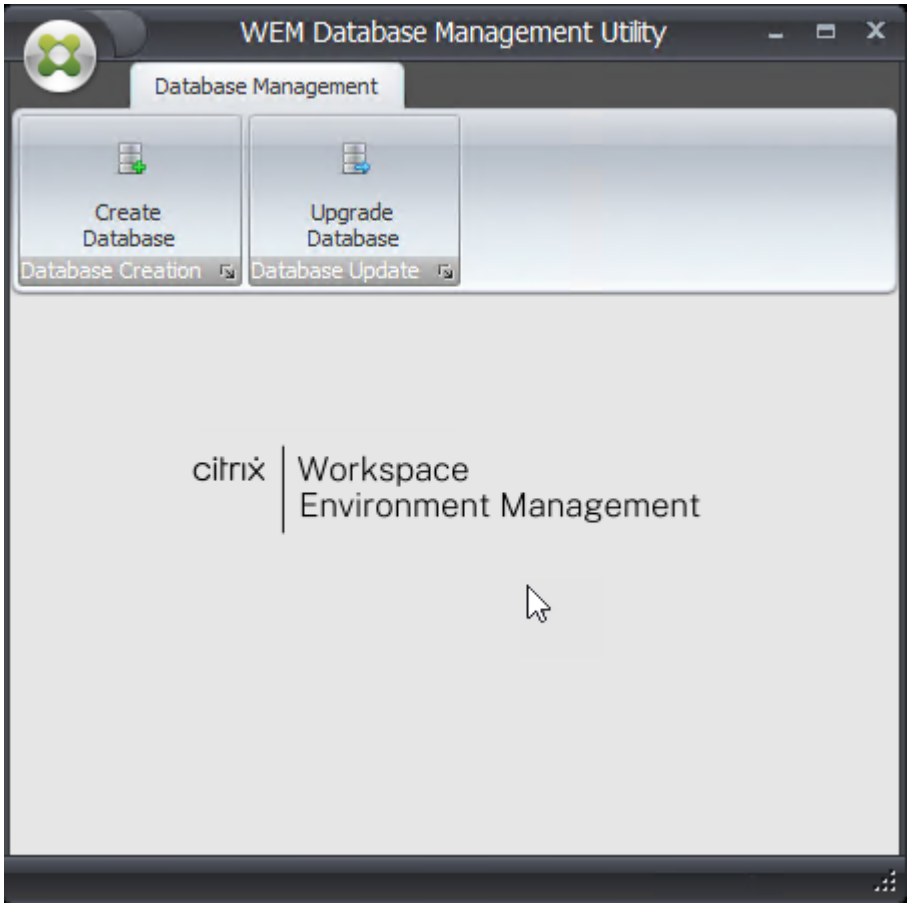


Step 2: Create a WEM database

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

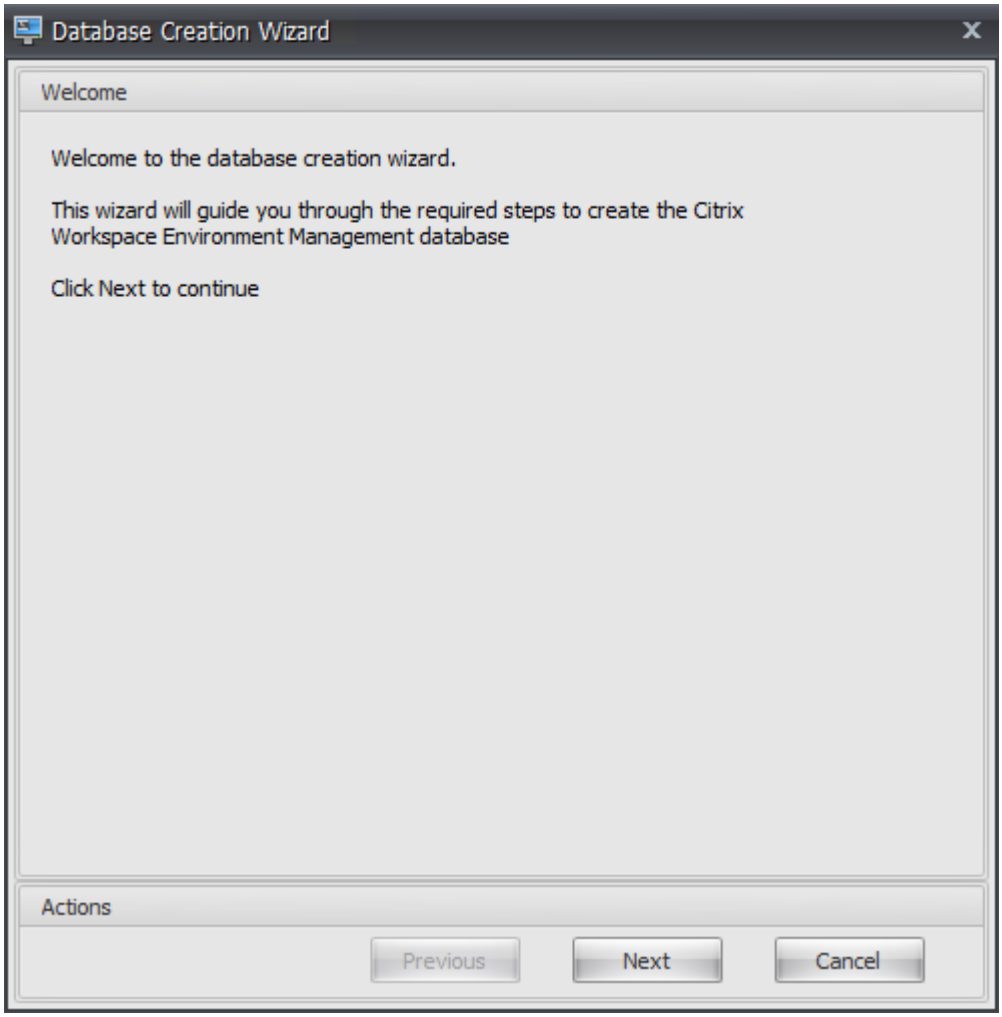
   > **Note:**
   >
   > If you are using Windows authentication for your SQL Server, run the database creation utility under an identity that has system administrator permissions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

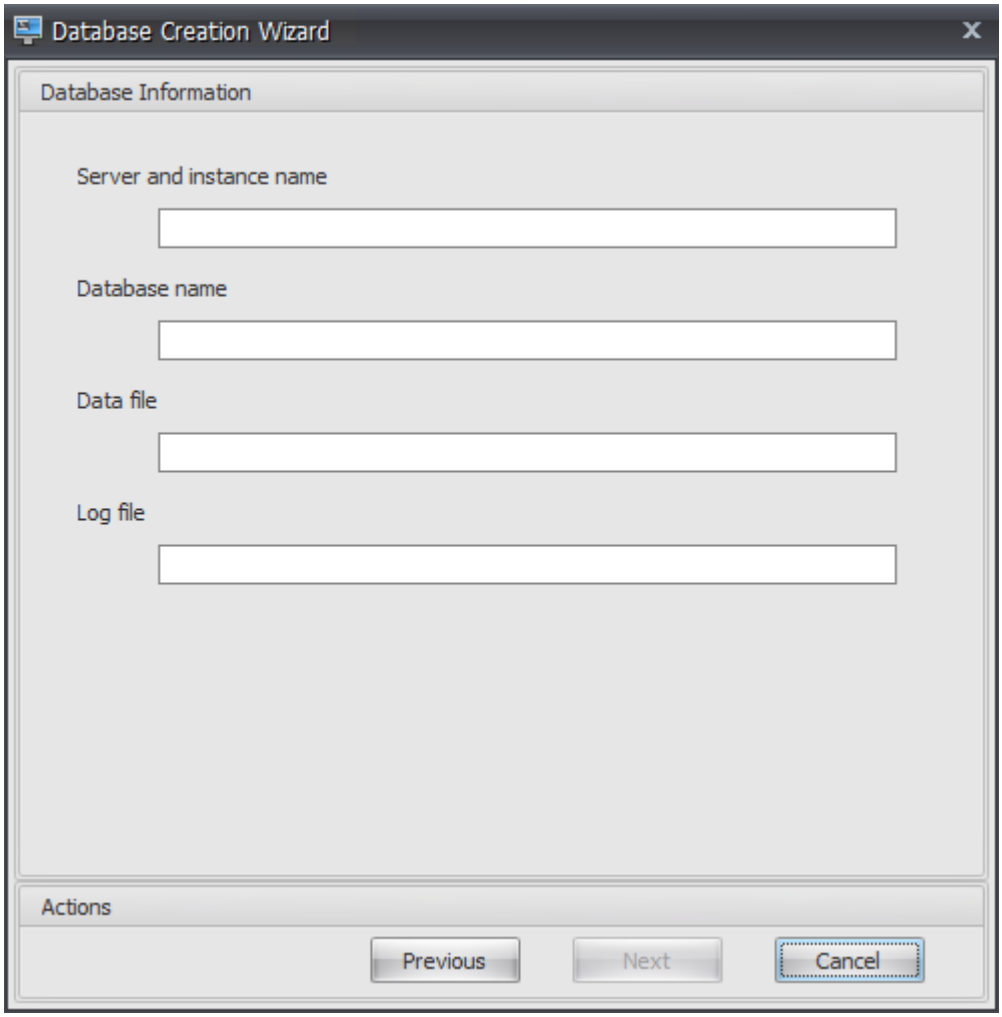
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

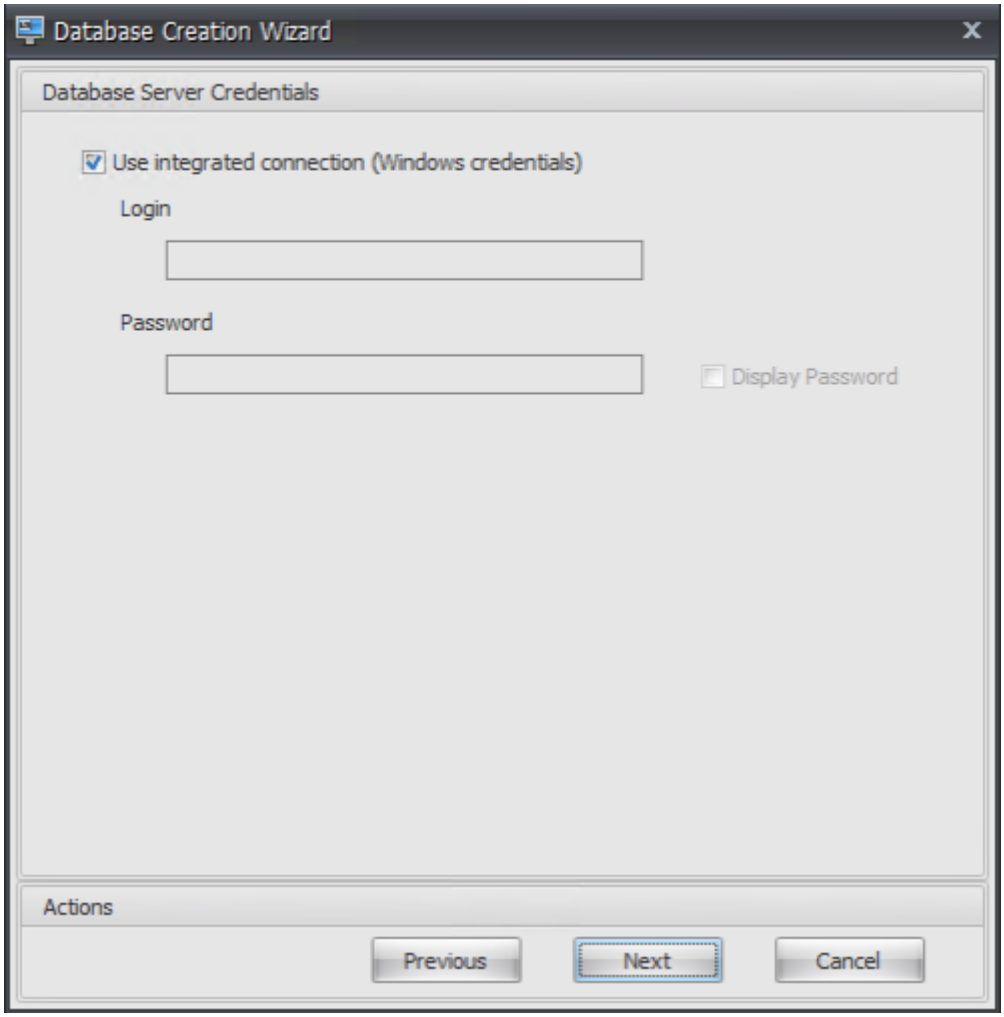
> **Note:**
>
> - For the server and instance name, type the machine name, fully qualified domain name, or IP address.
> - For the file paths, type the exact paths specified by your database administrator. Make sure that any auto-completed file paths are correct.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



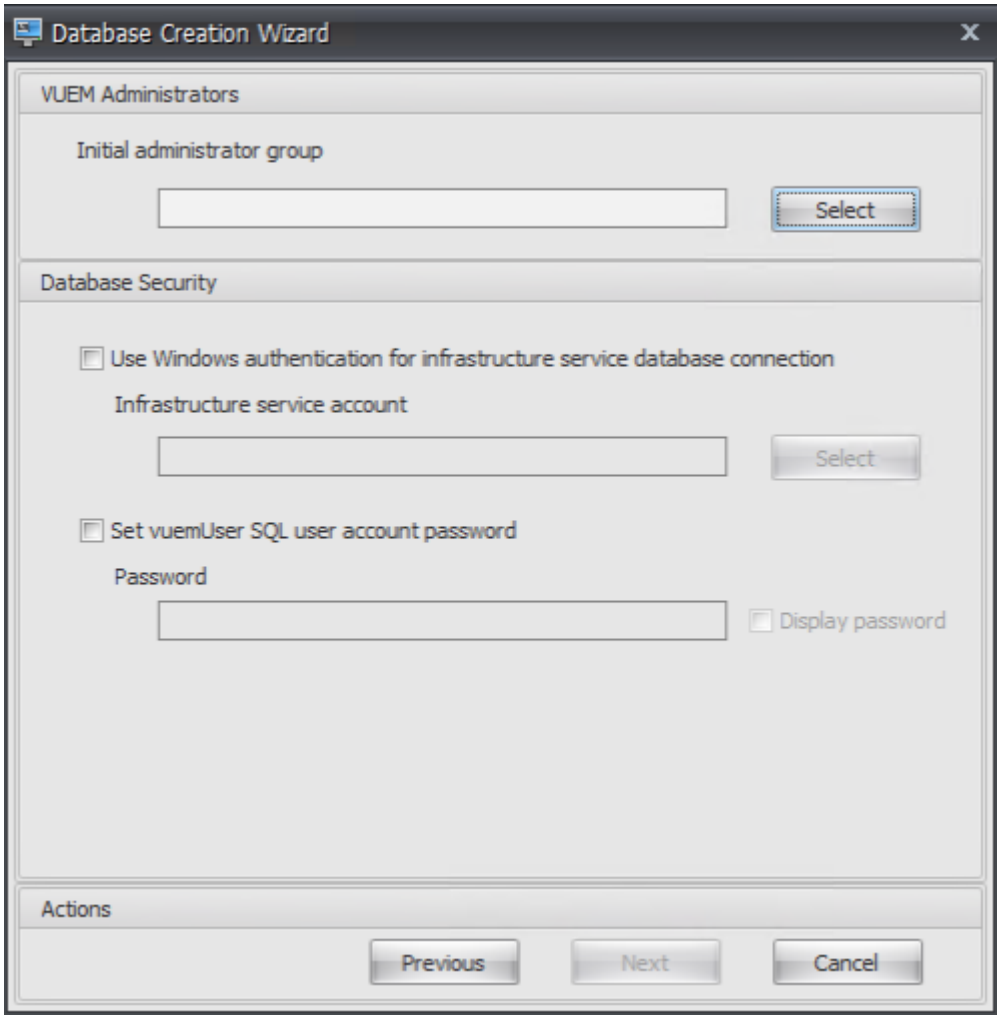
4. On the Database Server Credentials page, type the required information and then click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

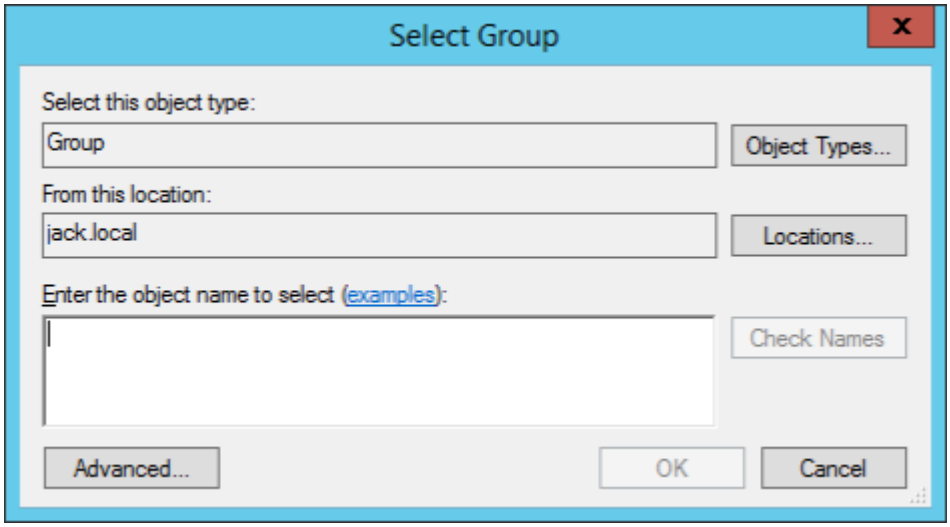


5. Under VUEM Administrators, click **Select**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

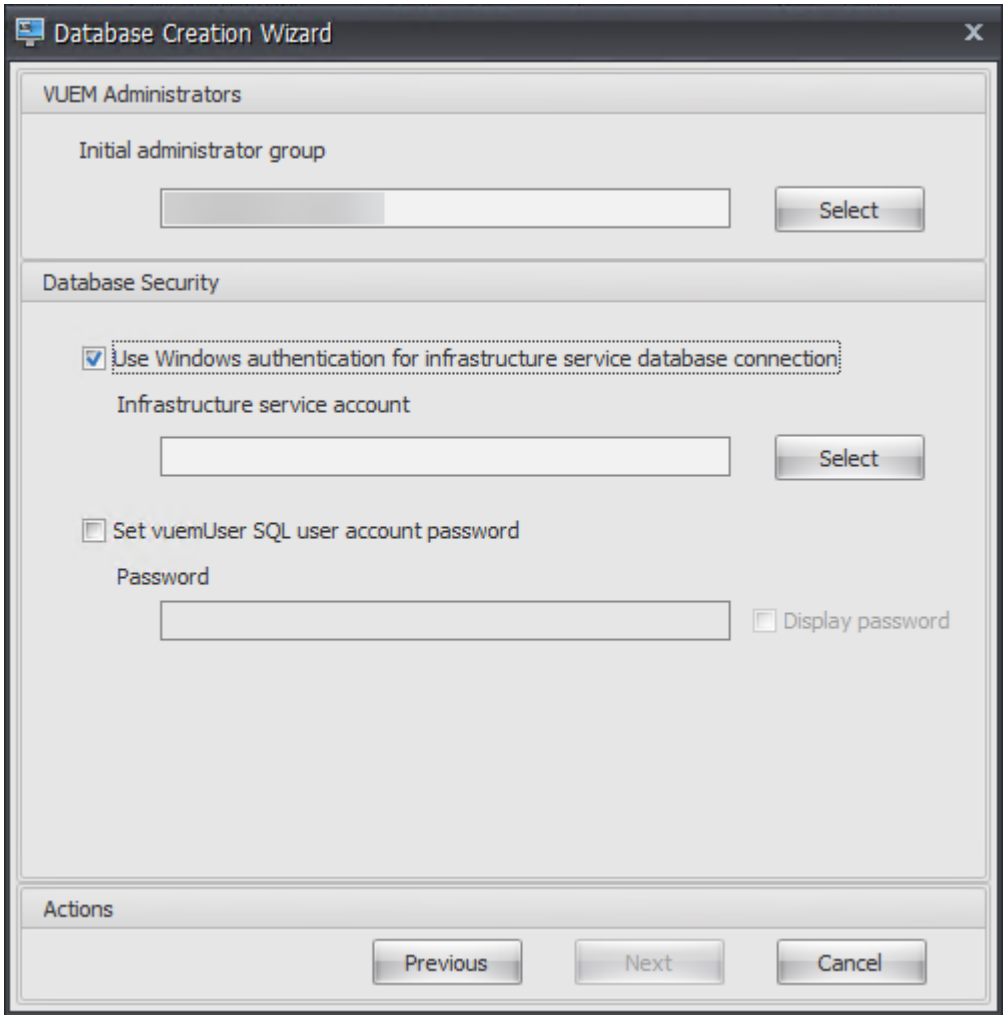


7. Under Database Security, select **Use Windows authentication for infrastructure service**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

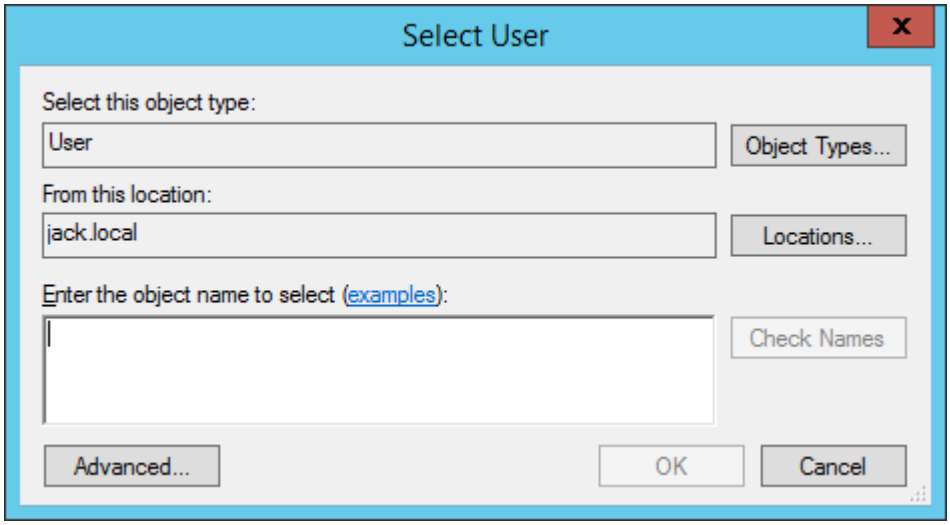
database connection and then click **Select**.

> **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**.

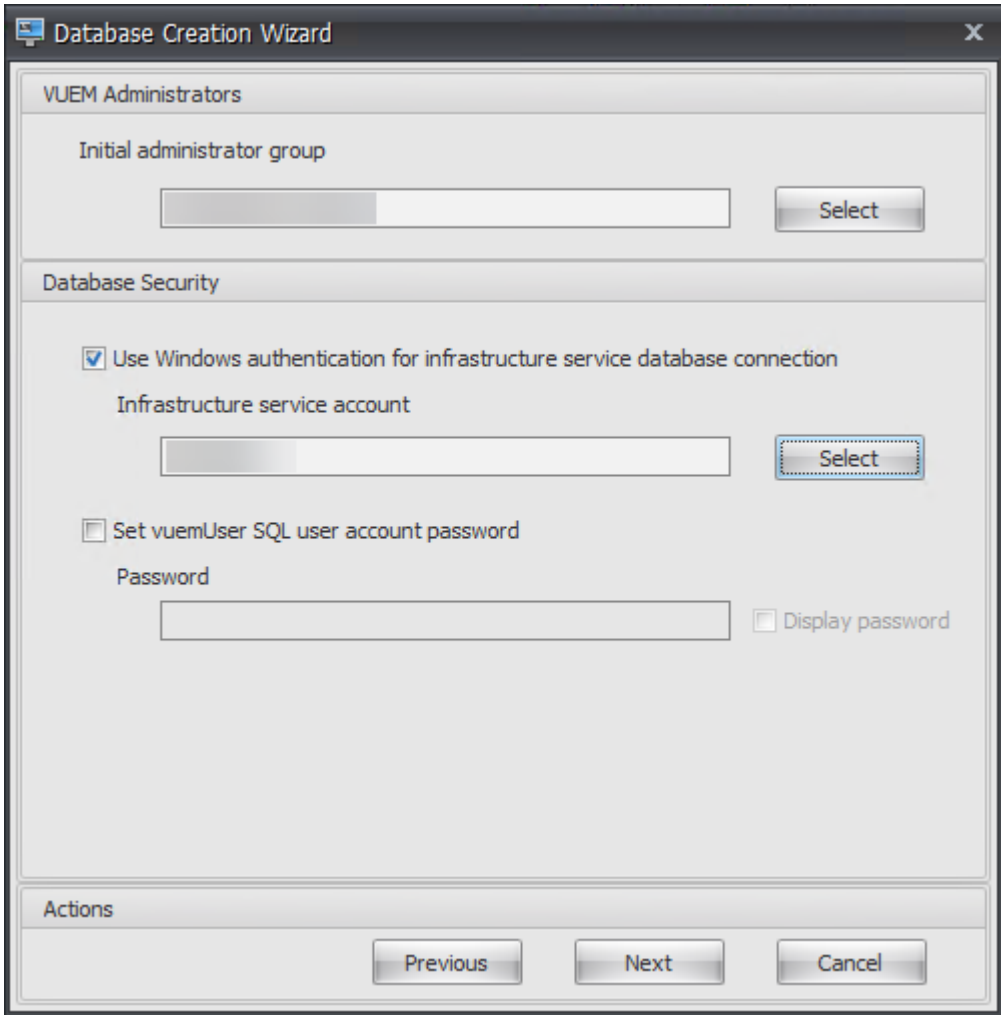


8. In the Select User window, type the name of the infrastructure service account, click **Check Names**, and then click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

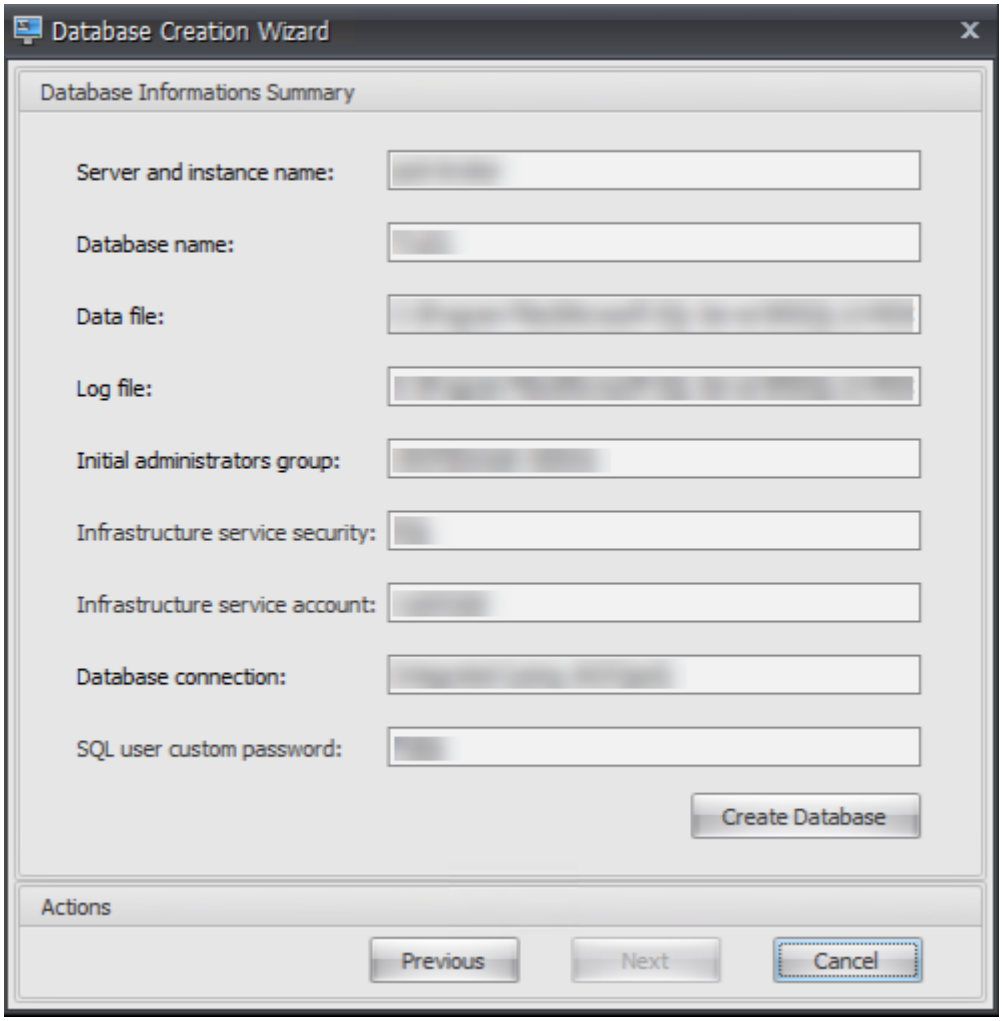


9. Click **Next**.

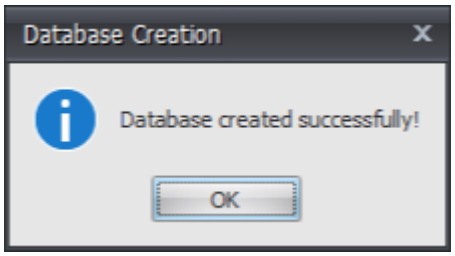


10. On the Database Information Summary page, click **Create Database**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

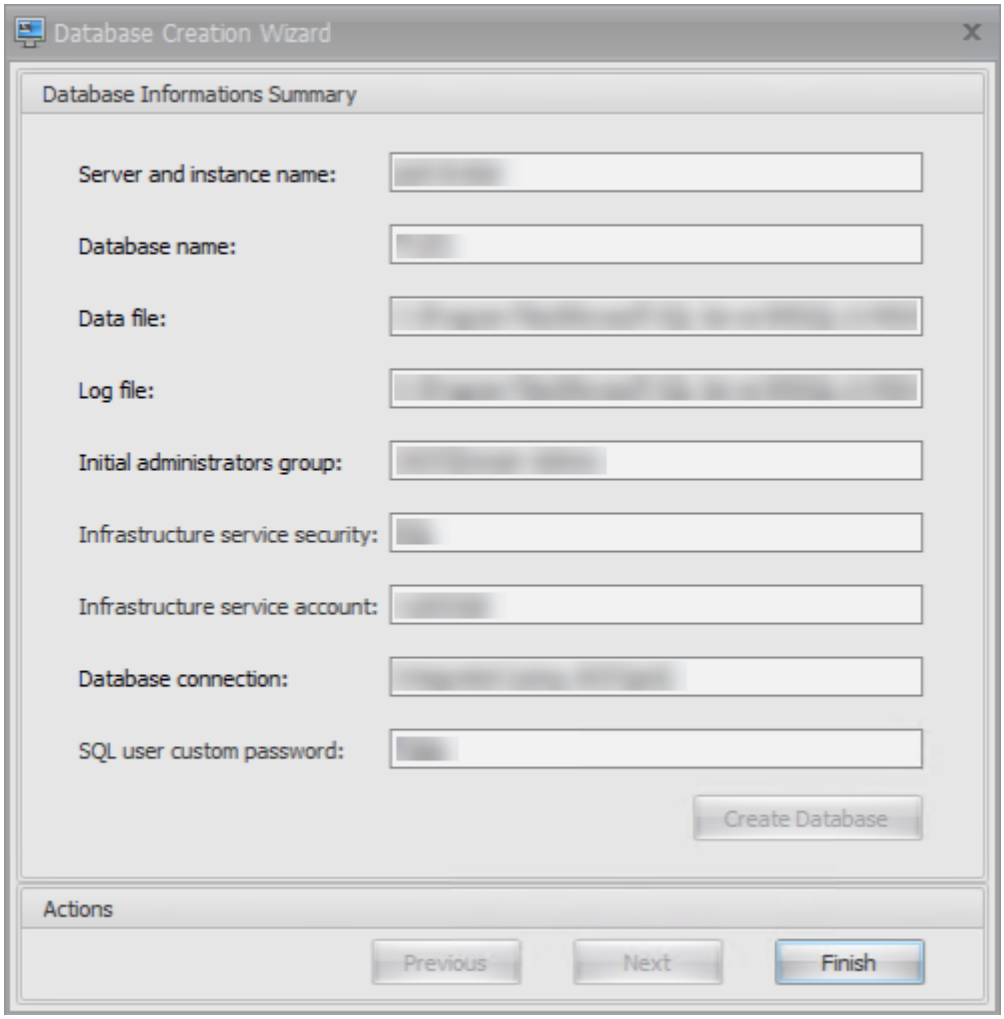


11. Click **OK**.



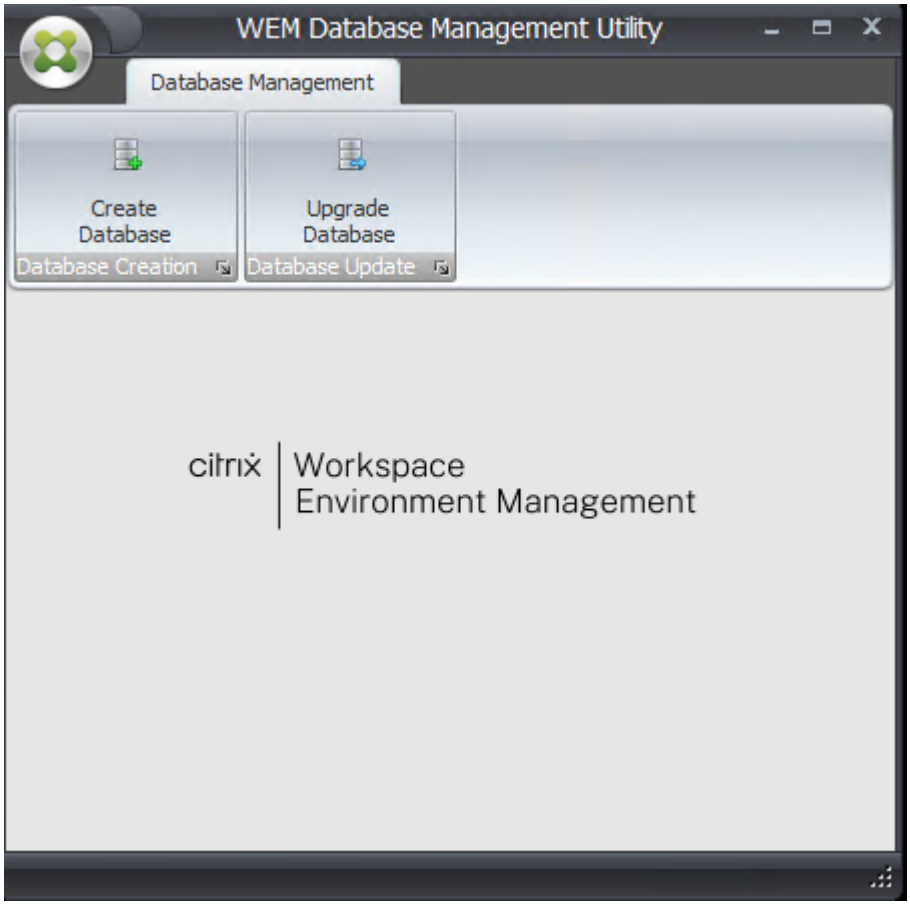
12. On the Database Information Summary page, click **Finish**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



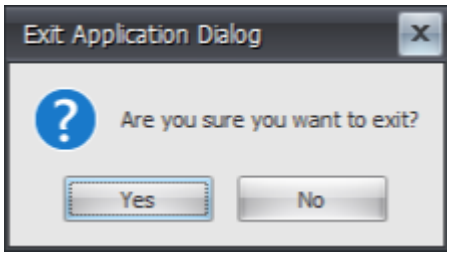
13. Close the **WEM Database Management Utility**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

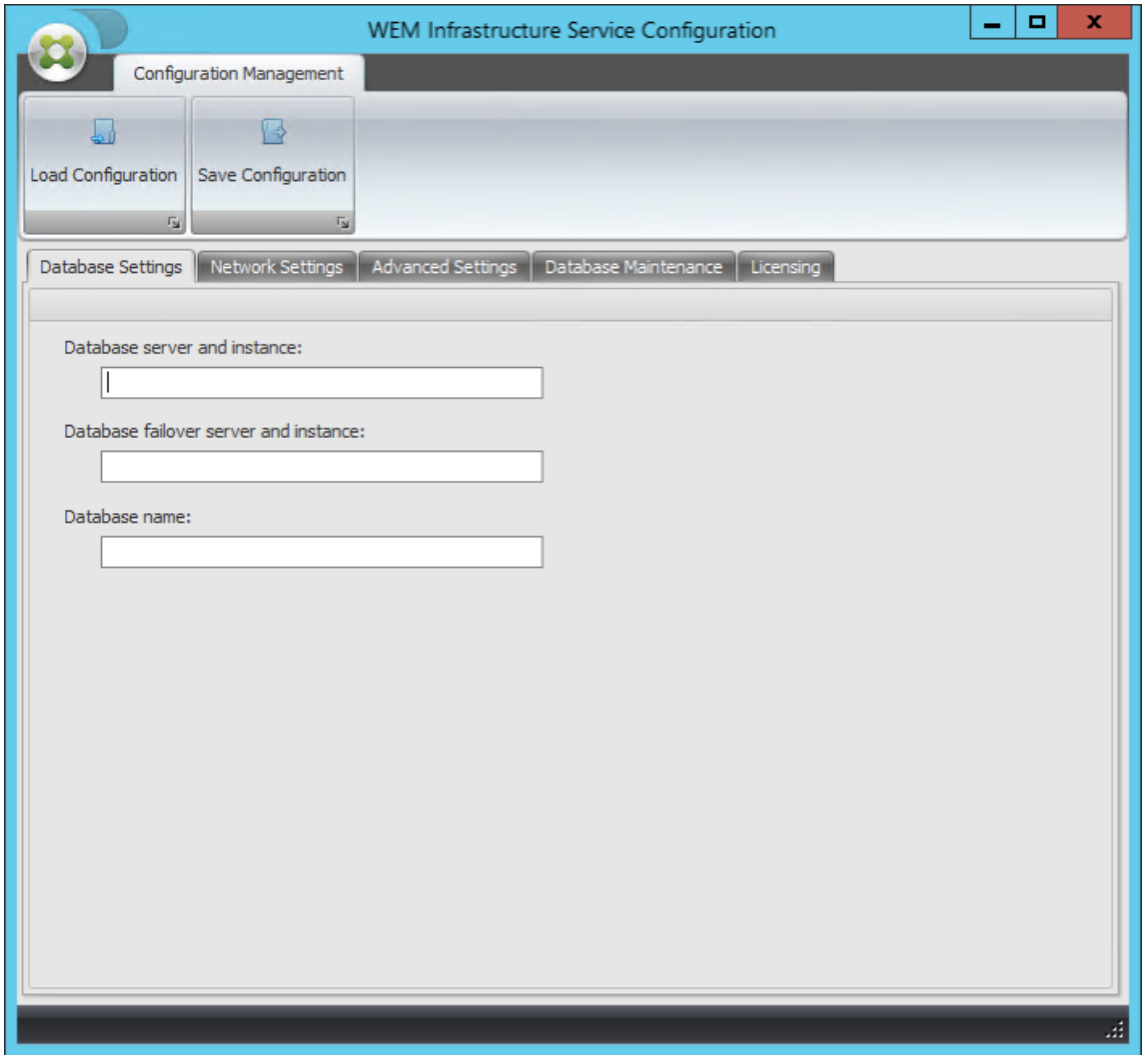
> **Note:**
>
> If an error occurs during the database creation, check the log file “Citrix WEM Database Management Utility Debug Log.log”in the infrastructure services installation folder for more information.



Step 3: Configure infrastructure services

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

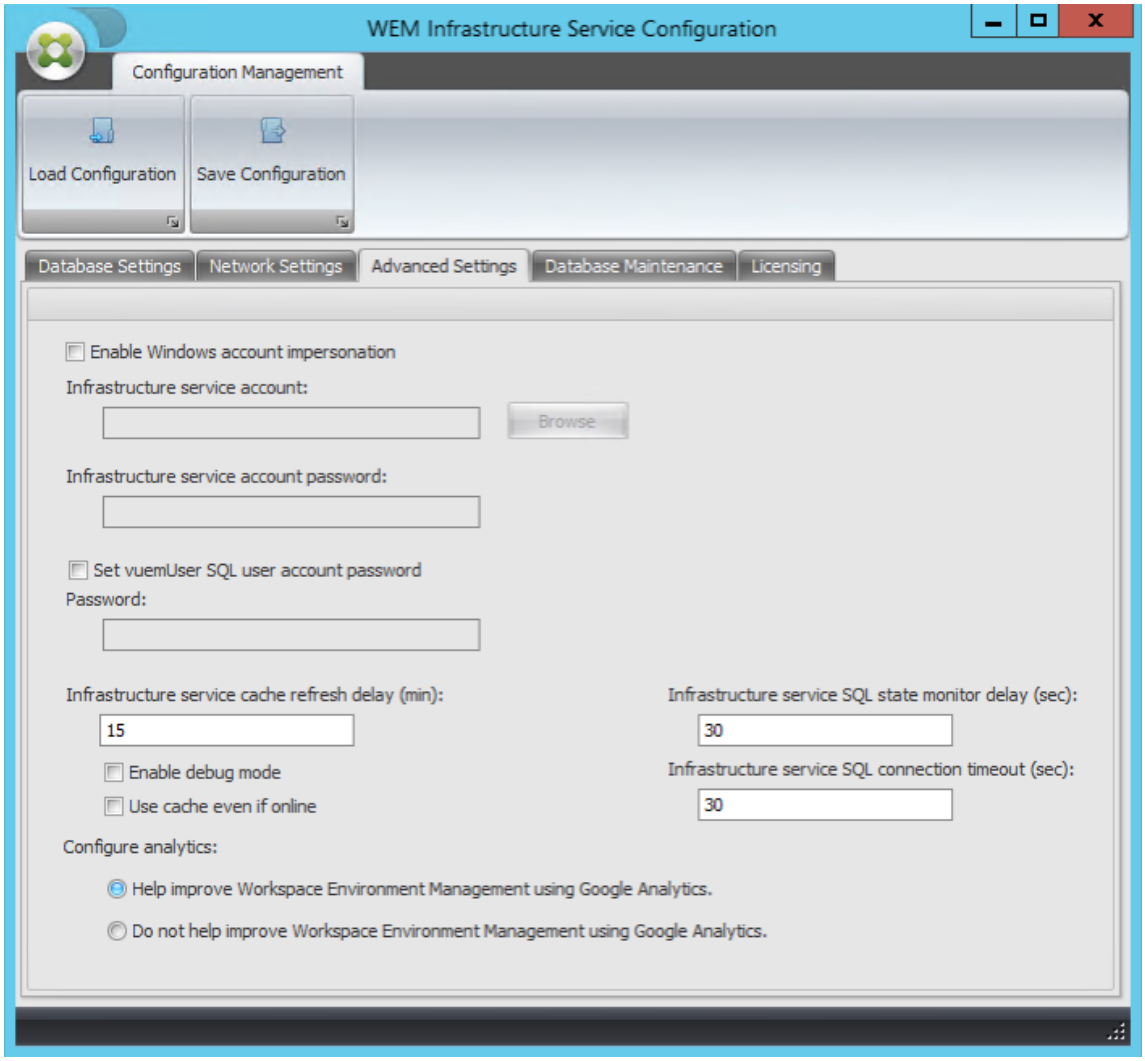
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



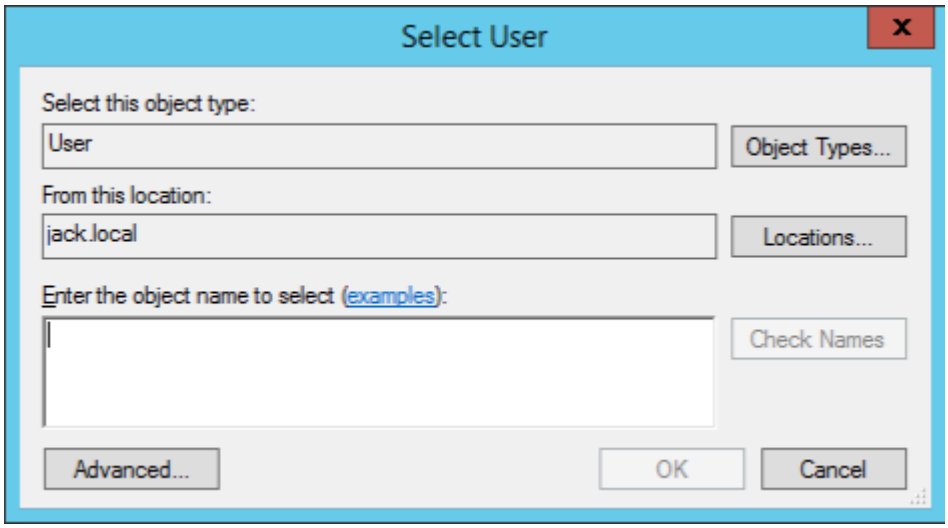
3. On the **Advanced Settings** tab, select **Enable Windows account impersonation** and then click **Browse**.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

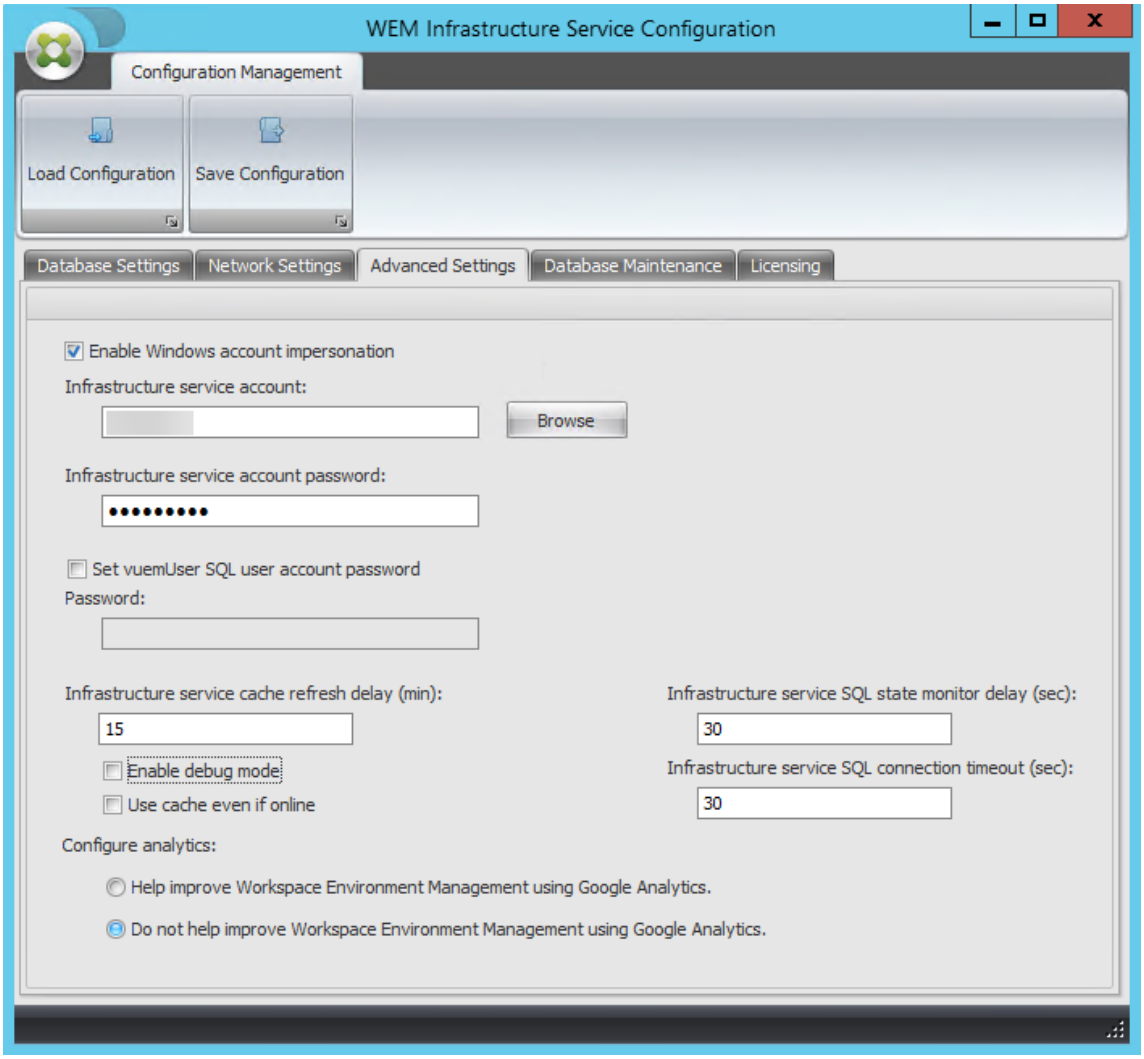


4. Type a user name, click **Check Names**, and then click **OK**.



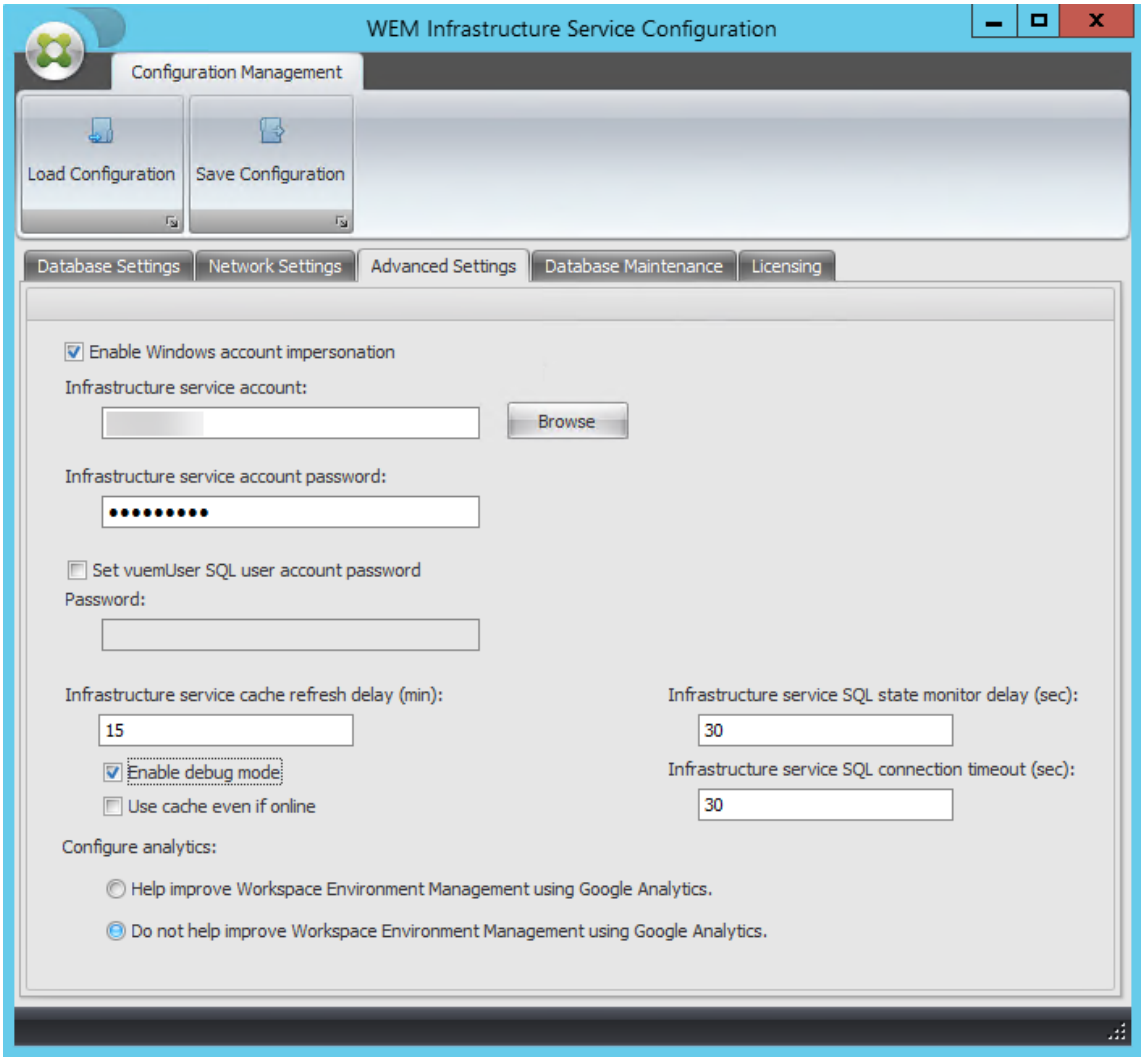
5. Type the infrastructure service account password.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Select **Enable debug mode**.

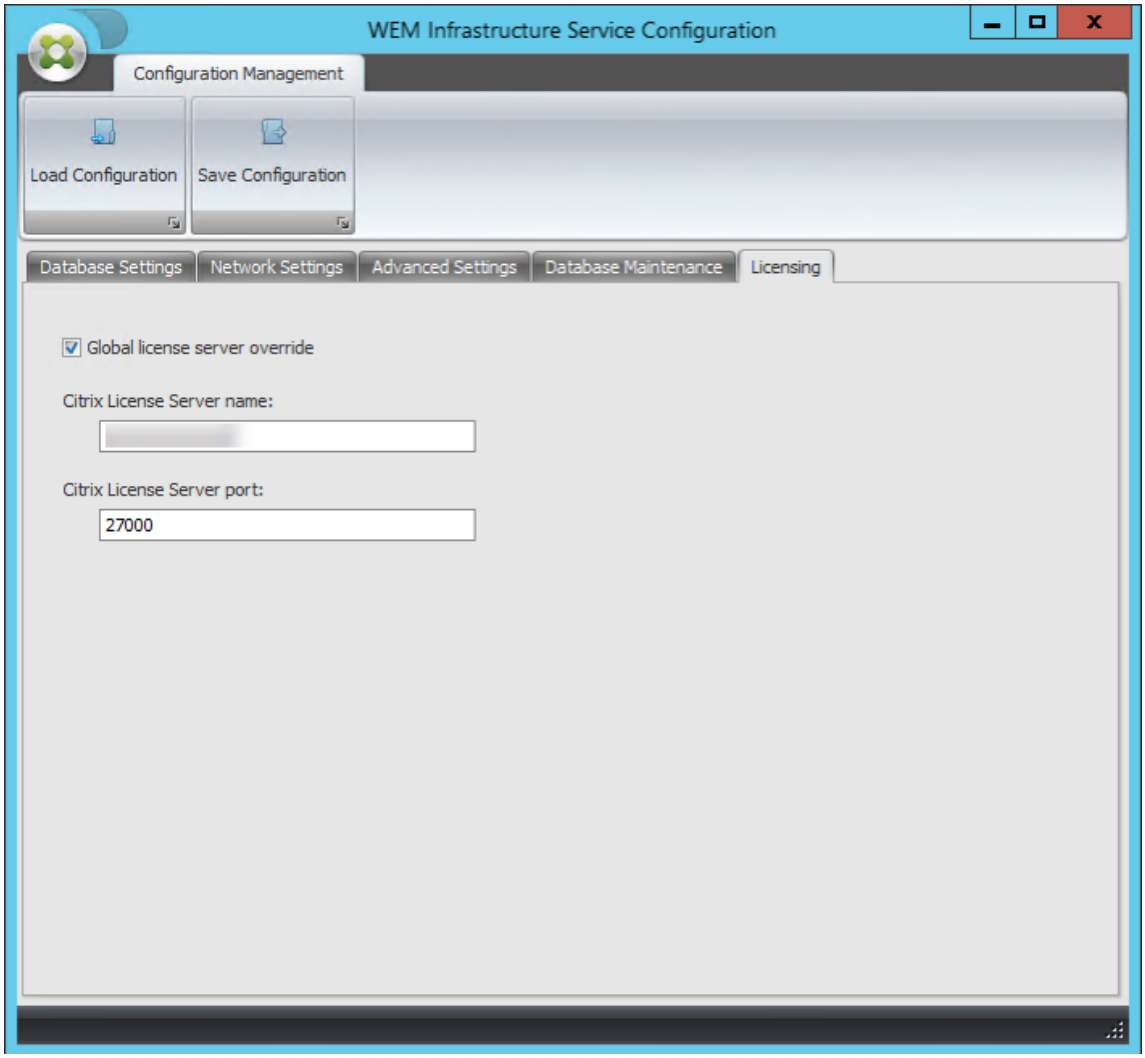
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



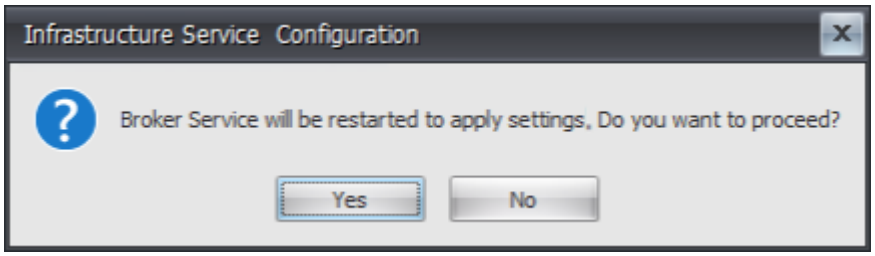
7. On the **Licensing** tab, select **Global license server override**, type your license information, and then click **Save Configuration.**

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Click **Yes**.

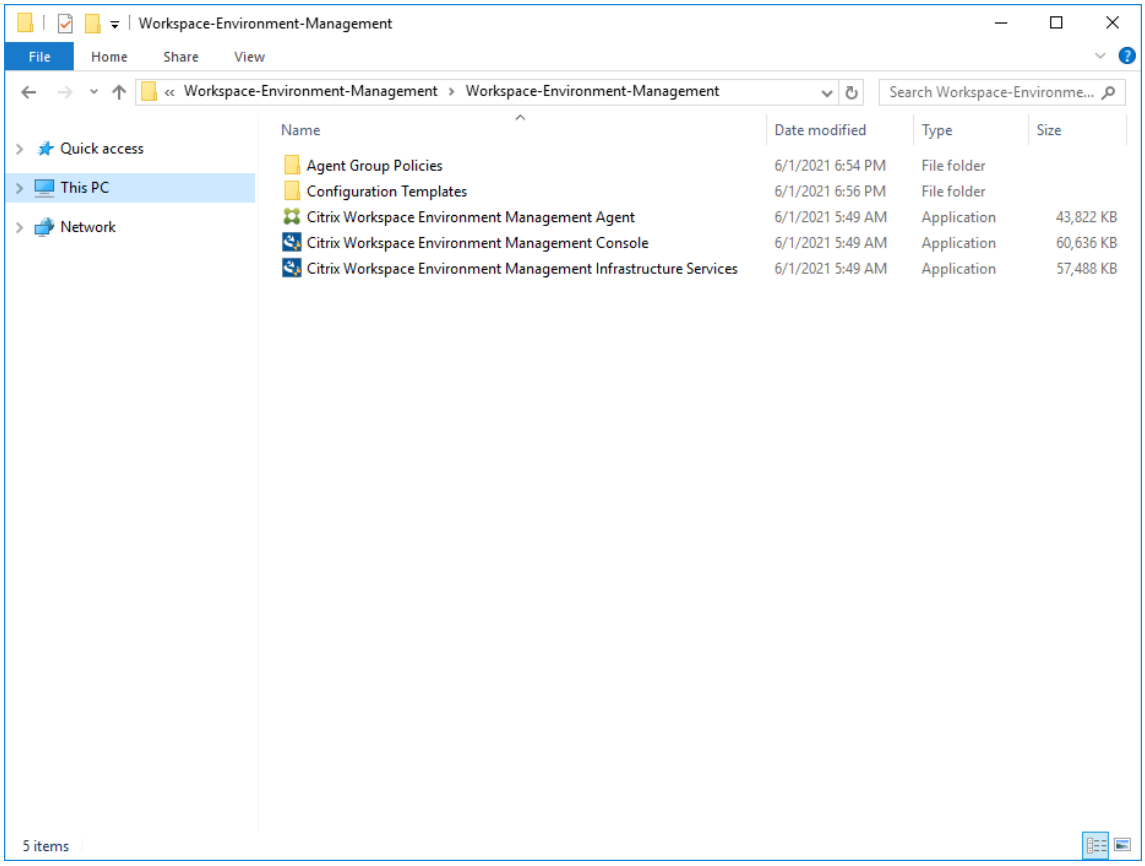


9. Close the **WEM Infrastructure Service Configuration** utility.

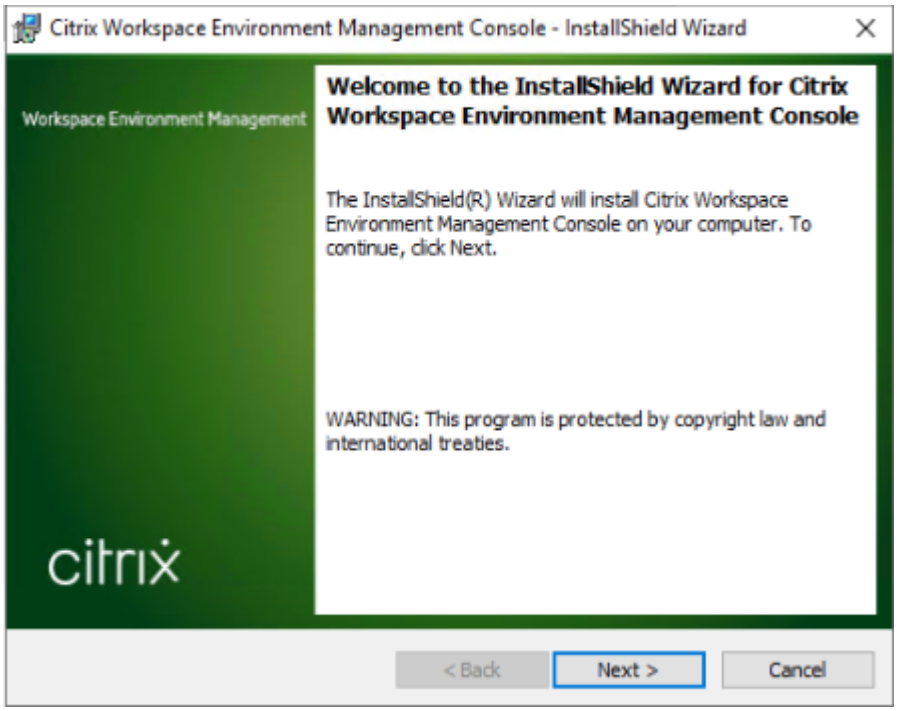
Step 4: Install the administration console

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



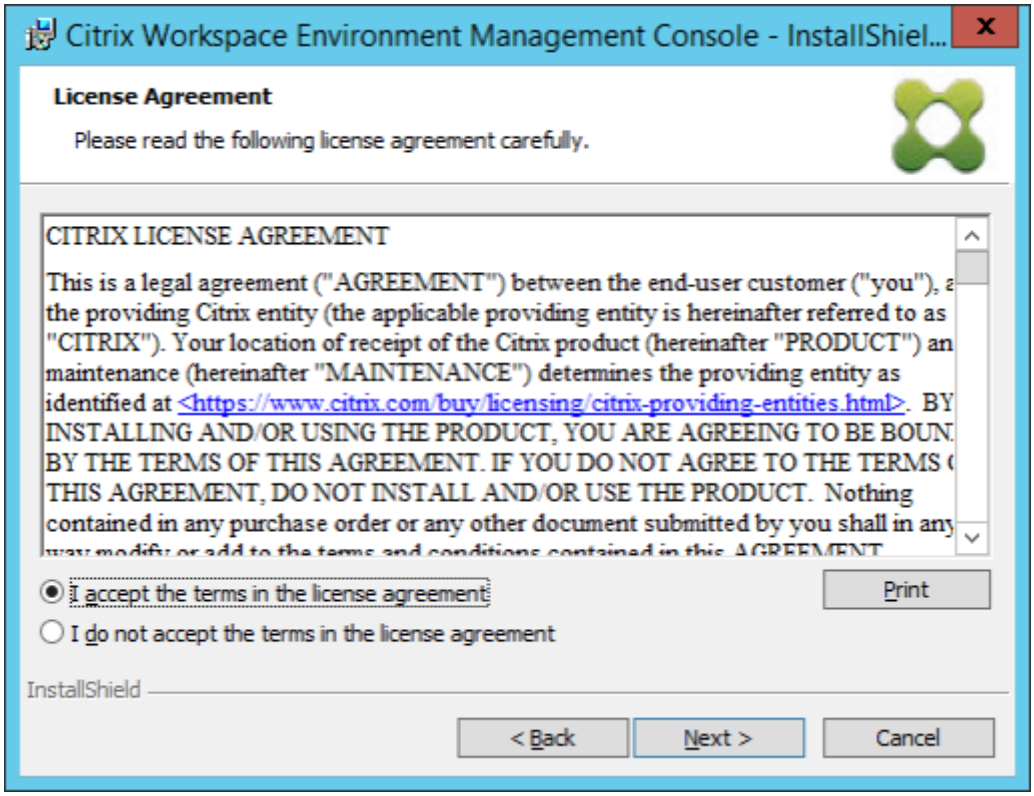
2. On the Welcome page, click **Next**.



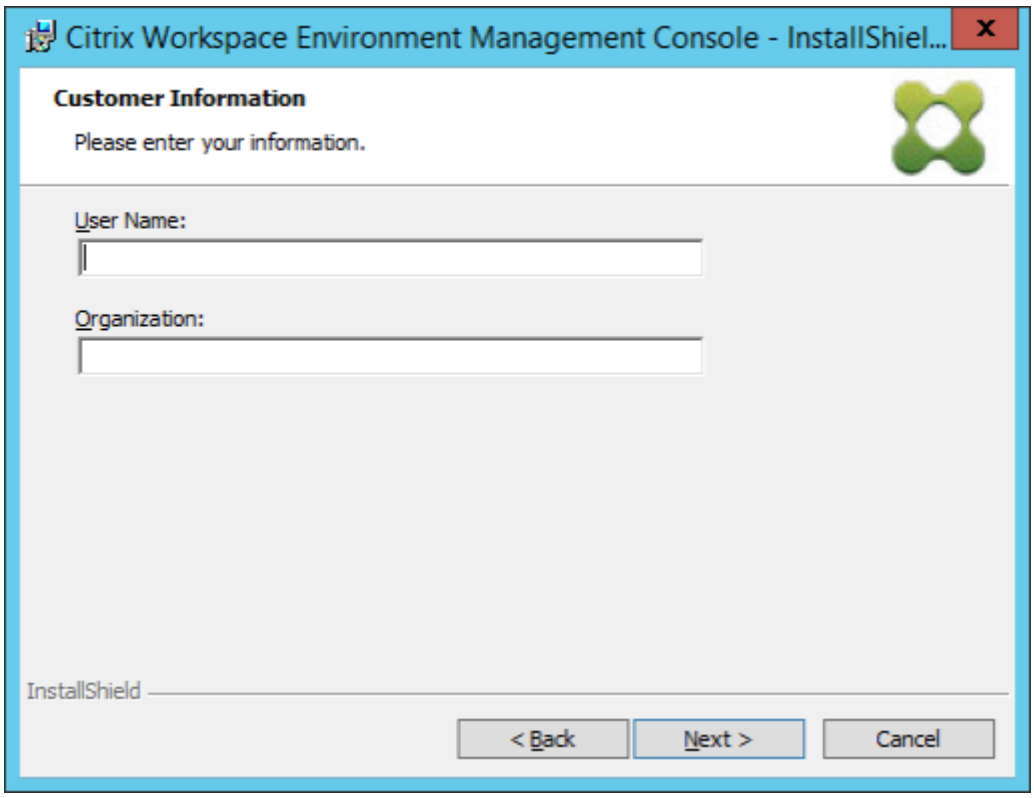
3. On the License Agreement page, select "I accept the terms in the license agreement"and then

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

click **Next**.

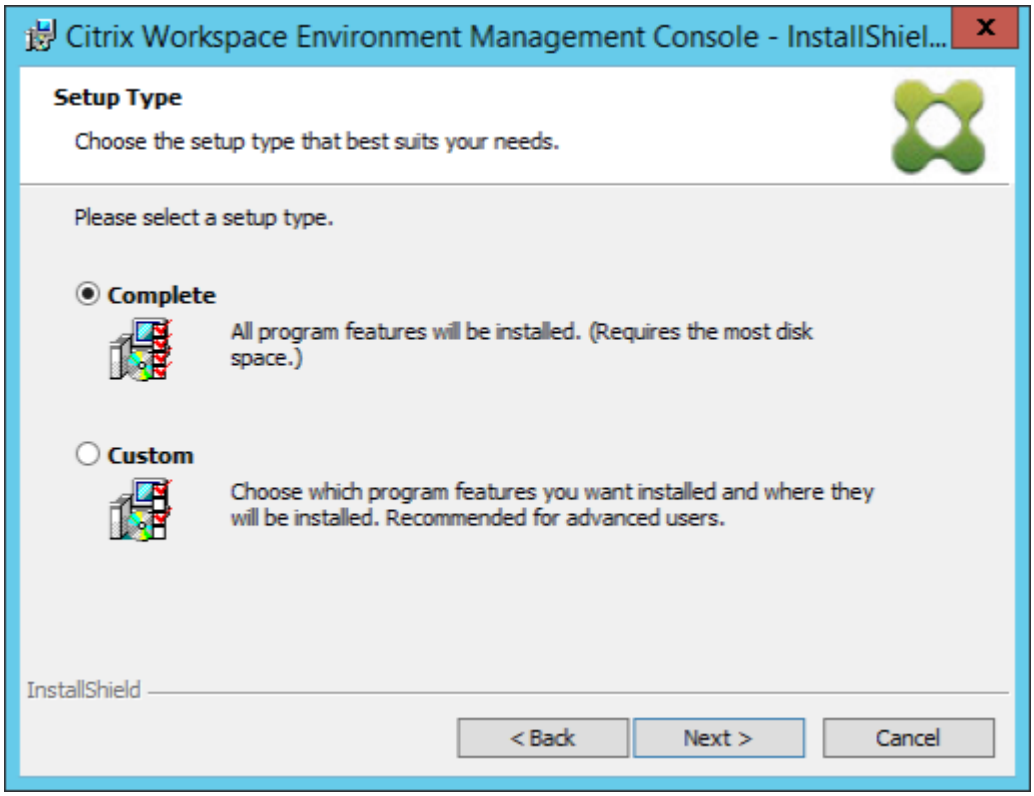


4. On the Customer Information page, type the required information and then click **Next**.

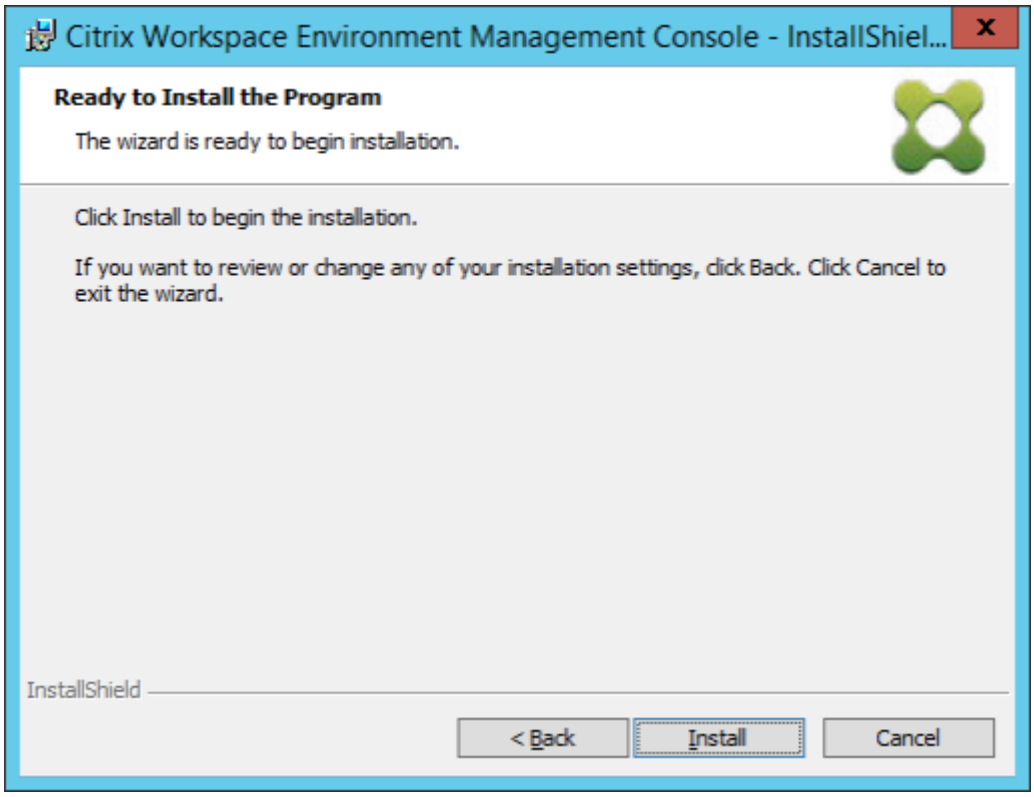


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

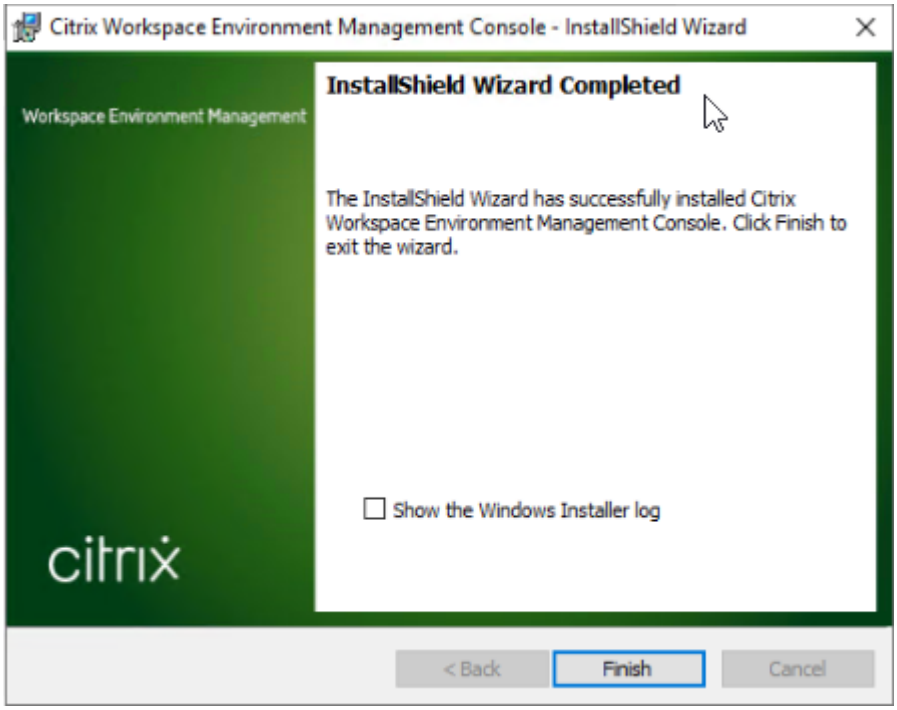


6. On the Ready to Install the Program page, click **Install**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

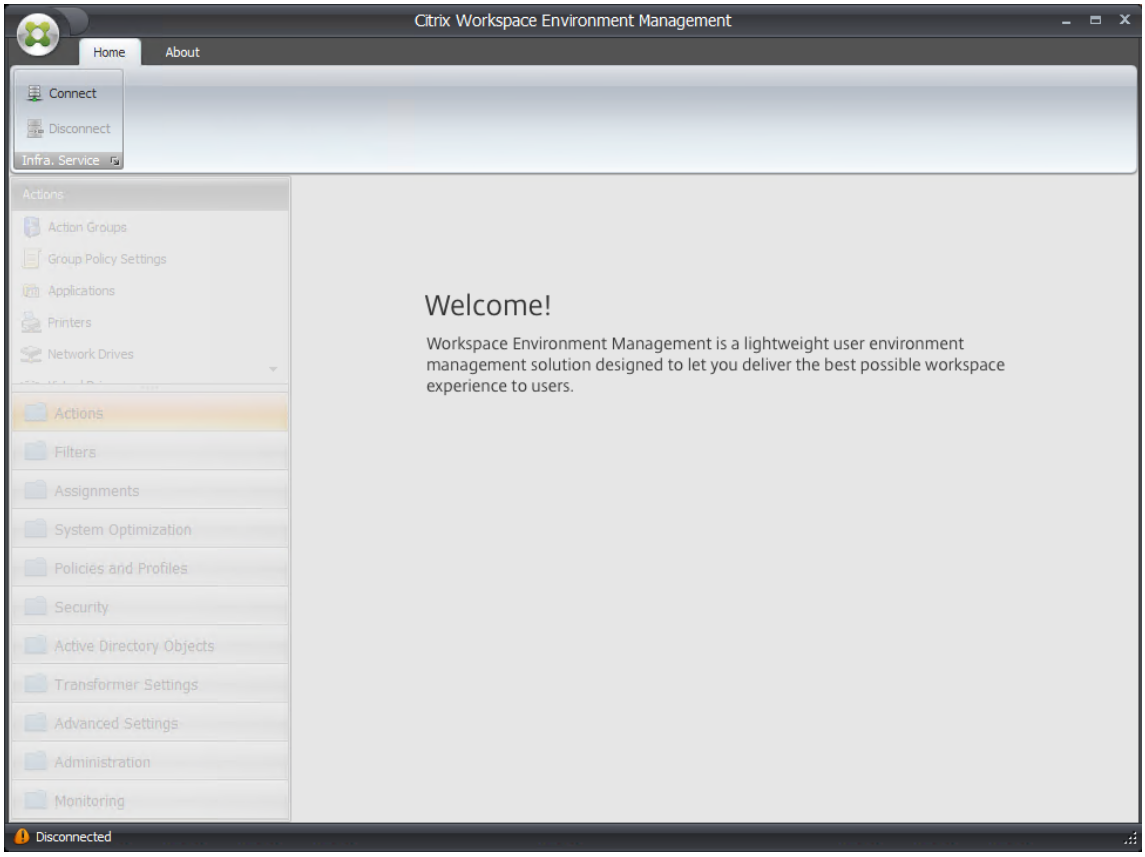
7. Click **Finish** to exit the wizard.



Step 5: Configure configuration sets

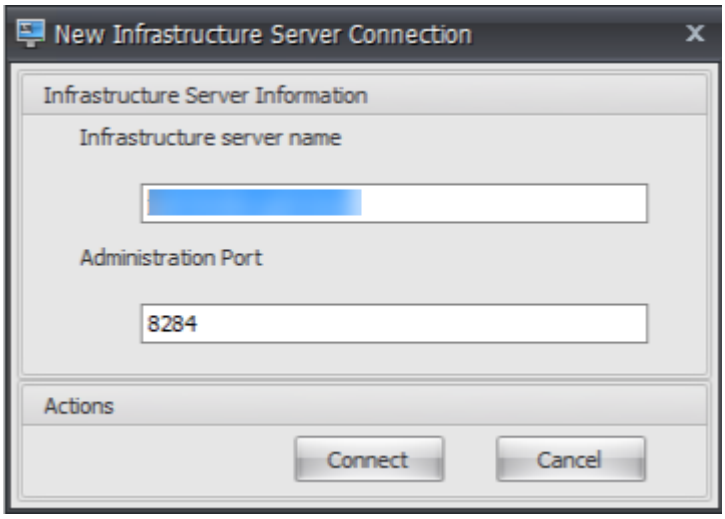
1. Open the **WEM Administration Console** from the **Start** menu and click **Connect**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



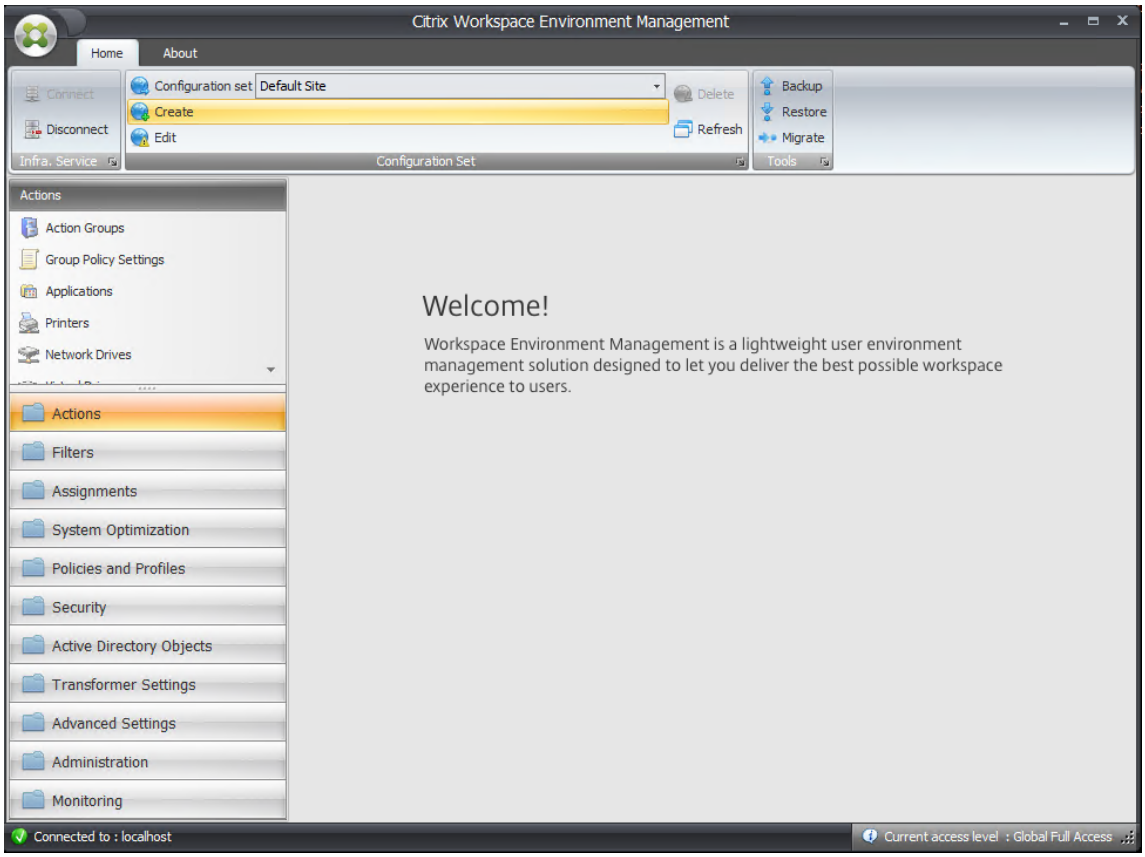
2. In the New Infrastructure Server Connection window, check the information and then click **Connect**.

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

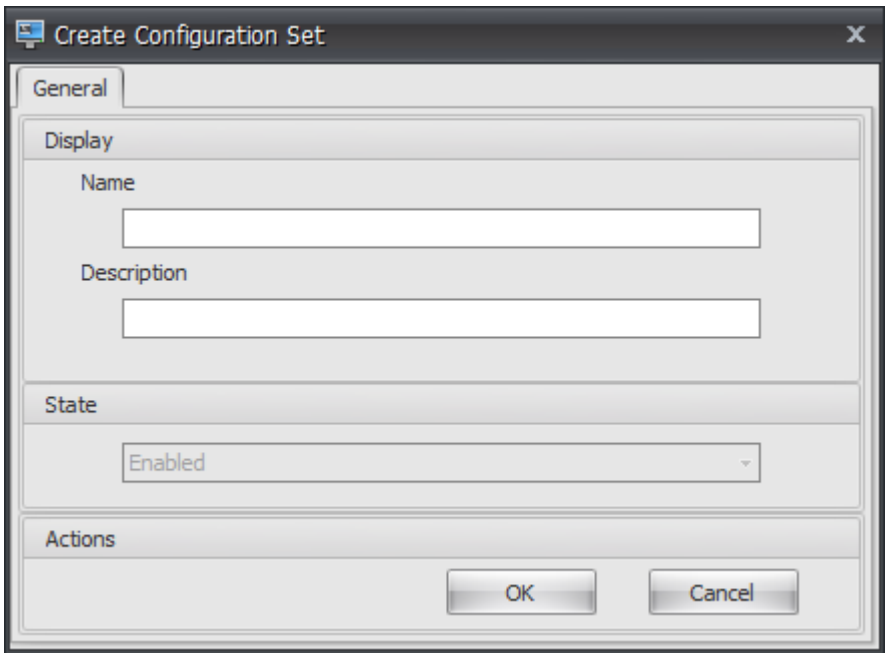


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

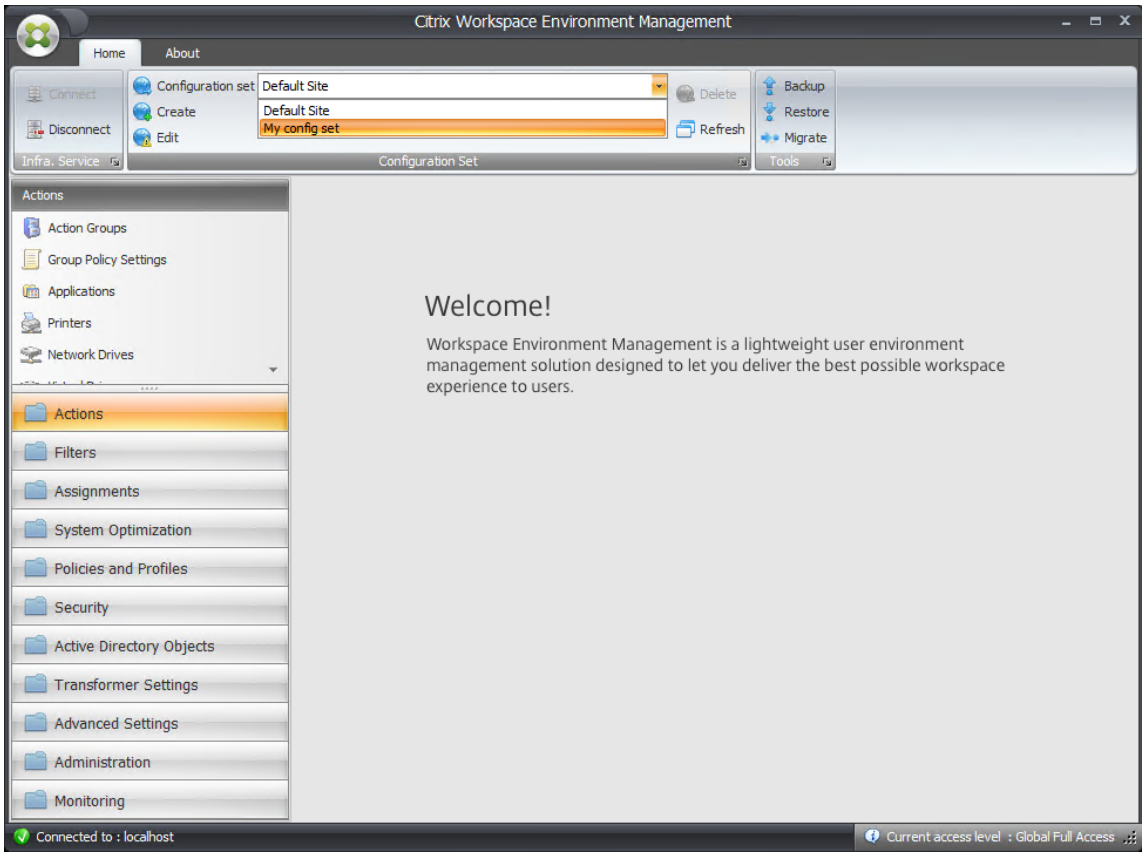


4. In the Create Configuration Set window, type a name and description for your configuration set and then click **OK**.



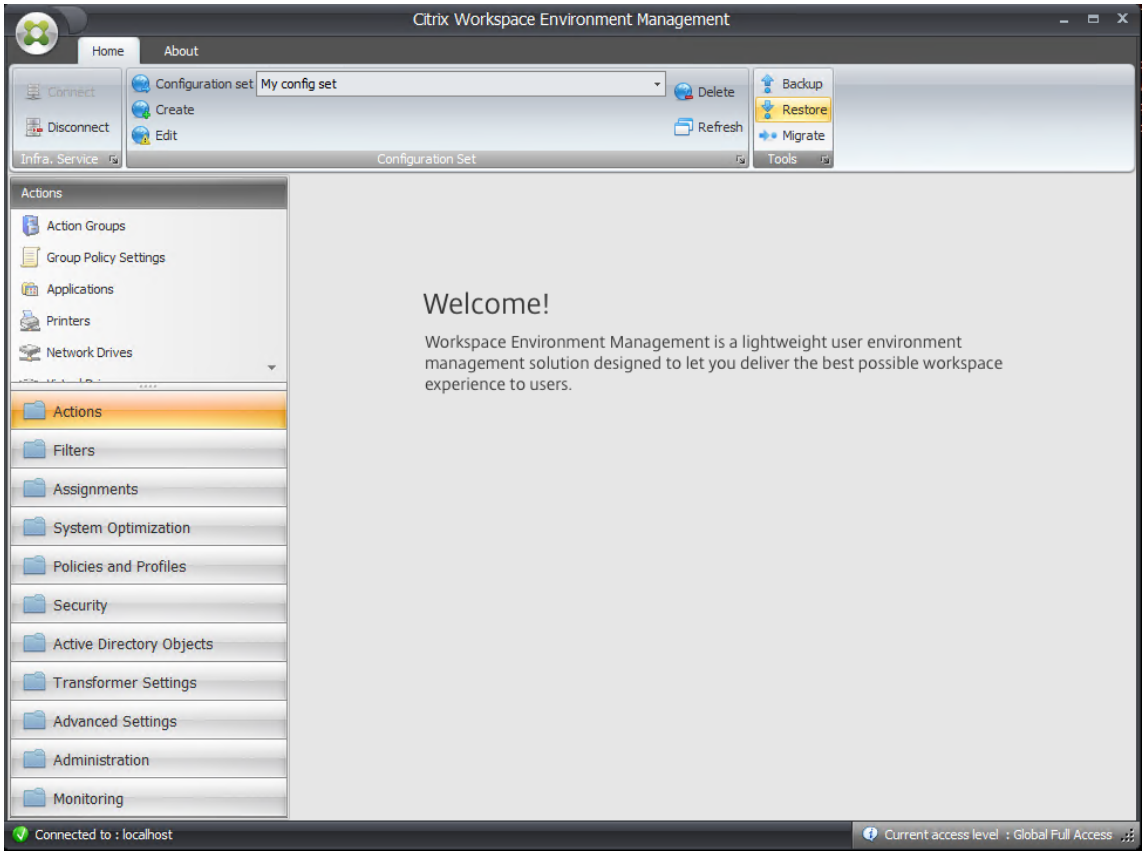
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



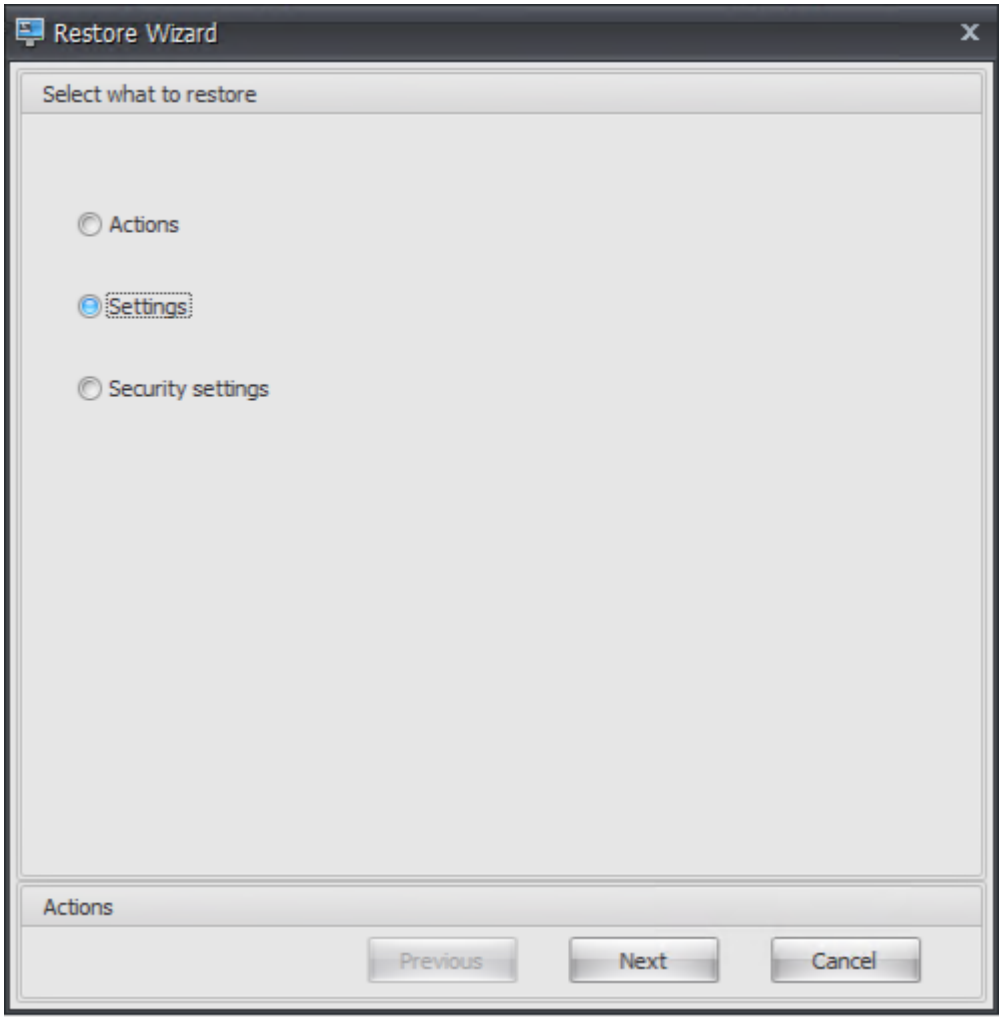
6. On the ribbon, under **Backup**, click **Restore**. The Restore wizard appears.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



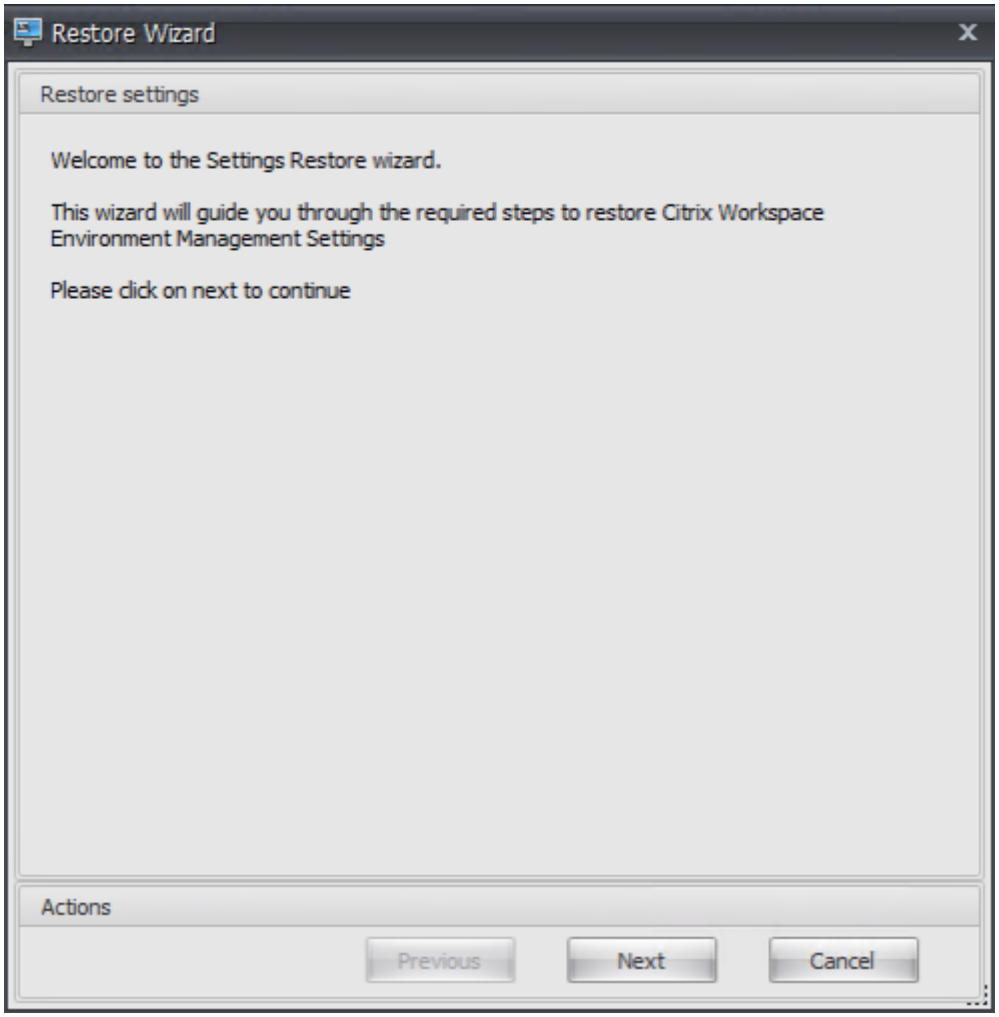
7. On the Select what to restore page, select **Settings** and then click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



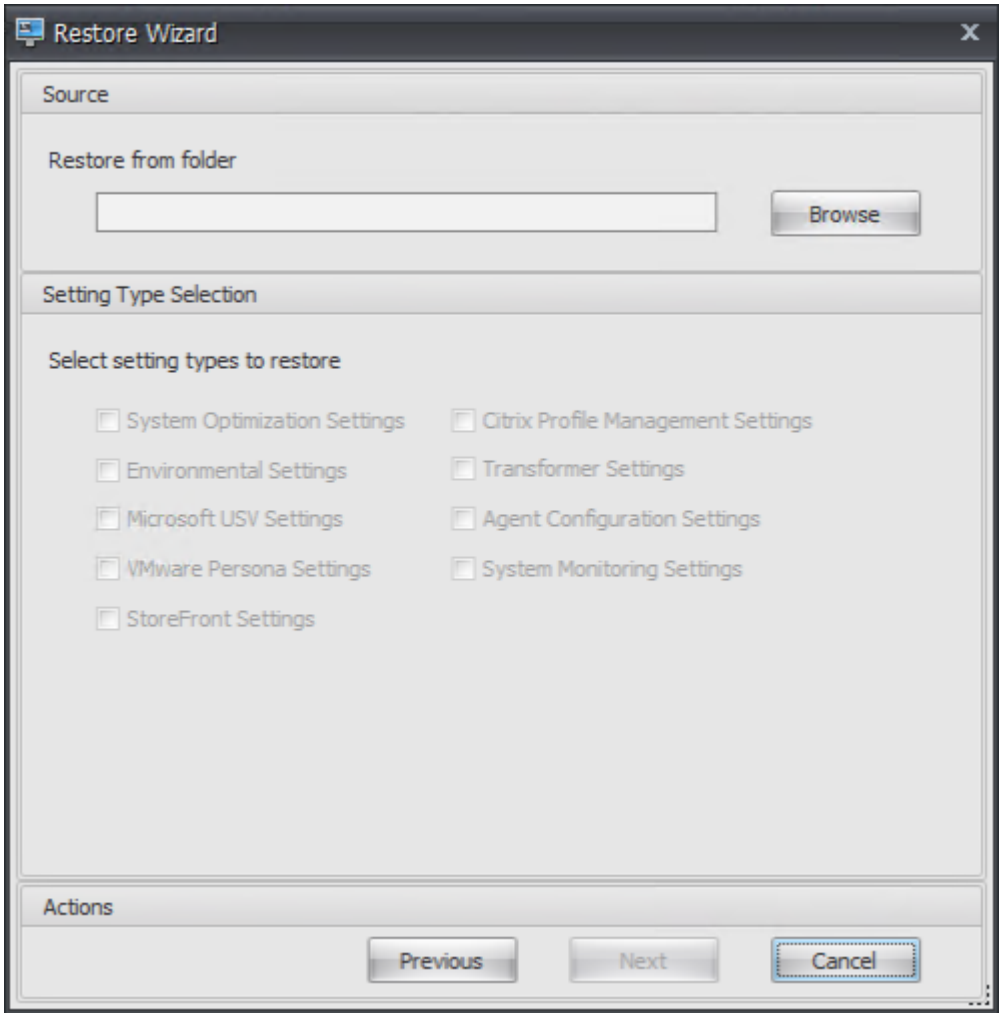
8. On the Restore settings page, click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



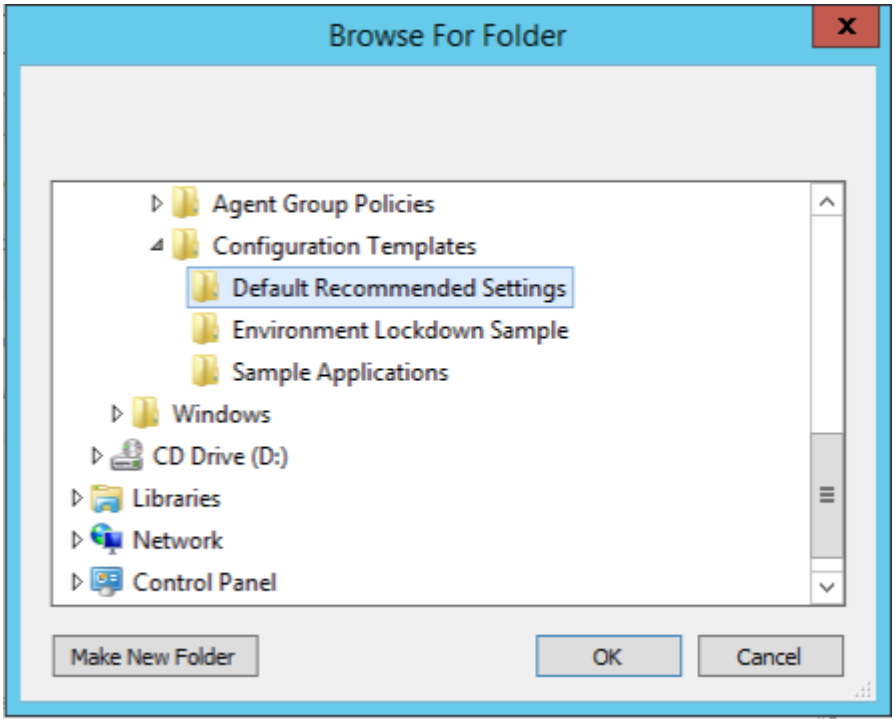
9. On the Source page, click **Browse**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



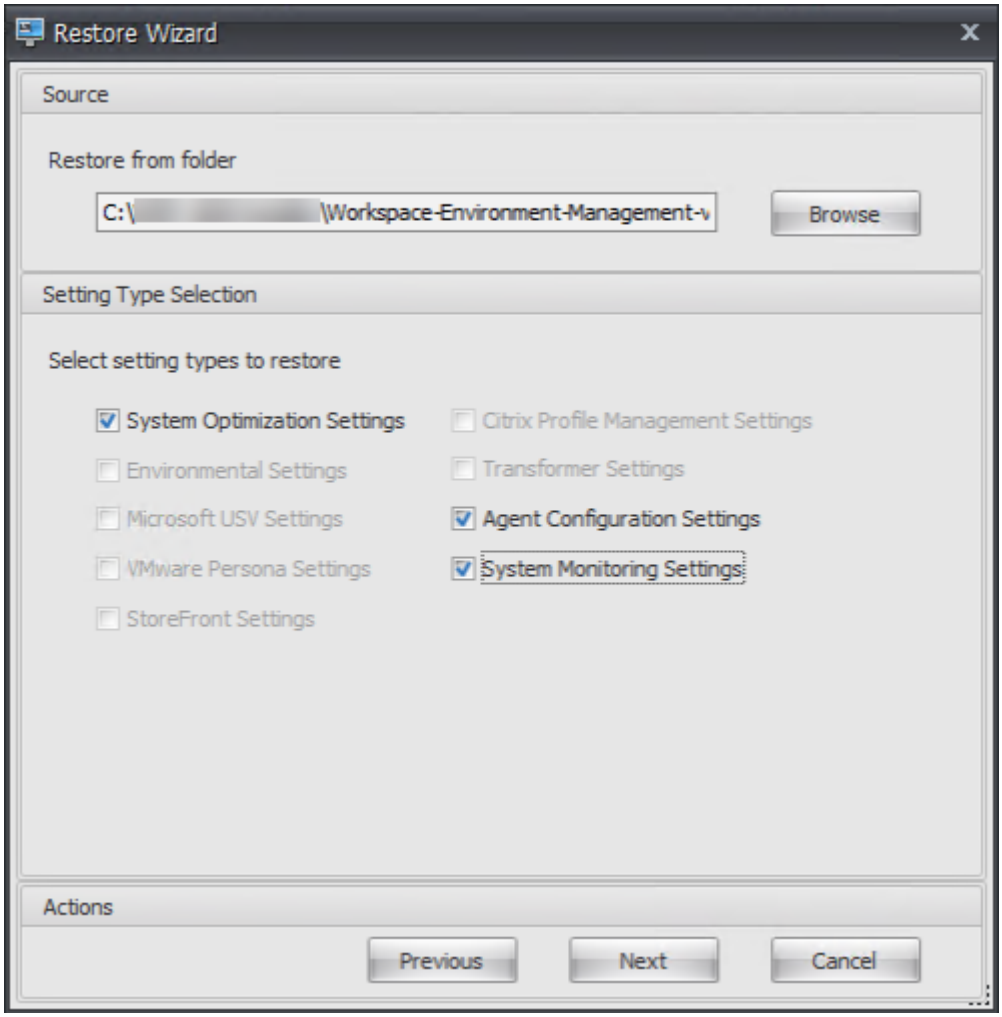
10. In the Browse For Folder window, browse to the **Default Recommended Settings** folder (provided with Workspace Environment Management) and then click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



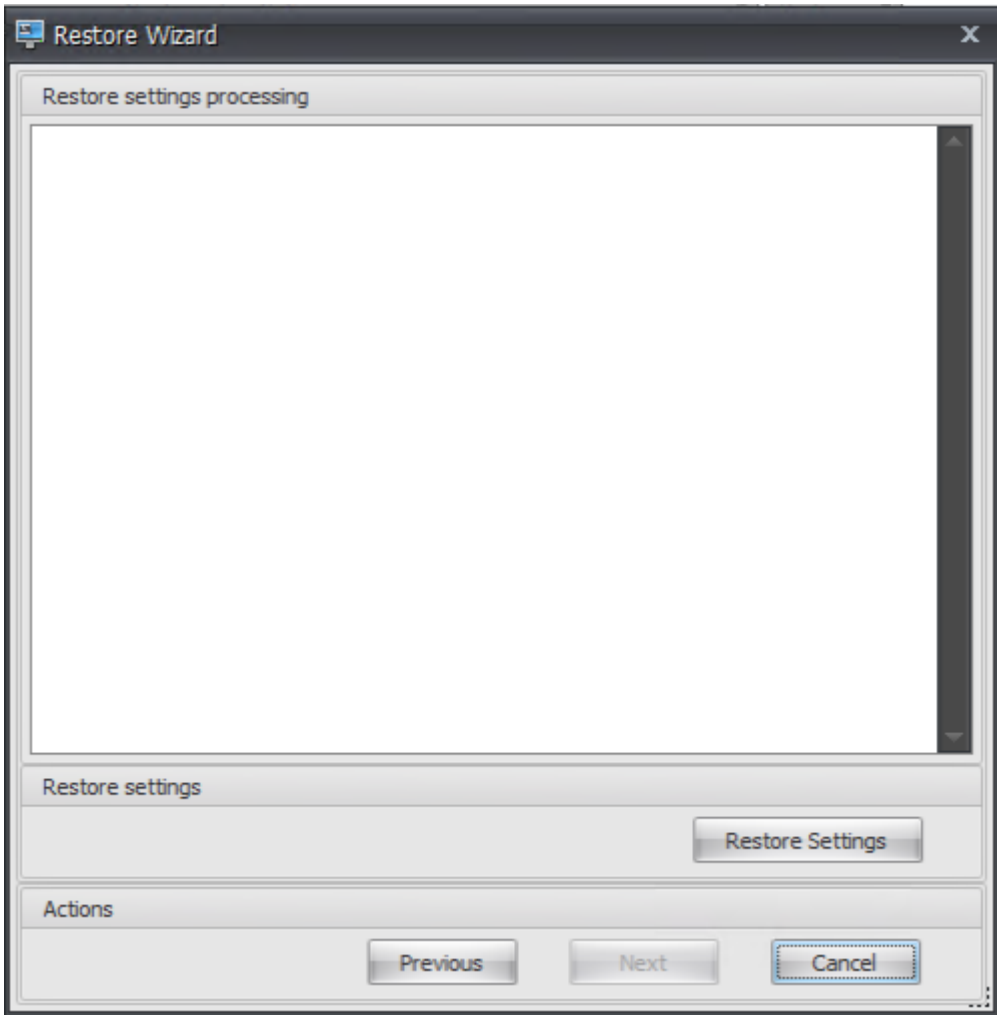
11. On the Source page, select **System Optimization Settings**, **Agent Configuration Settings**, and **System Monitoring Settings**, and then click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

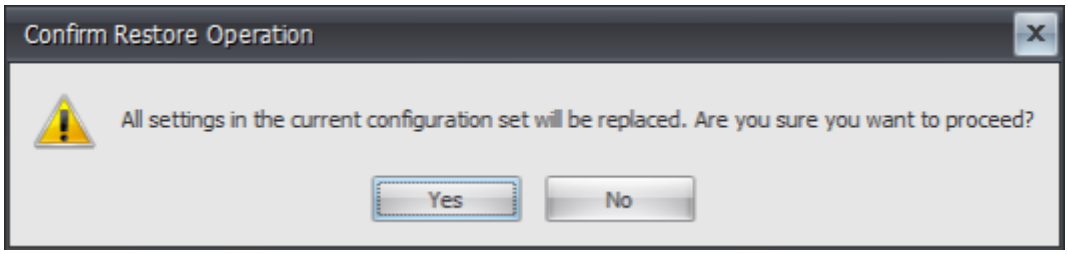


12. On the Restore settings processing page, under Restore settings, click **Restore Settings**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

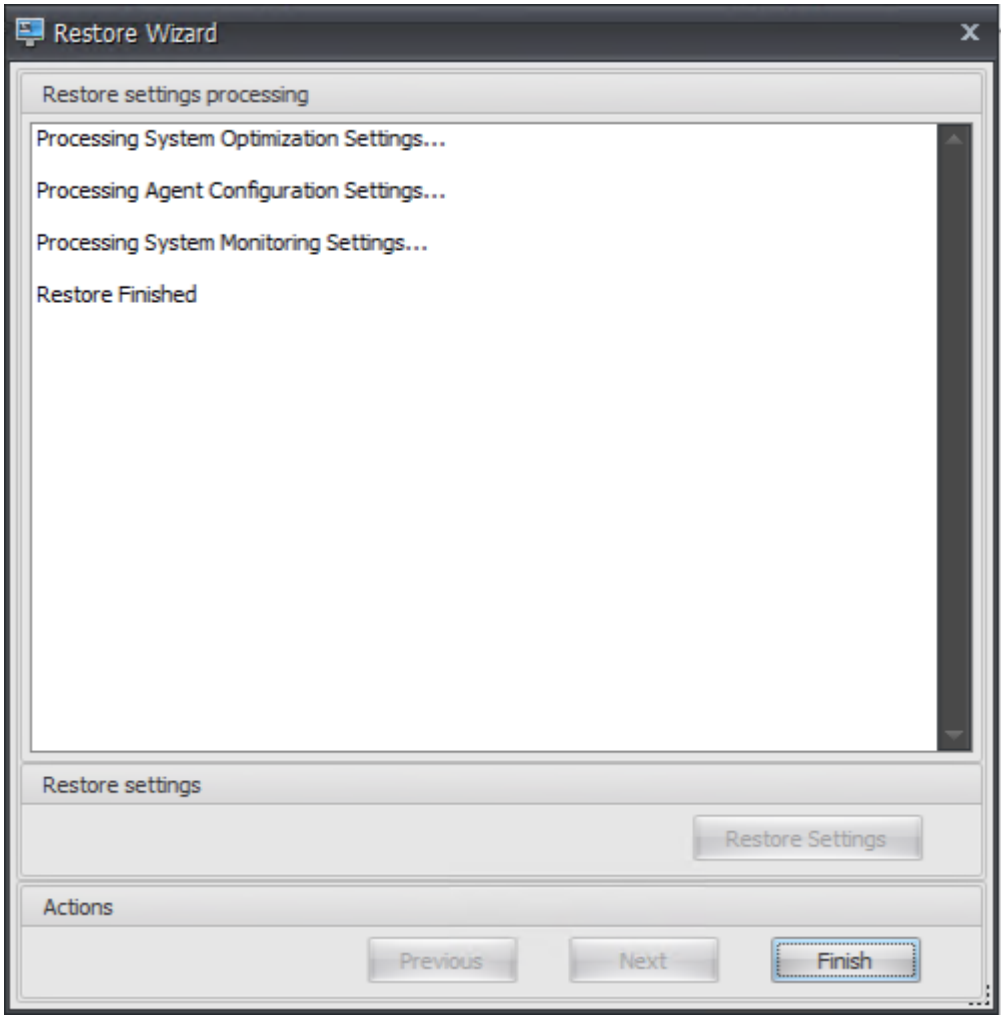


13. Click **Yes**.



14. Click **Finish**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Step 6: Add the group policy template (optional)

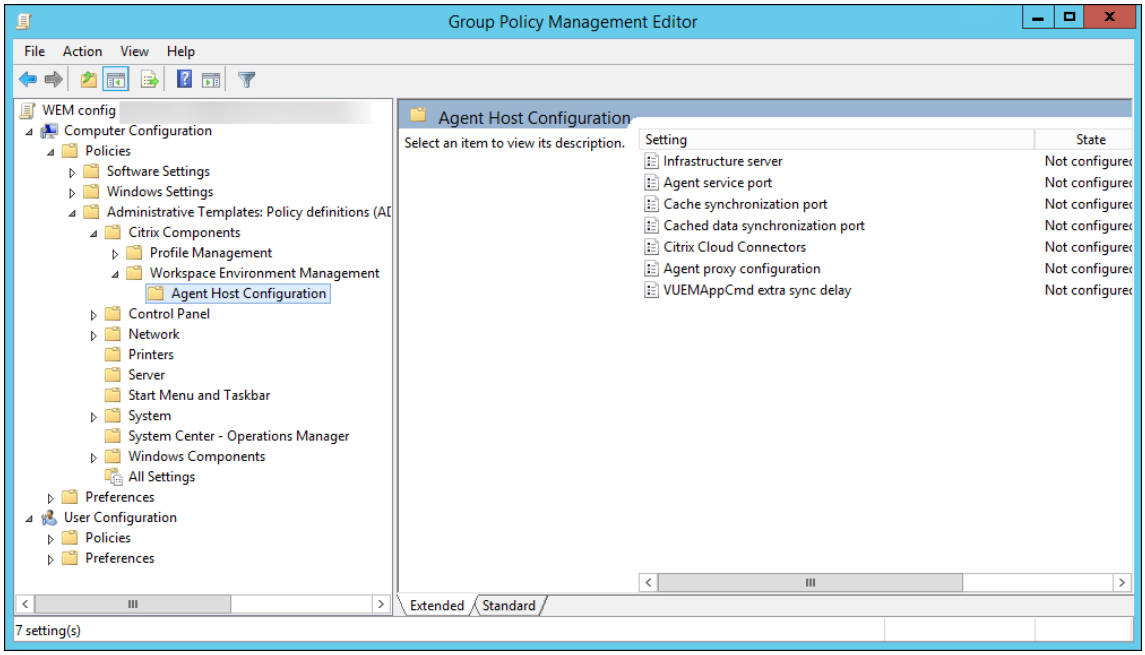
Optionally, you can choose to configure the group policies. The **Agent Group Policies** administrative template, provided in the WEM agent package, adds the Agent Host Configuration policy.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

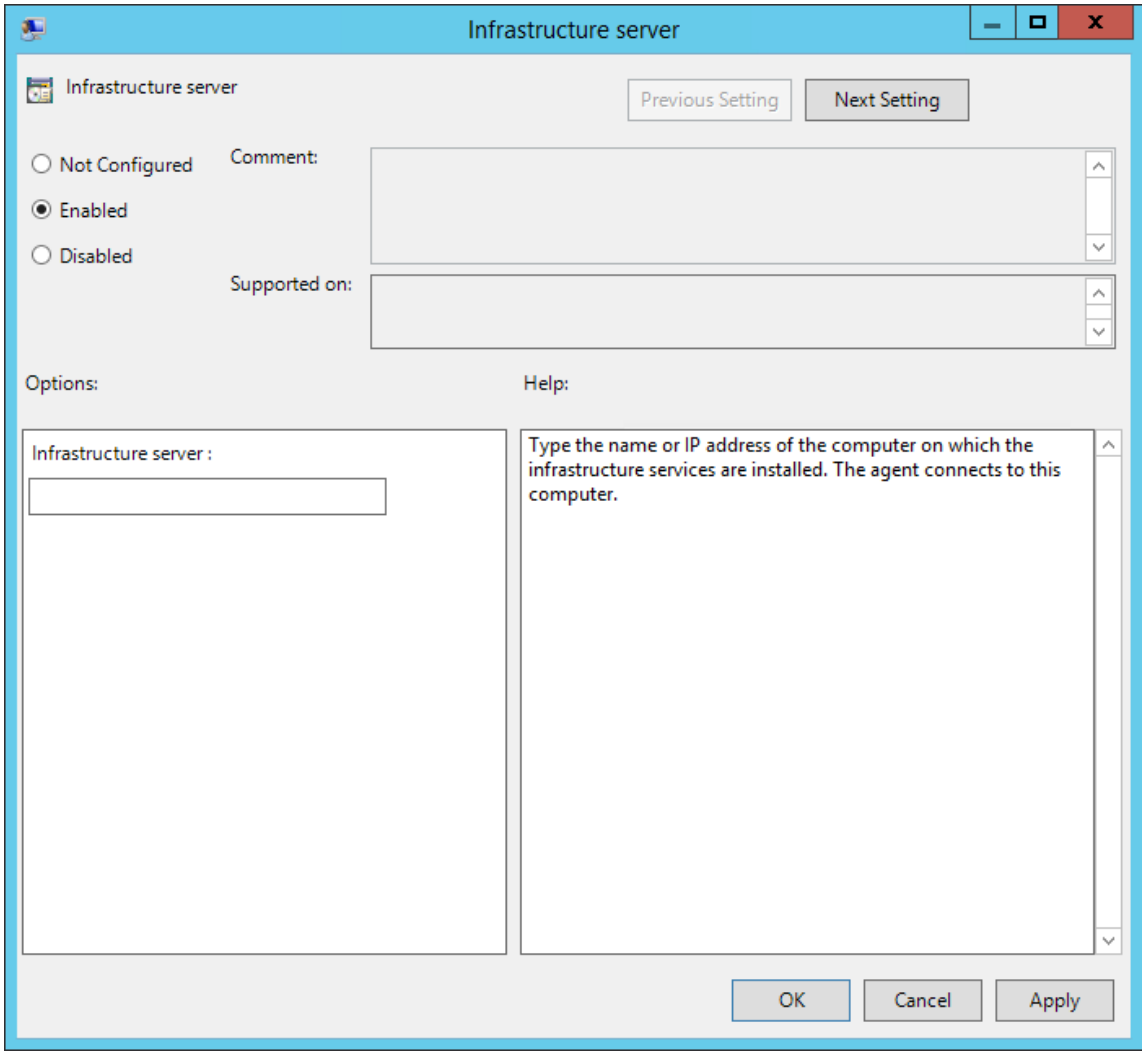
a) Go to the **Agent Group Policies > ADMX > en-US** folder.
b) Copy the two files (*Citrix Workspace Environment Management Agent Host Configuration.adml* and *CitrixBase.adml*).
c) Go to the <C:\Windows>\PolicyDefinitions\en-US folder and then paste the files.

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



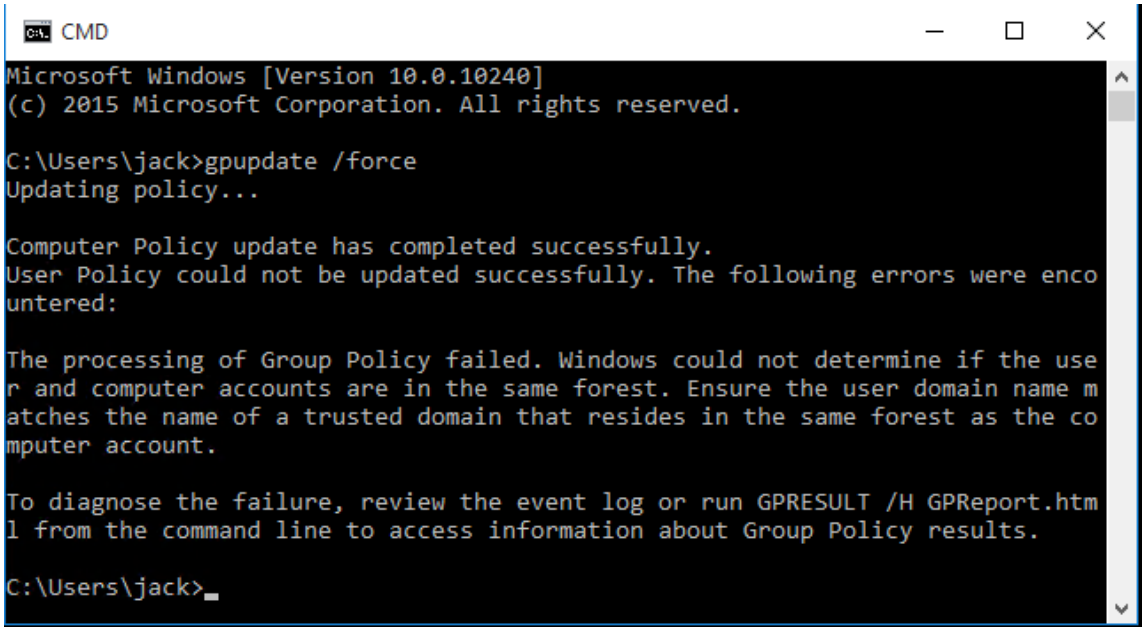
5. In the Infrastructure server window, select **Enabled**, and under Options, type the IP address of the computer on which the infrastructure services are installed, and then click **Apply** and **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

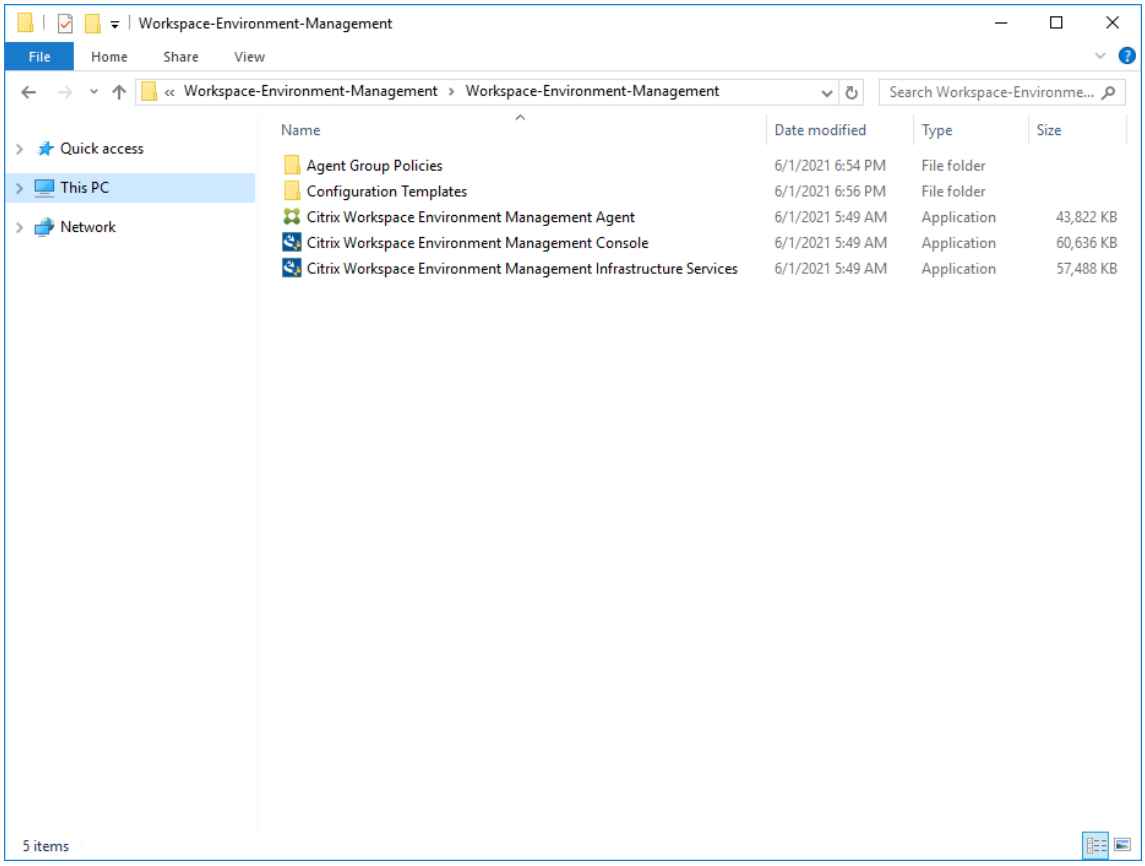


Step 7: Install the agent

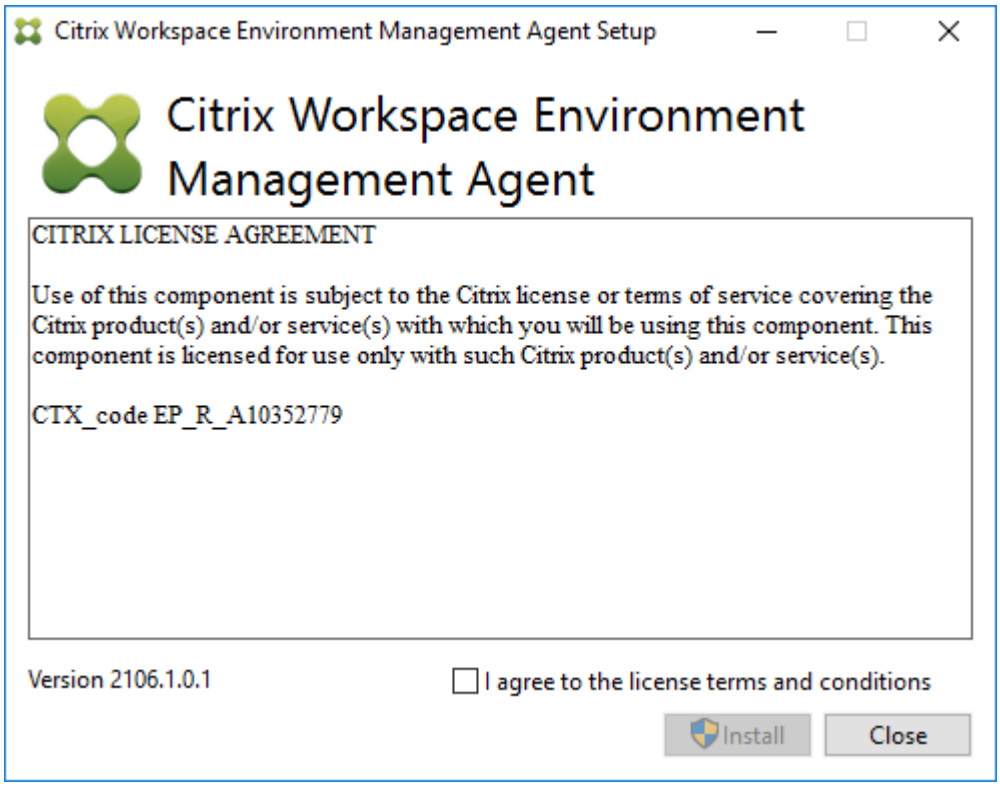
> **Important:**
>
> Do not install the WEM agent on the infrastructure server.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

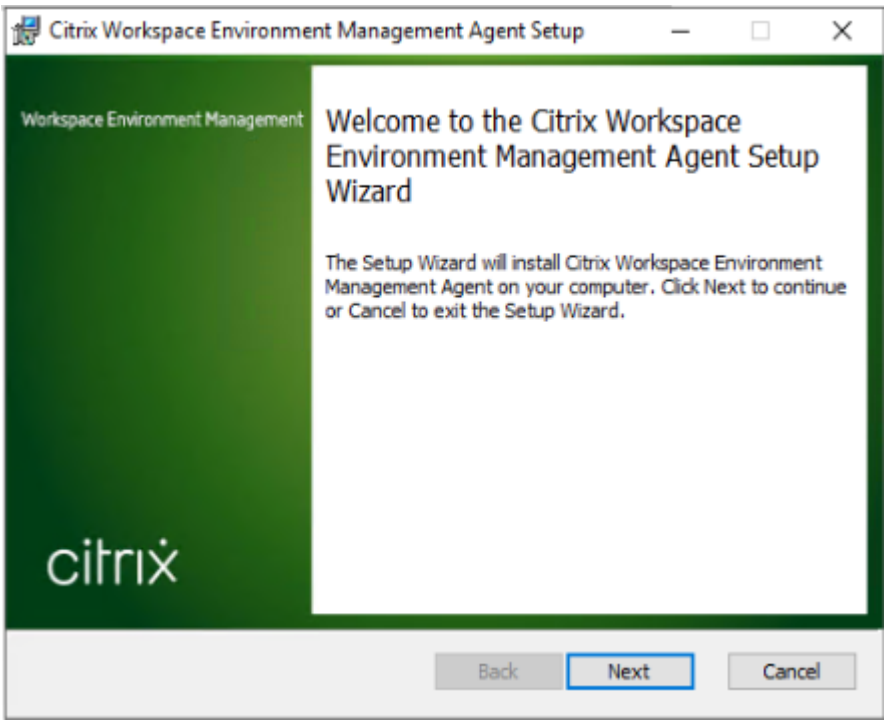


2. Select **I agree to the license terms and conditions** and then click **Install**.

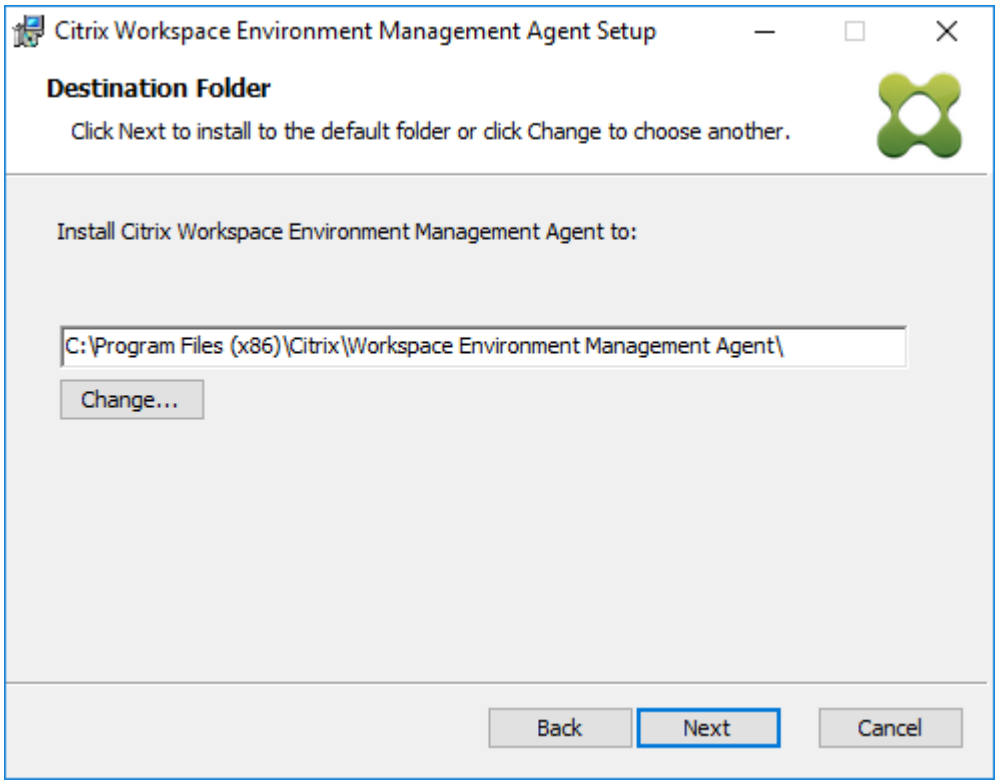


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



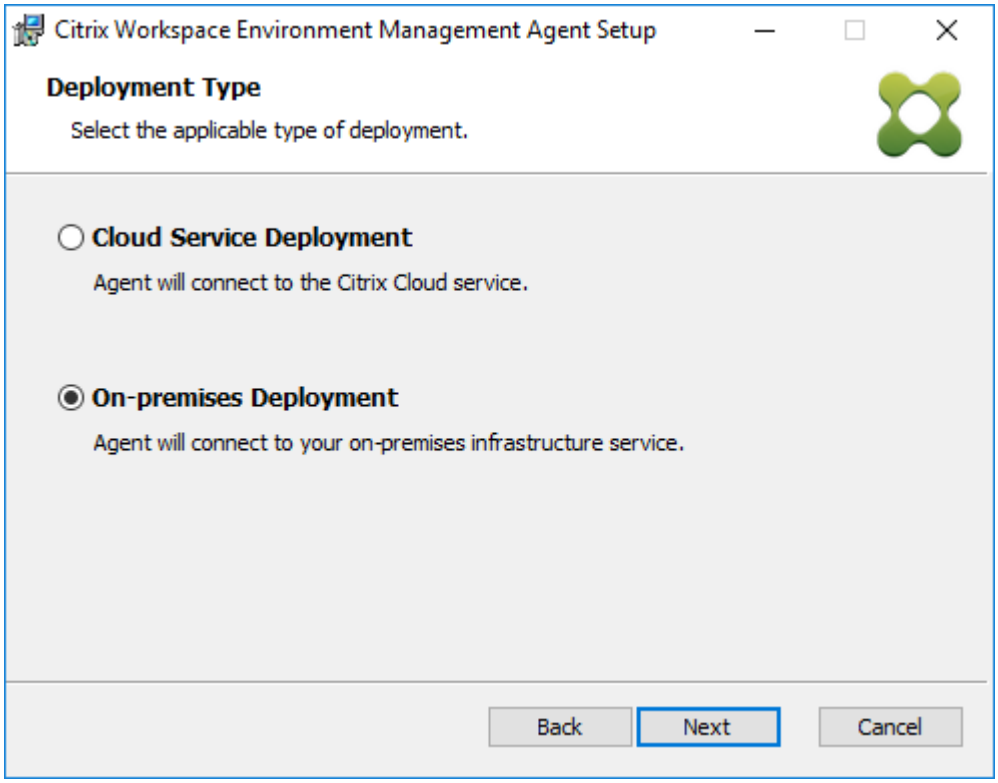
4. On the Destination Folder page, click **Next**.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

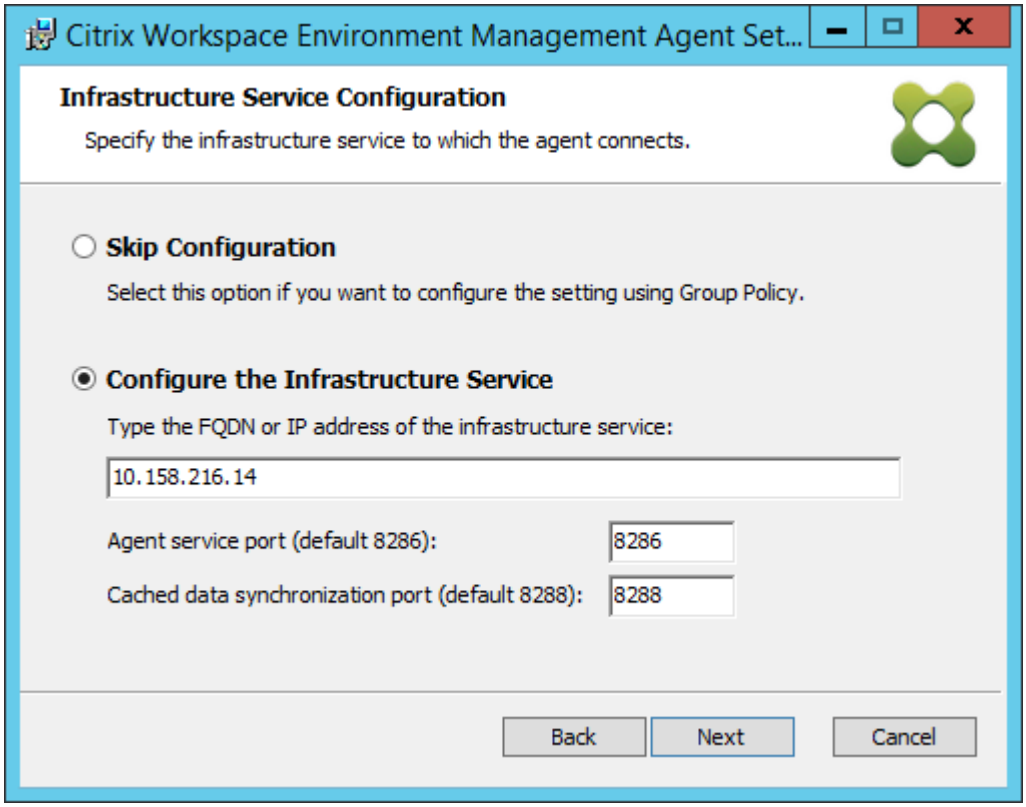
In this case, select **On-premises Deployment**.



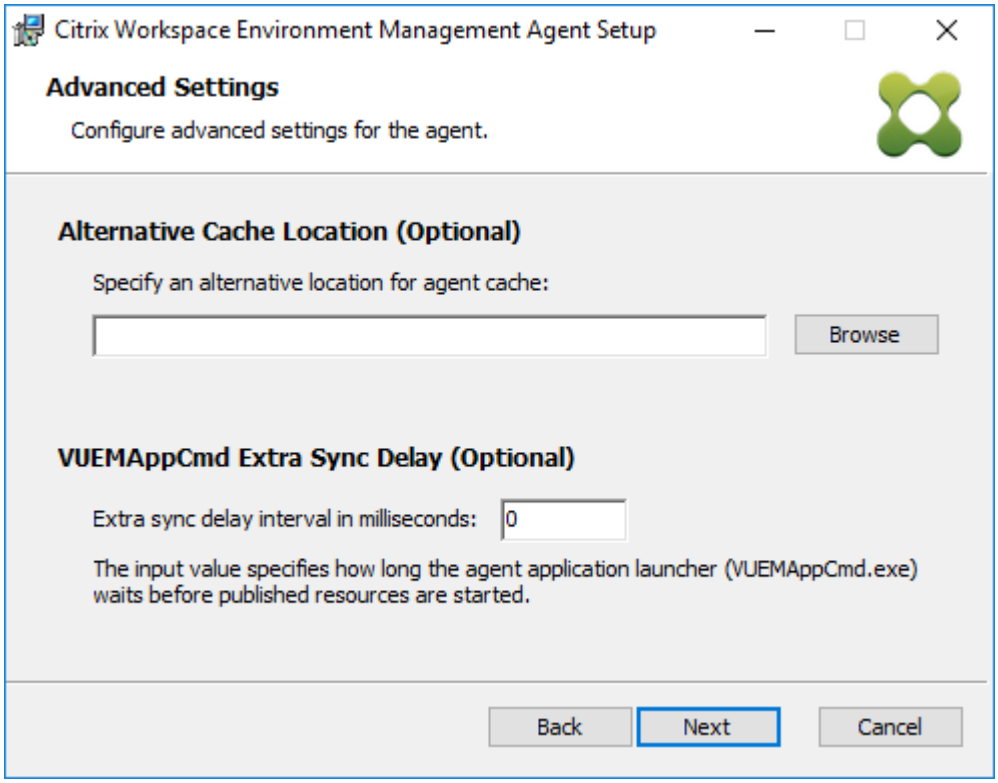
6. On the Infrastructure Service Configuration page, select **Configure the Infrastructure Service**, type the FQDN or IP address of the infrastructure service, and then click **Next**.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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



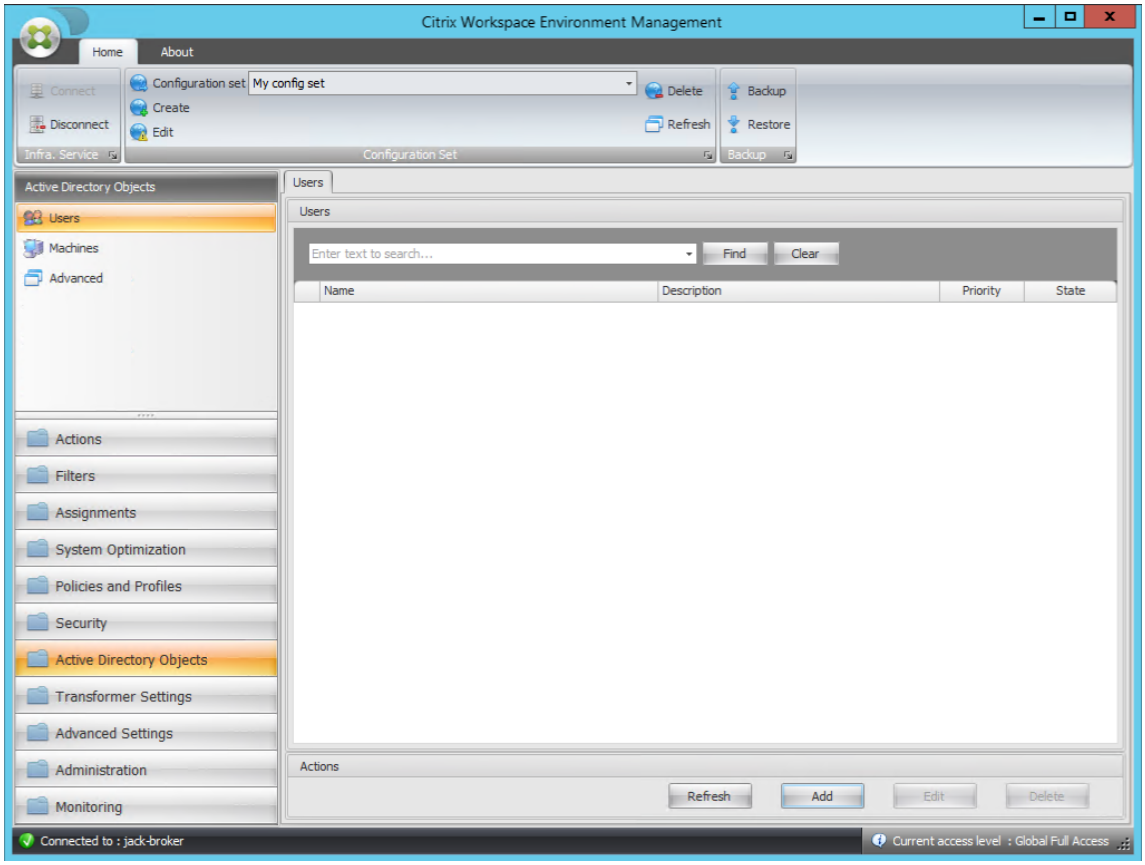
8. On the Ready to install page, click **Install**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

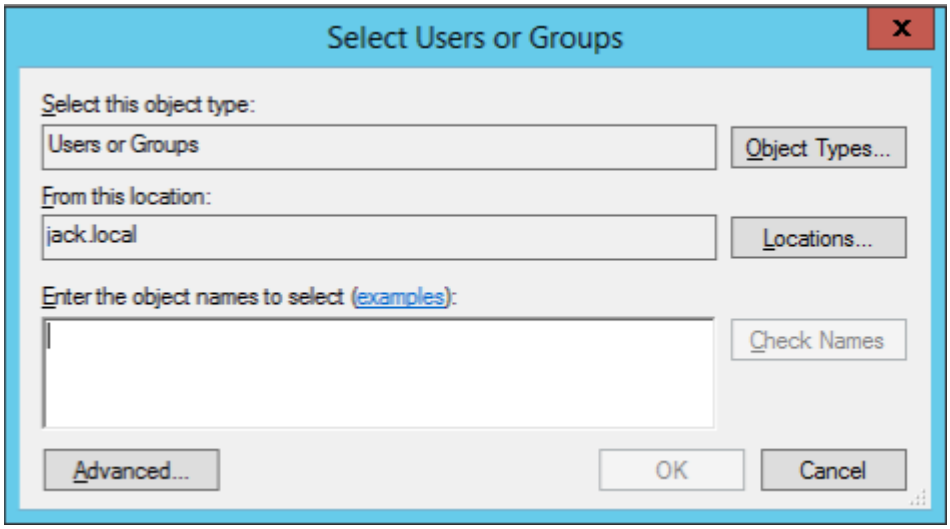
Step 8: Add the agent to the configuration set you created

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

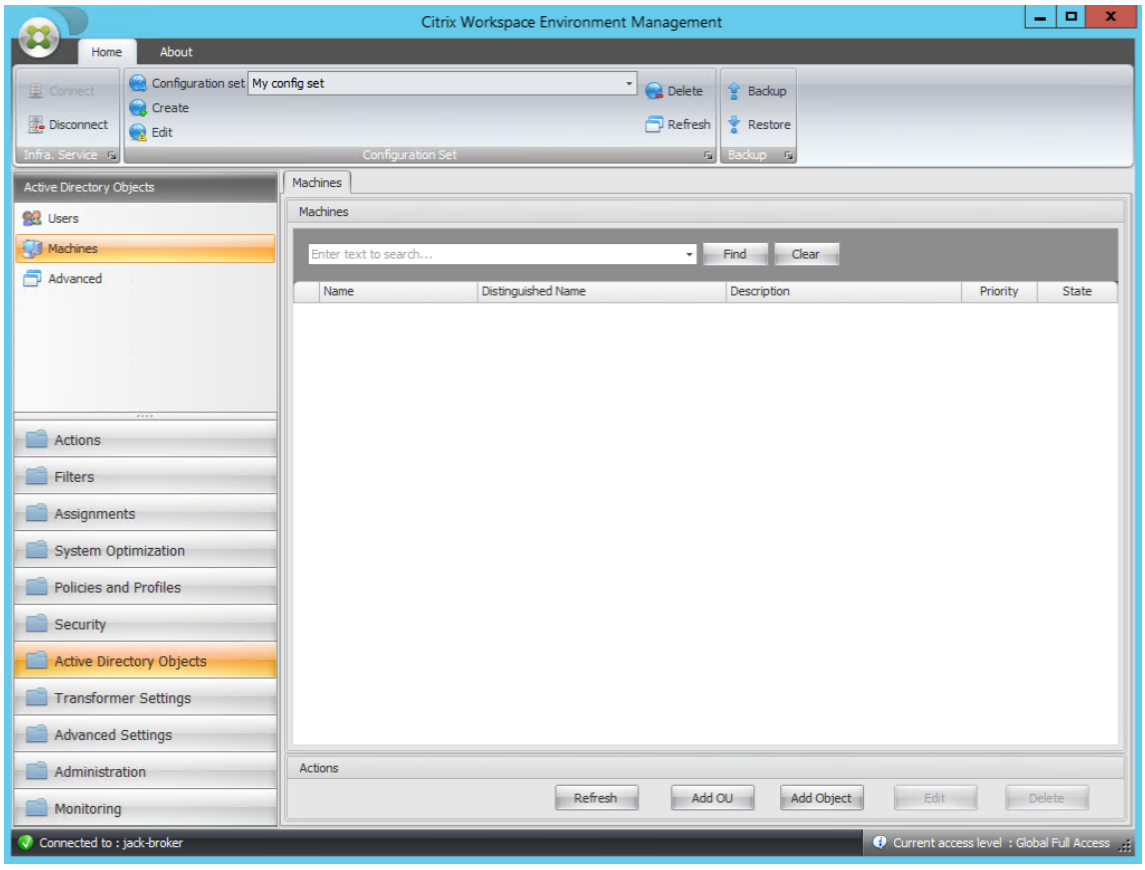


2. In the Select Users or Groups window, type the name, click **Check Names**, and then click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

System requirements

April 24, 2023

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

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

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

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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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 2022 Standard and Datacenter Editions
- Windows Server 2019 Standard and Datacenter Editions
- Windows Server 2016 Standard and Datacenter Editions
- Windows Server 2012 R2 Standard and Datacenter Editions

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Administration console

Supported operating systems:

- Windows 11, 32-bit and 64-bit
- Windows 10 version 1607 and newer, 32-bit and 64-bit
- Windows Server 2022 Standard and Datacenter Editions
- Windows Server 2019 Standard and Datacenter Editions
- Windows Server 2016 Standard and Datacenter Editions
- Windows Server 2012 R2 Standard and Datacenter Editions

Agent

Supported operating systems:

- Windows 11, 32-bit and 64-bit
- Windows 10 version 1607 and later, 32-bit and 64-bit
- Windows 8.1 Professional and Enterprise Editions, 32-bit and 64-bit
- Windows 7 SP1 Professional, Enterprise, and Ultimate Editions, 32-bit and 64-bit
- Windows Server 2022 Standard and Datacenter Editions*
- Windows Server 2019 Standard and Datacenter Editions*
- Windows Server 2016 Standard and Datacenter Editions*
- Windows Server 2012 R2 Standard and Datacenter Editions*
- Windows Server 2012 Standard and Datacenter Editions*
- Windows Server 2008 R2 SP1 Standard, Enterprise, and Datacenter Editions*

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

In WEM 4.4, Windows XP was supported.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Hardware prerequisites

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

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

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

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

Service dependencies

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

Antivirus exclusions

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

In the infrastructure services installation folder

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

In the agent installation folder

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

Install and configure

December 6, 2022

Install and configure the following components:

- Infrastructure services
- Administration console
- Agent

Infrastructure services

December 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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\\""
```

You can choose a silent installation or upgrade of the infrastructure services. The syntax is as follows:

- .\setup.exe /s /v"'/qn CLOUD=0'"
  - `setup.exe`. Lets you replace it with the file name of the installer.
  - `/s`. Indicates silent mode.
  - `/v`. Passes arguments to msiexec.
  - `/qn`. Indicates that no user interface appears during the installation.
  - `CLOUD=0`. Indicates on-premise deployments.
- For example:
  - .\Citrix Workspace Environment Management Infrastructure Services.exe /s /v"'/qn CLOUD=0'"

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **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), use the following command:

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

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

- If you use a gMSA solution, use the following command:

  - **setspn -C -S Norskale/BrokerService [*gMSA*]$**

  where [*gMSA*] is the name of the gMSA account.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

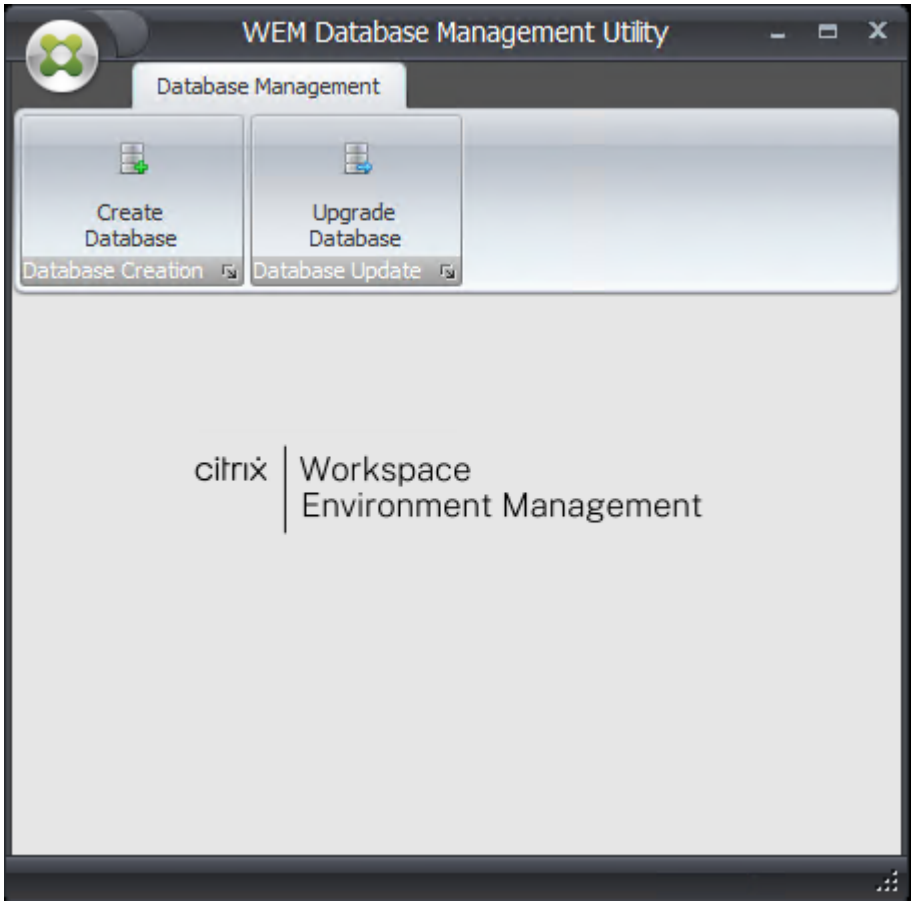
Create a Workspace Environment Management database

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

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

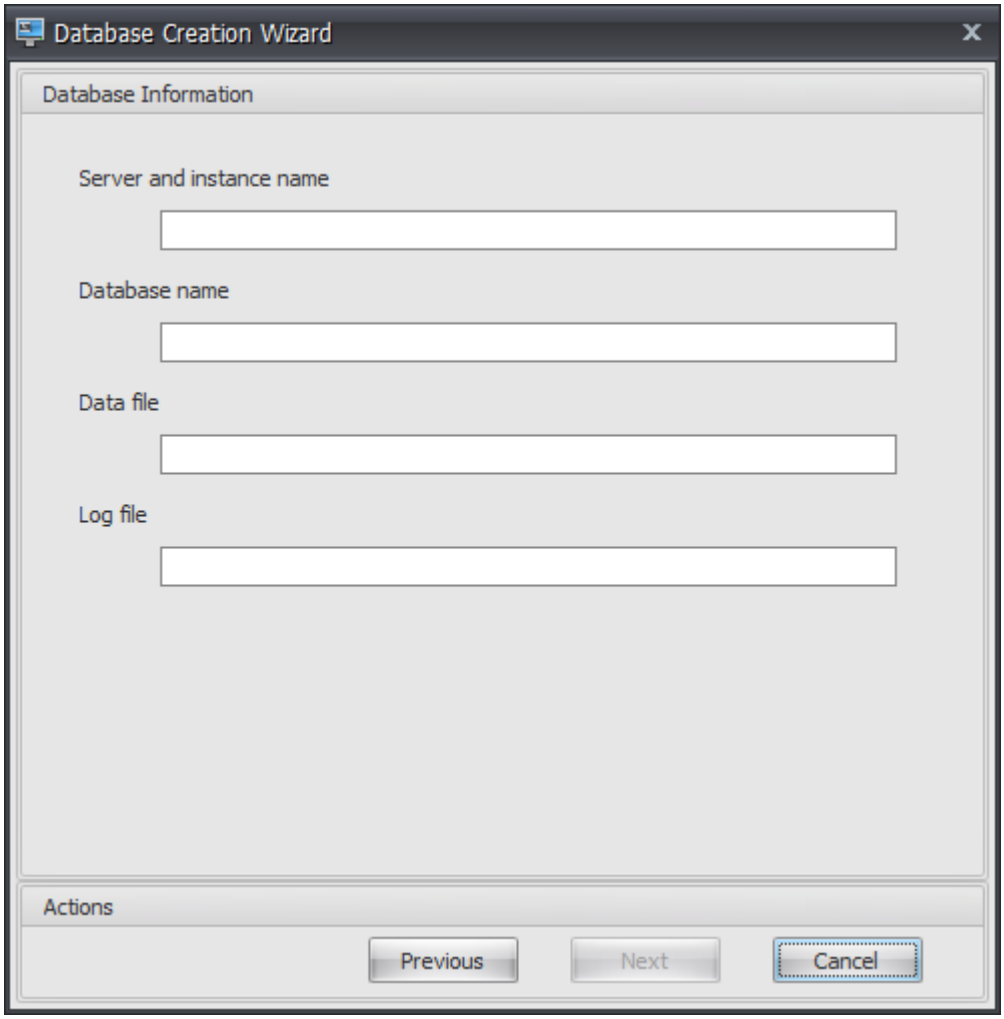
1. If the Database Management Utility is not already open, from the **Start** menu select **Citrix>Workspace Environment Management>WEM Database Management Utility**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

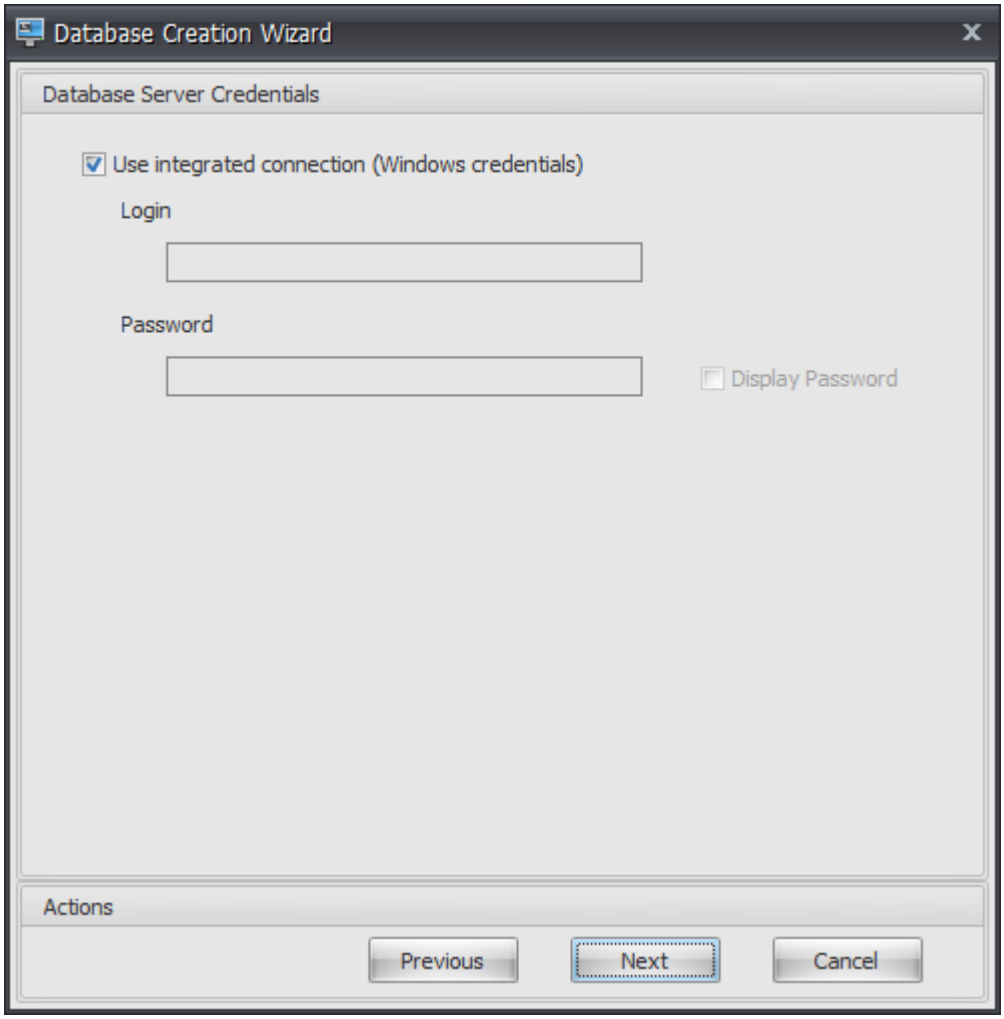
   - **Server and instance name**. Address of the SQL Server on which the database will be hosted. This address must be reachable exactly as typed from the infrastructure server. Type server and instance name as the machine name, fully qualified domain name, or IP address. Specify a full instance address 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

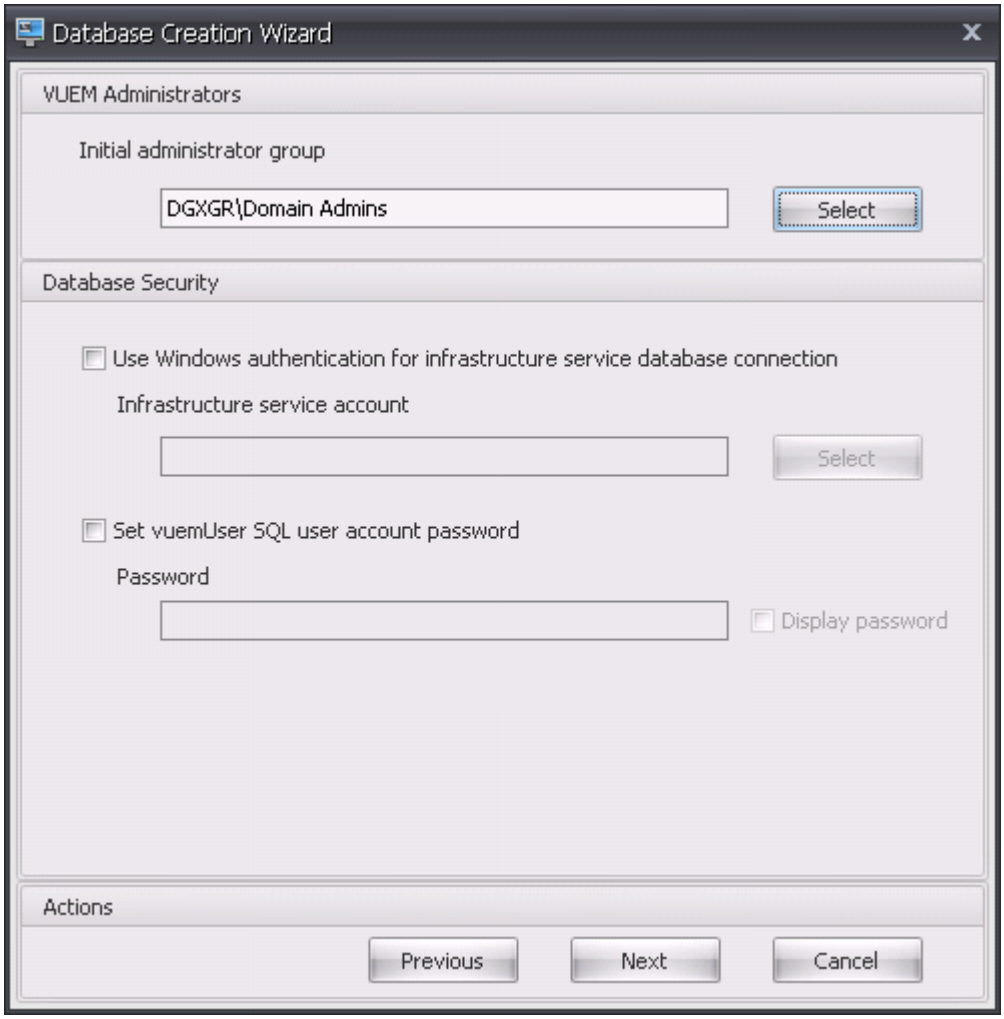
> **Note:**
>
> The database management utility cannot query your SQL Server for the default location of the data and log files. They default to the default values for a default installation of MS SQL Server. Make sure that the values in these two fields are correct for your MS SQL Server installation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



4. Provide Database Server Credentials which the wizard can use to create the database, then click **Next**. These credentials are independent from the credentials 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

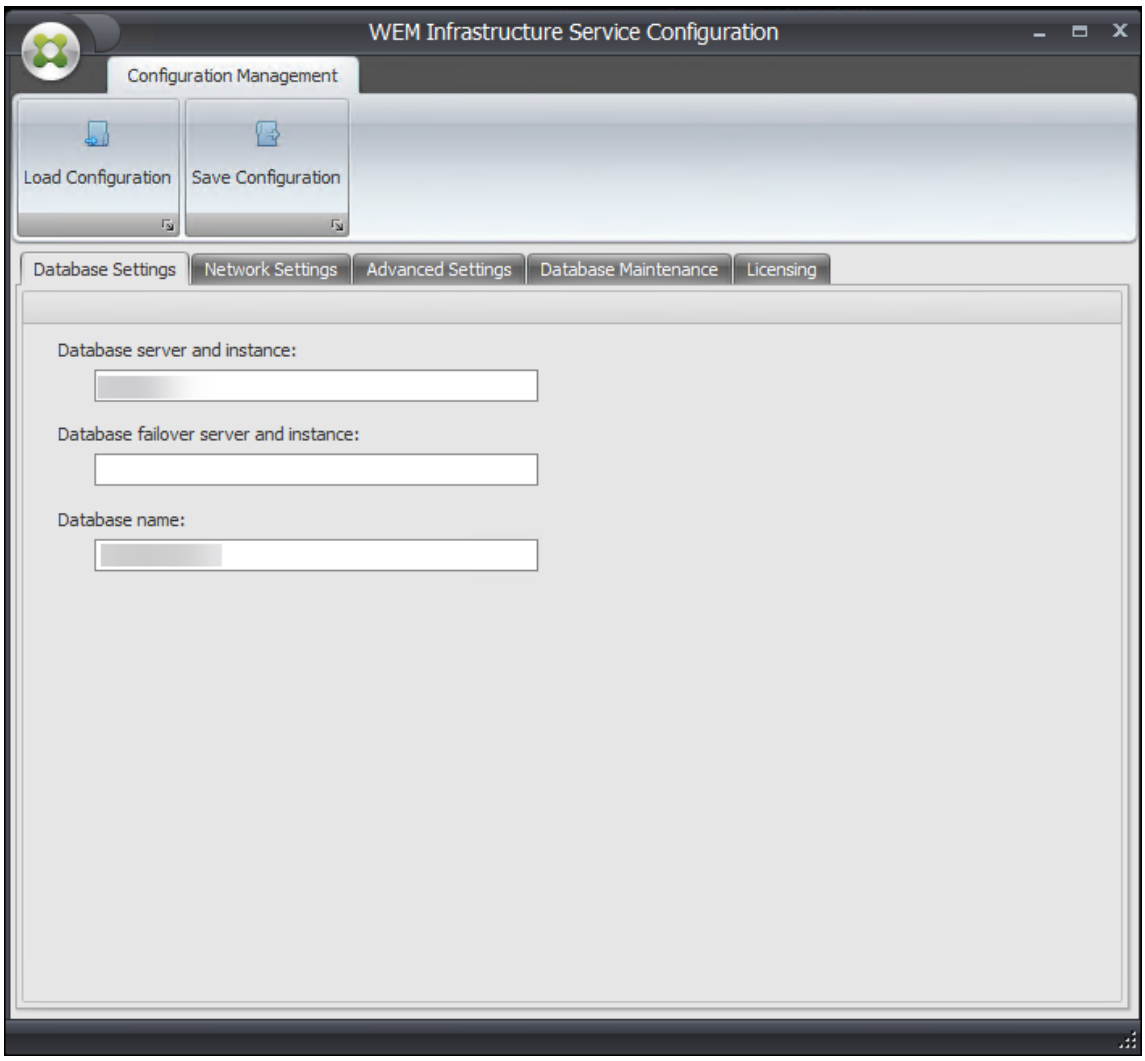
Before the infrastructure service runs, you must configure it using the **WEM Infrastructure Service Configuration** utility, as described here.

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.

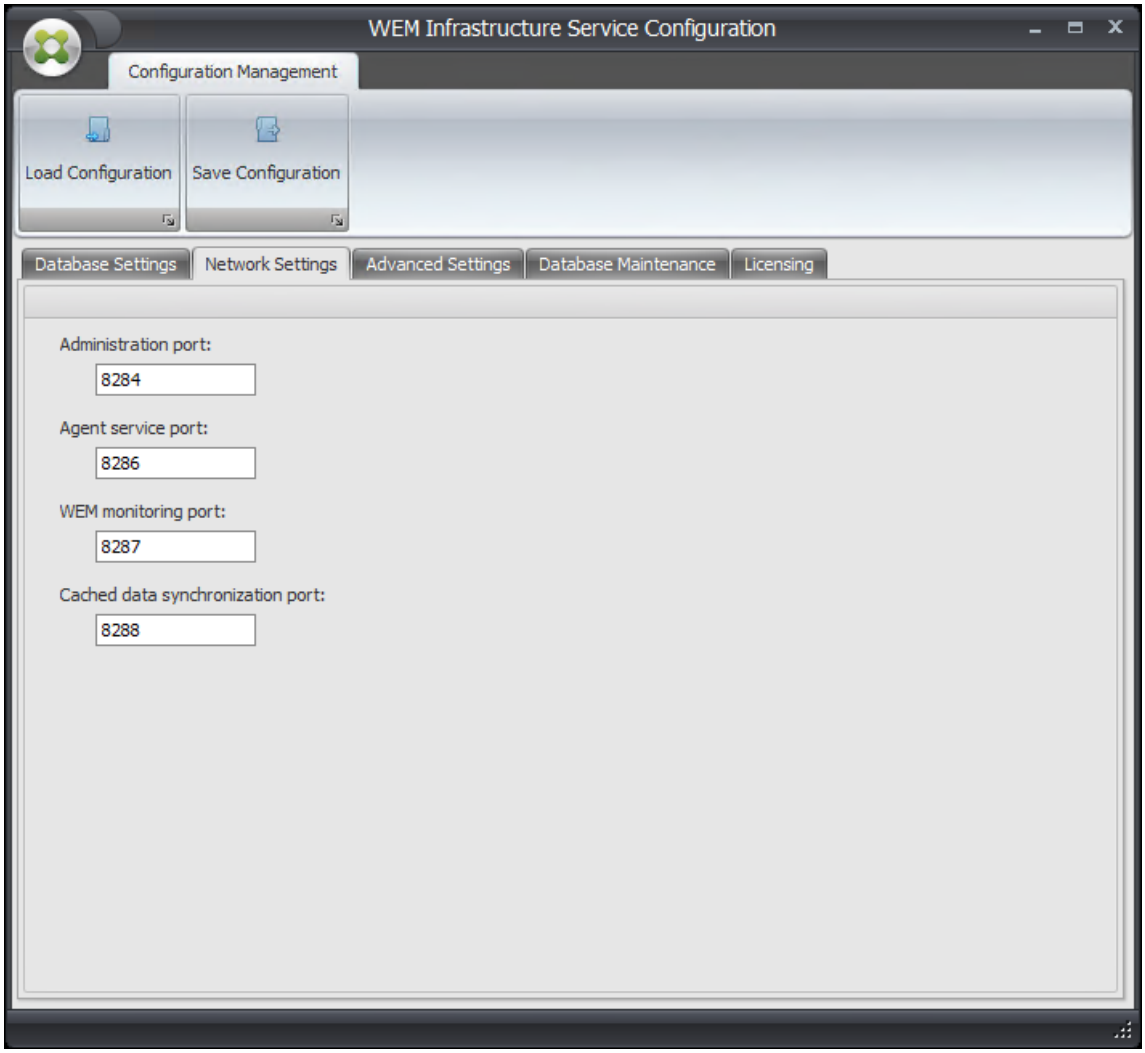
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

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

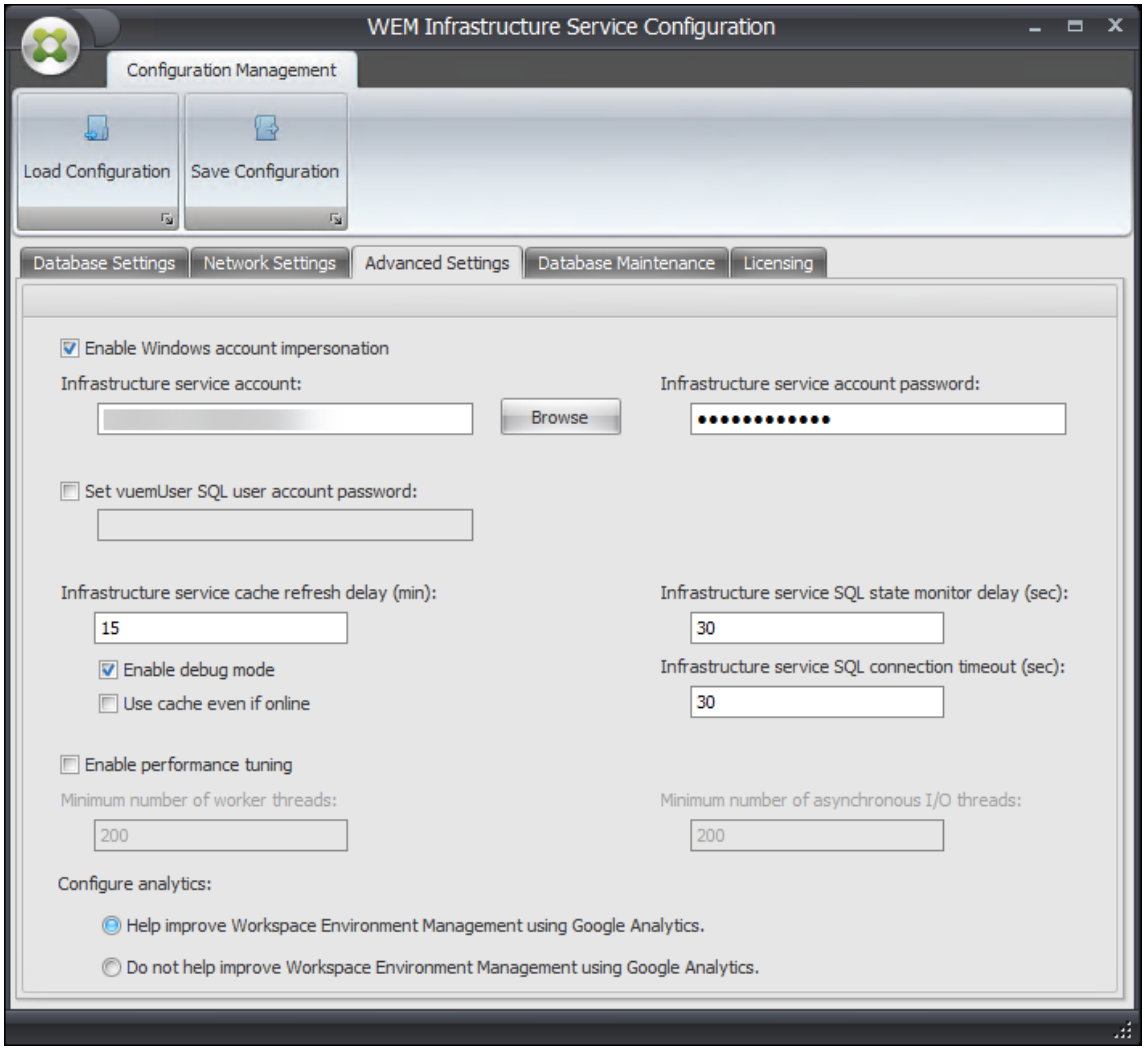
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

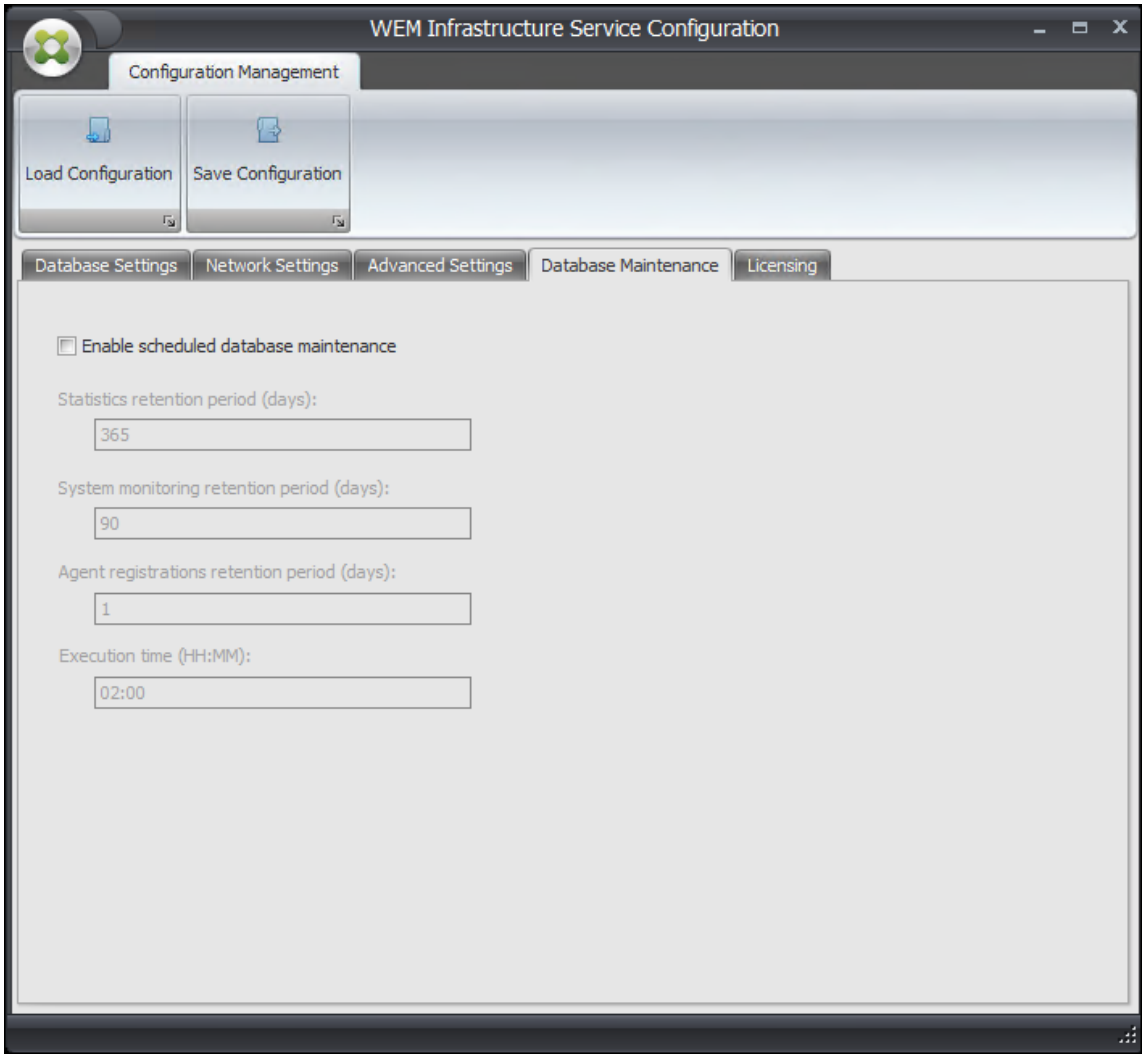


5. You can use the **Database Maintenance** tab to configure database maintenance.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

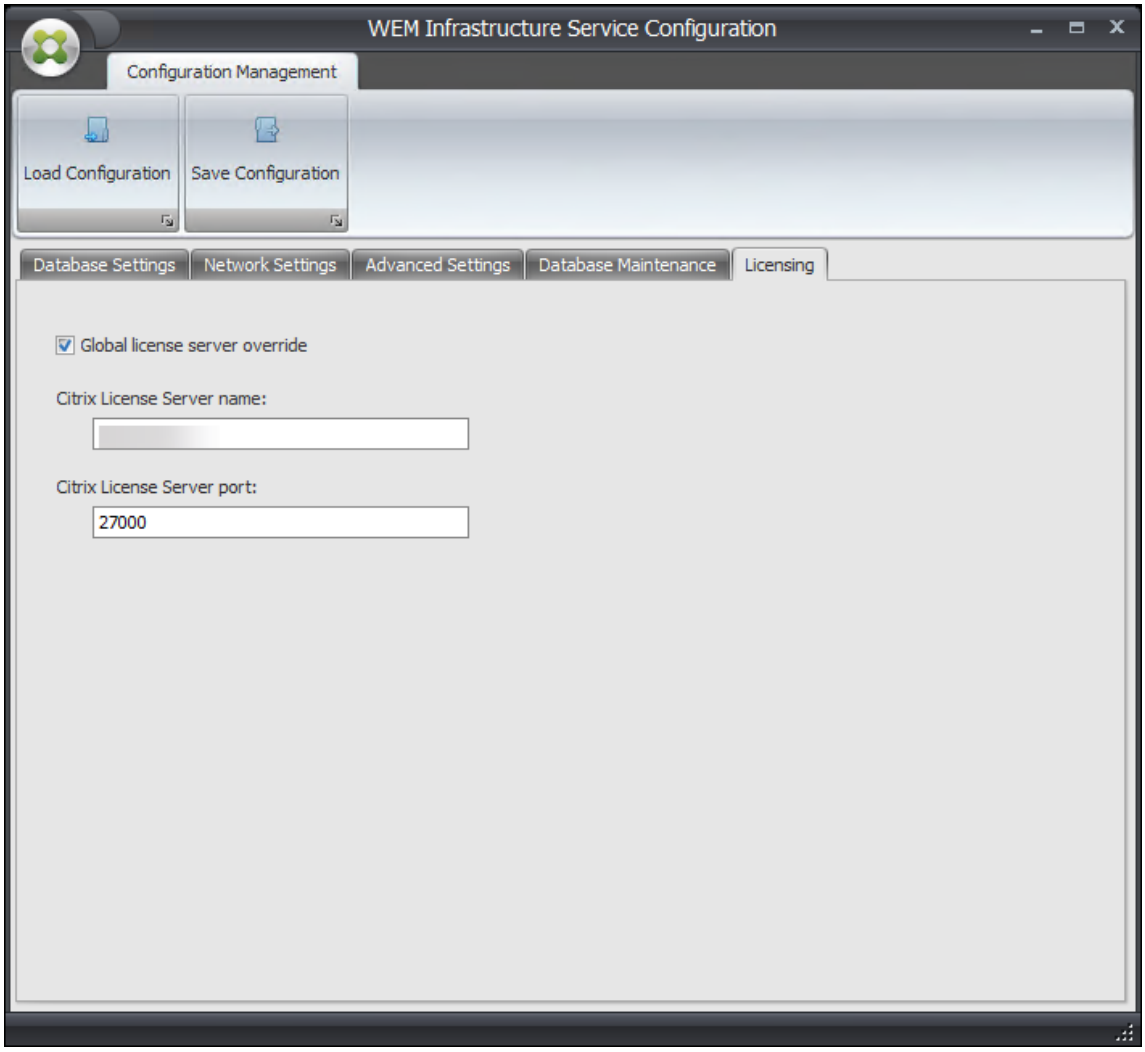
> **Tip**
>
> As a best practice, we recommend that you enable scheduled database maintenance to reduce the database size and achieve the best performance. If there is more than one infrastructure service in a single WEM deployment, enable it only for one infrastructure service.



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

    - **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

Administration console

December 6, 2022

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 Work-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> space app for Windows is installed on the administration console machine and on the agent host machine. For more information see System requirements.

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

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.exe "/v"
argument=\\"value\\""
```

You can choose a silent installation or upgrade of the administration console. The syntax is as follows:

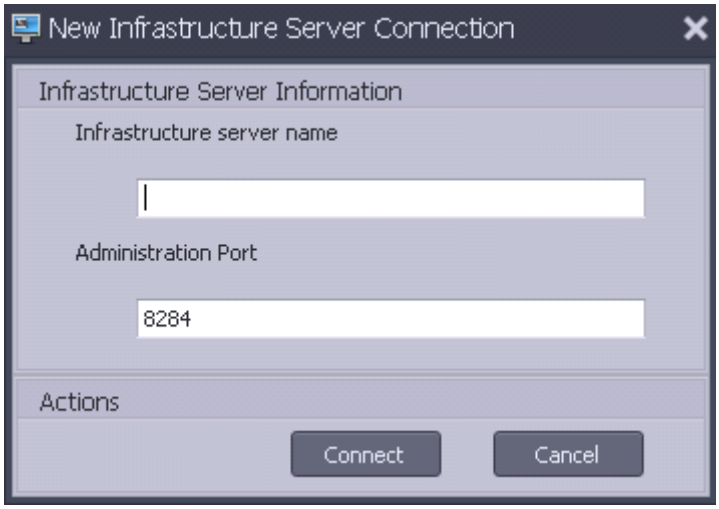
- .\setup.exe /s /v‘“/qn CLOUD=0‘”
  - `setup.exe`. Lets you replace it with the file name of the installer.
  - `/s`. Indicates silent mode.
  - `/v`. Passes arguments to msiexec.
  - `/qn`. Indicates that no user interface appears during the installation.
  - `CLOUD=0`. Indicates on-premise deployments.
- For example:
  - .\Citrix Workspace Environment Management Console.exe /s /v‘“/qn CLOUD=0‘”

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

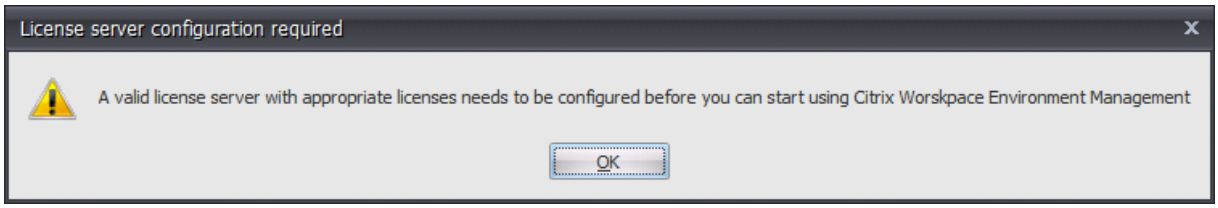


Enter the following values then click **Connect**:

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.

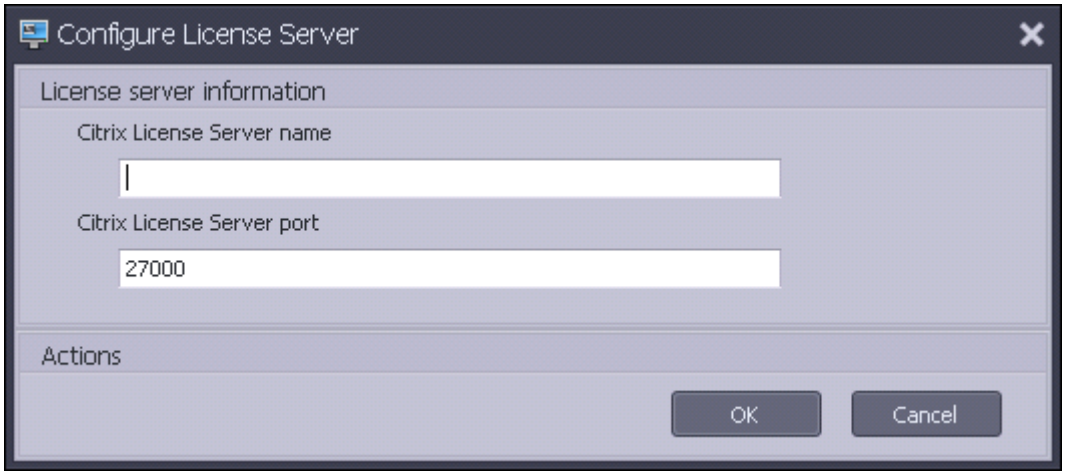
The first time you connect to a new database, you see the following message because a Citrix License Server with valid licenses is not yet configured:



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.

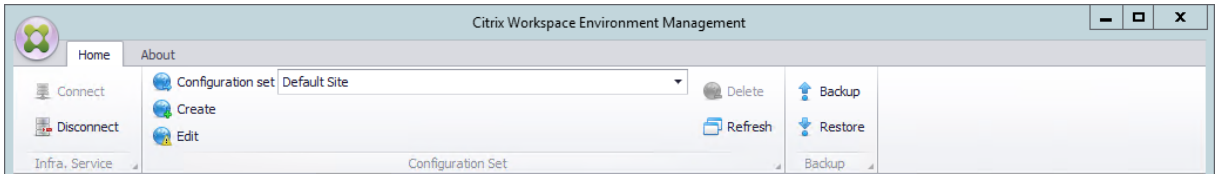
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



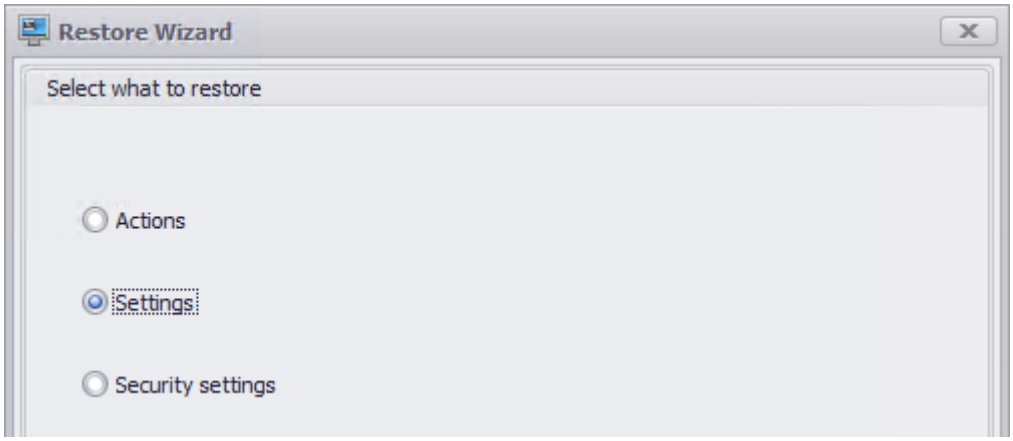
Import quickstart settings

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Agent

April 25, 2023

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)

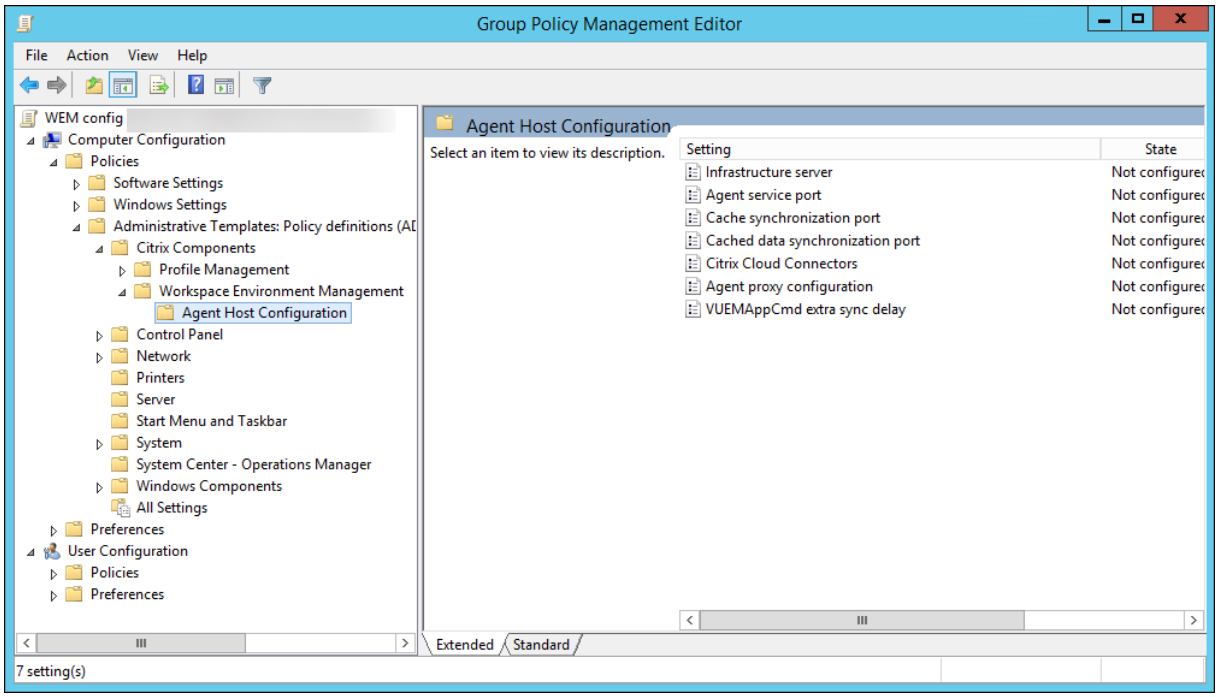
Optionally, you can choose to configure the group policies for the agent using the **Agent Group Policies** administrative template. The WEM installation package contains this template. The template files are divided into .admx files and language-specific .adml files. We recommend that you configure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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

To install the agent interactively, complete these steps:

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

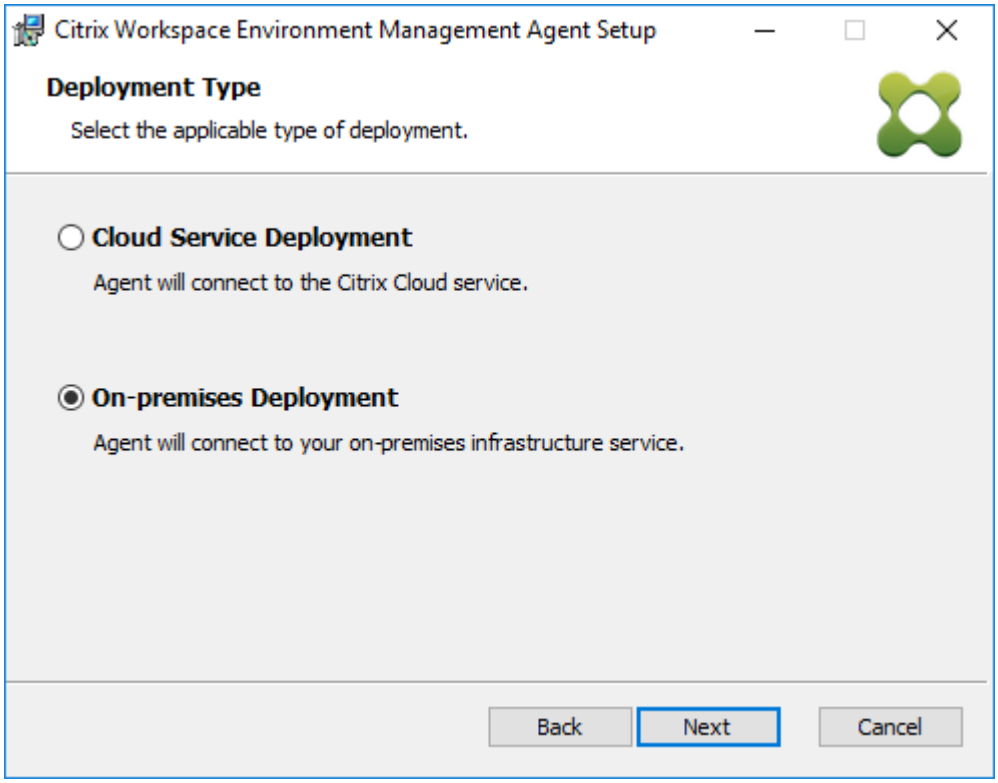
   > **Note:**
   >
   > The Welcome page can take some time to appear. This delay happens when the required software is missing and is being installed in the background.

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

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

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

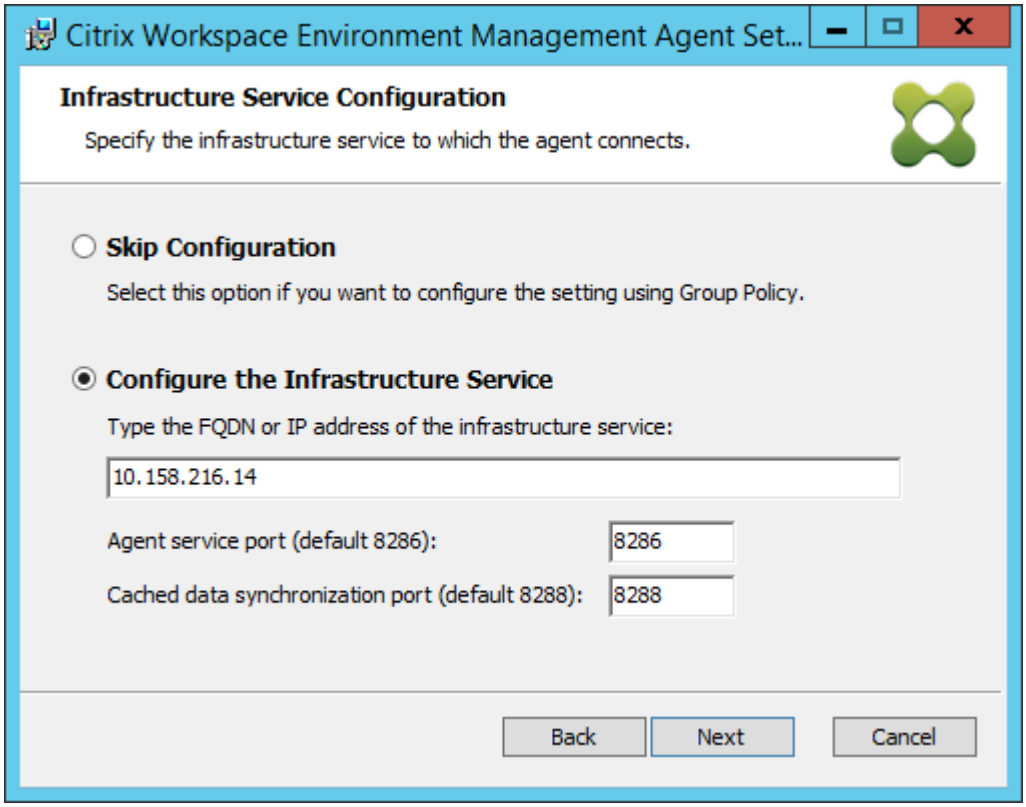
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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. Alternatively, you can do that through the registry. To do that, first stop the Citrix WEM Agent Host Service and then modify the following registry key.

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

     Name: AgentCacheAlternateLocation

     Type: REG_SZ

     Value: Empty

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

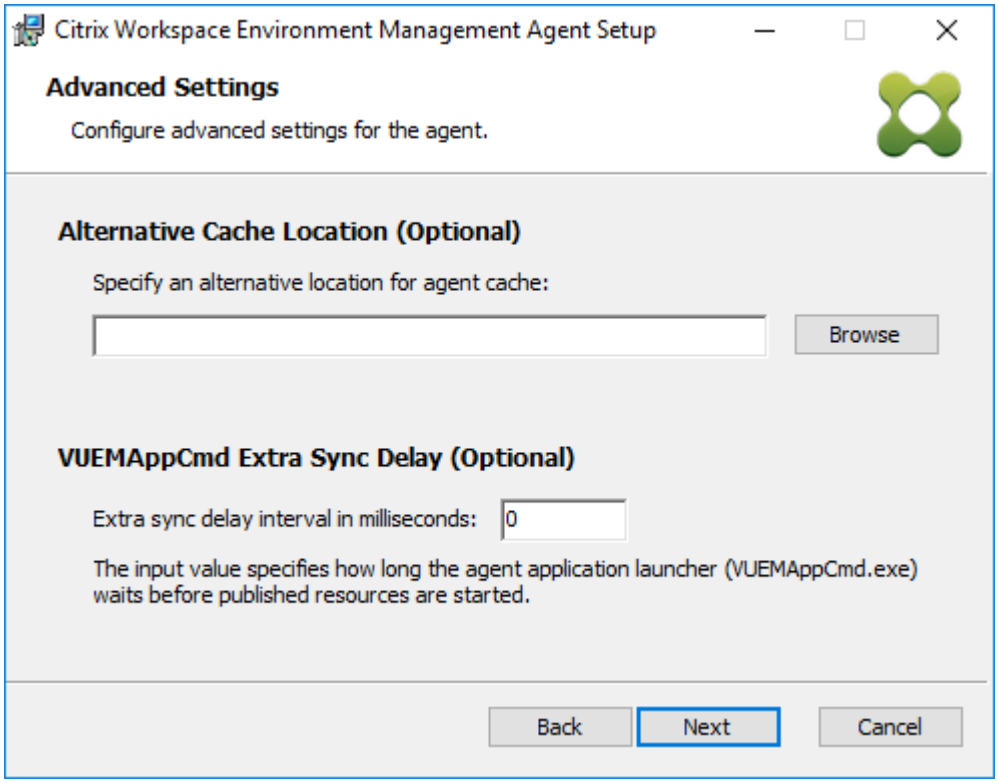
     > **Caution:**
     >
     > Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

- **VUEMAppCmd Extra Sync Delay (Optional)**. Lets you specify how long the agent application launcher (VUEMAppCmd.exe) waits before published resources 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.exe"/quiet Cloud=0`

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

Step 3: Restart the machine to complete the installation

Prerequisites and recommendations

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

Prerequisites

Verify that the following requirements are met:

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

Recommendations

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Agent startup behaviors

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

Agent cache utility options

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

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

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

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

- Refresh agent host settings:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - `AgentCacheUtility.exe -RefreshSettings`

- Refresh agent host settings and agent cache simultaneously:

  - `AgentCacheUtility.exe -RefreshSettings -RefreshCache`

- Reinitialize the agent cache:

  - `AgentCacheUtility.exe -RefreshCache -Reinitialize`

Good to know

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

Agent settings

The WEM agent settings include:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Examples

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

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

For example:

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

Scale and size considerations for deployments

December 6, 2022

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

> **Note:**
>
> - In scenarios with NTLM authentication, certain performance issues have been observed with Workspace Environment Management 2006 and earlier. Those issues have not been observed when Kerberos authentication is used.
> - No performance differences between NTLM authentication and Kerberos authentication have been observed with Workspace Environment Management 2006 and later.

Upgrade a deployment

December 6, 2022

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)
4.7	1808 or later	Yes

> **Note:**
>
> - The WEM database, infrastructure service, and administration console must all be of the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> same version.
> - Keep the following in mind when you plan to upgrade a WEM deployment earlier than 2006 to 2209 or later: To avoid database upgrade failures, upgrade to 2103 first and then to 2209 or later.

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

1. Infrastructure services
2. Database
3. Reconfiguring the infrastructure services
4. Administration console
5. Agent

Step 1: Upgrade the infrastructure services

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

Upgrade the operating system of an infrastructure server

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

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

Step 2: Upgrade the database

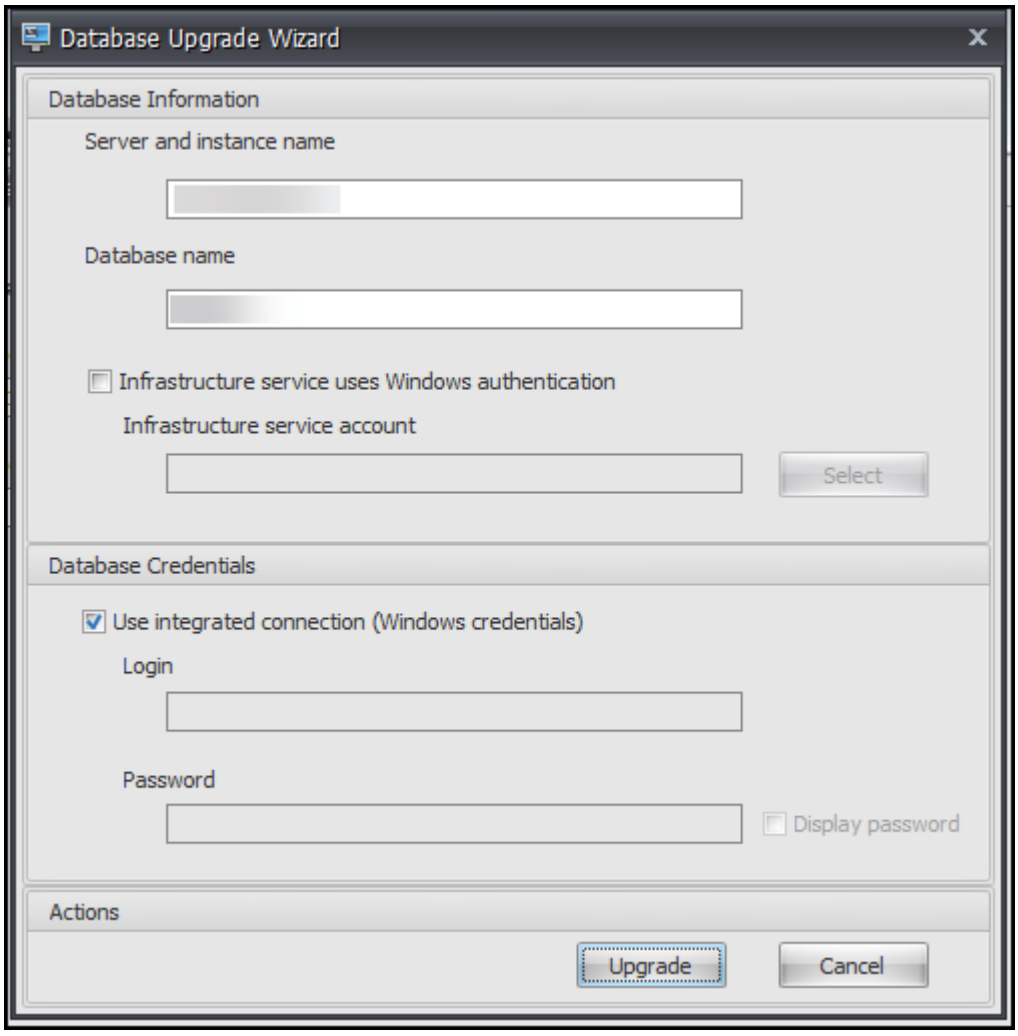
> **Important:**
>
> The database upgrade process is not reversible. Ensure that you have a valid database backup before launching the upgrade process.
>
> **Tip:**
>
> You can also upgrade the database using the Workspace Environment Management PowerShell SDK module. For SDK documentation, see Citrix Developer Documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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: Reconfigure the infrastructure services

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

Step 4: Upgrade the administration console

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

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

Step 5: Upgrade 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - 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

December 6, 2022

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

December 6, 2022

Home tab

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. You can back up the following items associated with a configuration set:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **AppLocker Rule Settings**
  - **Privilege Elevation Settings**

- **AD objects**. Backs up the users, computers, groups, and organizational units that WEM manages. The **Backup** wizard lets you specify which type of AD objects to back up. There are two types of AD objects:

  - Users. Single users and user groups
  - Machines. Single machines, machine groups, and OUs

- **Configuration set**. Backs up the WEM configuration set you selected. Each type of configuration set is exported as a separate XML file. You can back up only the current configuration set. You can back up the following items associated with a configuration set:

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

  You cannot back up the following:

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

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

- **Security Settings**. Restores all settings present on the Security tab. The settings in the backup files *replace* the existing settings in your current configuration set. When you switch to or refresh the **Security** tab, invalid application security rules are detected. Those rules are automatically deleted. Deleted rules are listed in a report that you can export if needed. The **Restore** wizard lets you select what to restore:

  - **AppLocker Rule Settings**
  - **Privilege Elevation Settings**
    - **Overwrite Existing Settings**. Controls whether to overwrite existing privilege elevation settings when there are conflicts.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actions

December 6, 2022

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

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

Fields and controls

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

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

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

Configuration

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

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

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

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

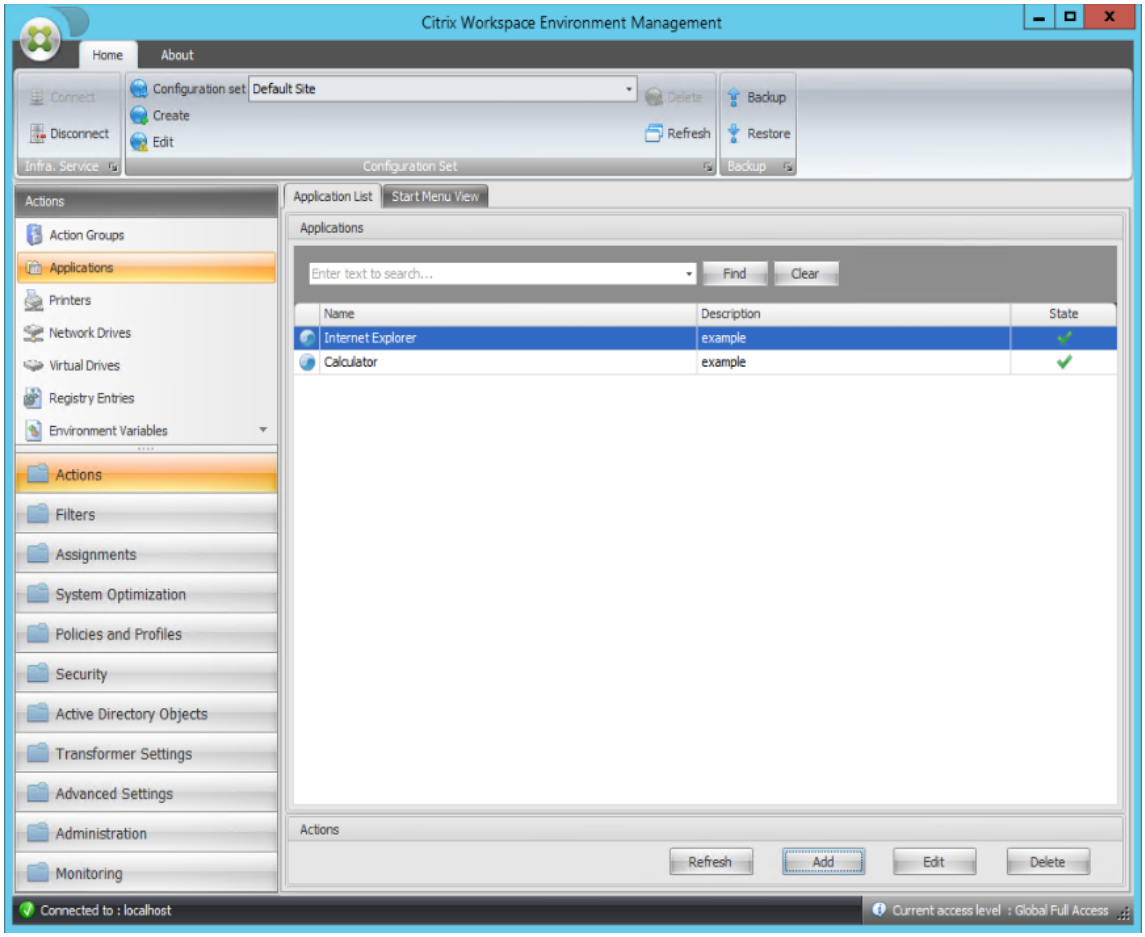
- If you assign an action group, all actions included in it are assigned.
- One or more actions might overlap in different action groups. For overlapping action groups, the group that is processed last overwrites groups that were processed earlier.
- After the actions in an action group are processed, 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.

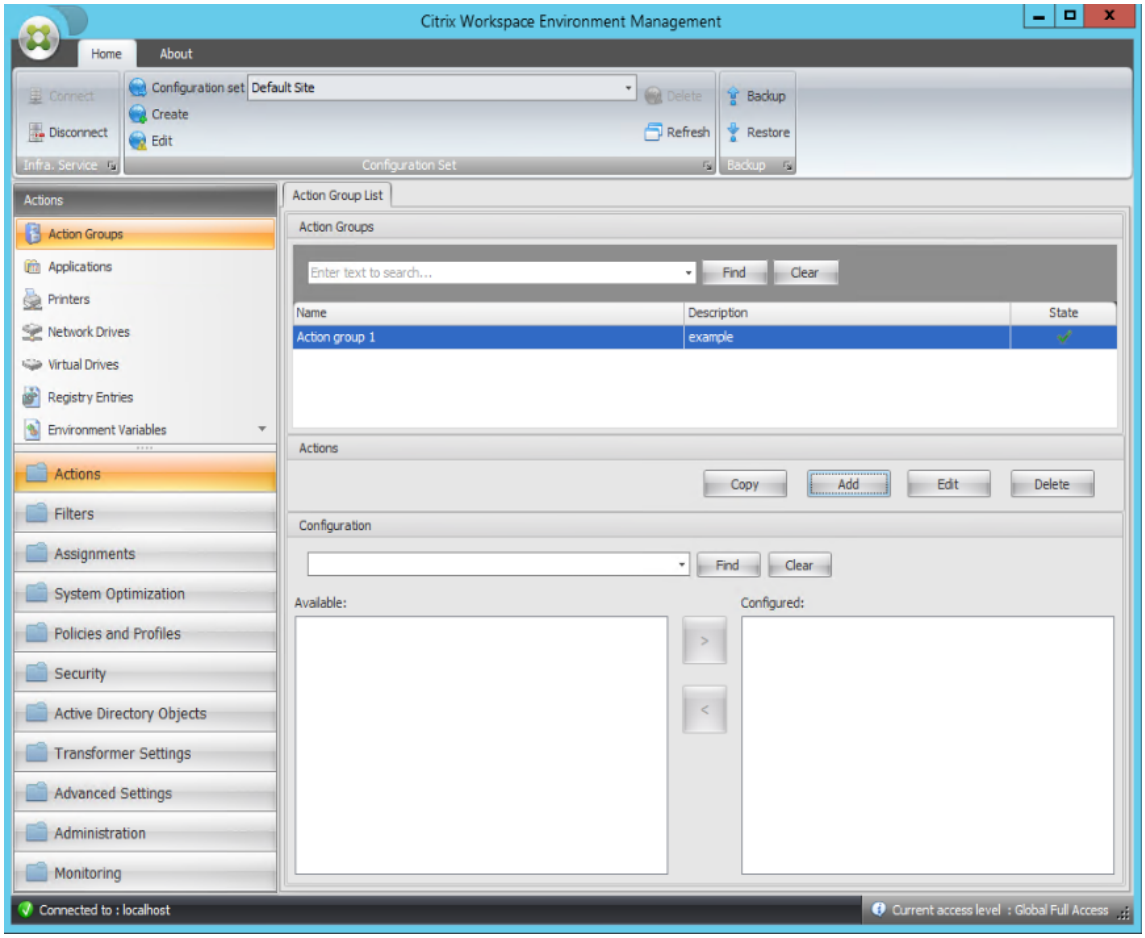
1. Go to the **Administration Console > Actions > Applications > Application List** tab and then add the applications (iexplore.exe and calc.exe).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



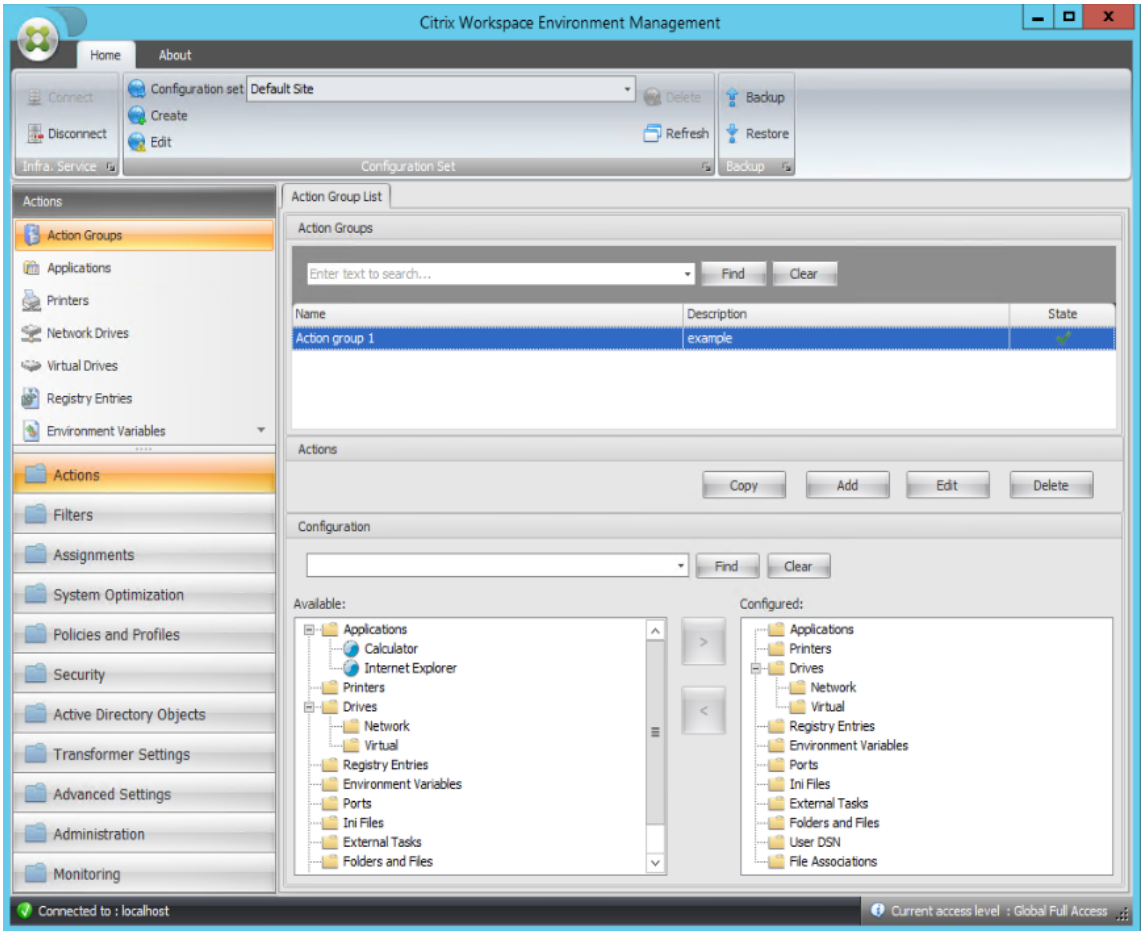
2. Go to the **Administration Console > Actions > Action Groups > Action Group List** tab and then click **Add** to create an action group.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



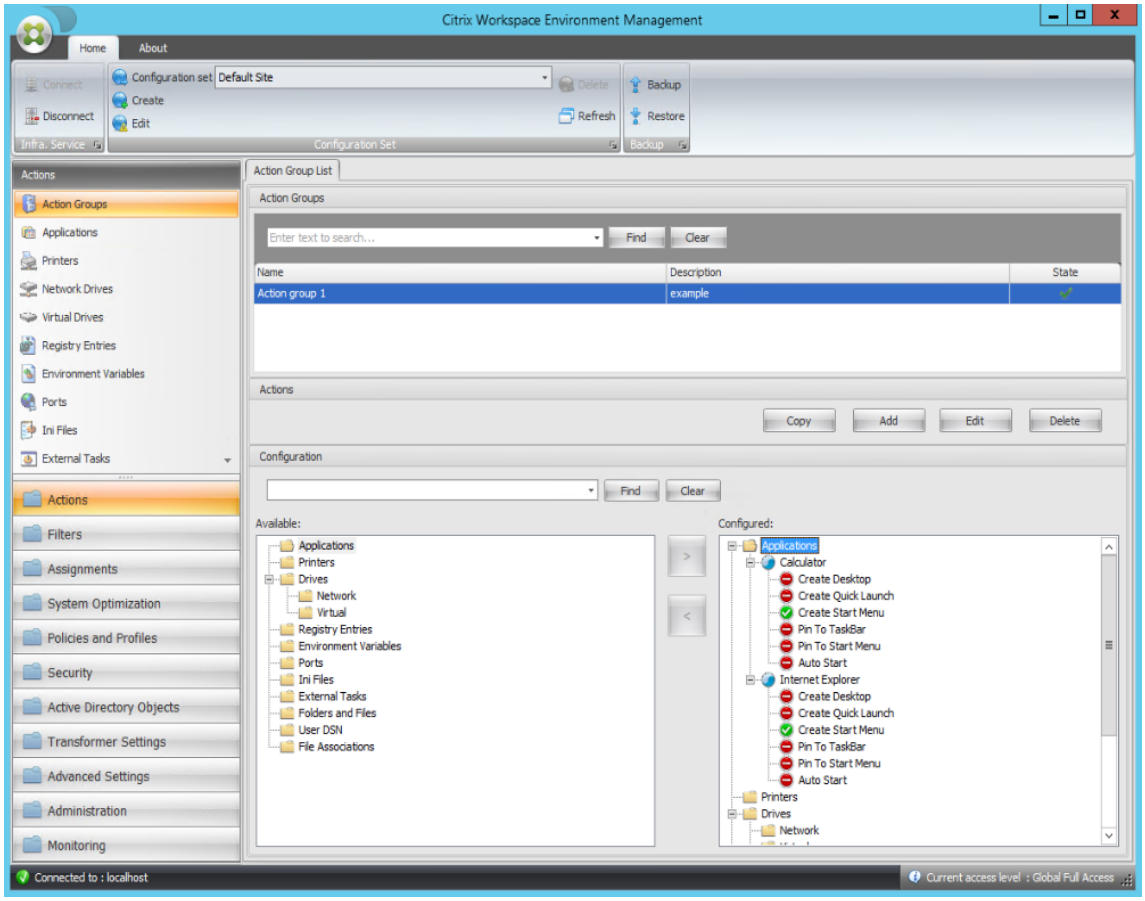
3. On the **Action Group List** tab, double-click the action group you created to display the action list in the **Available** and **Configured** panes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



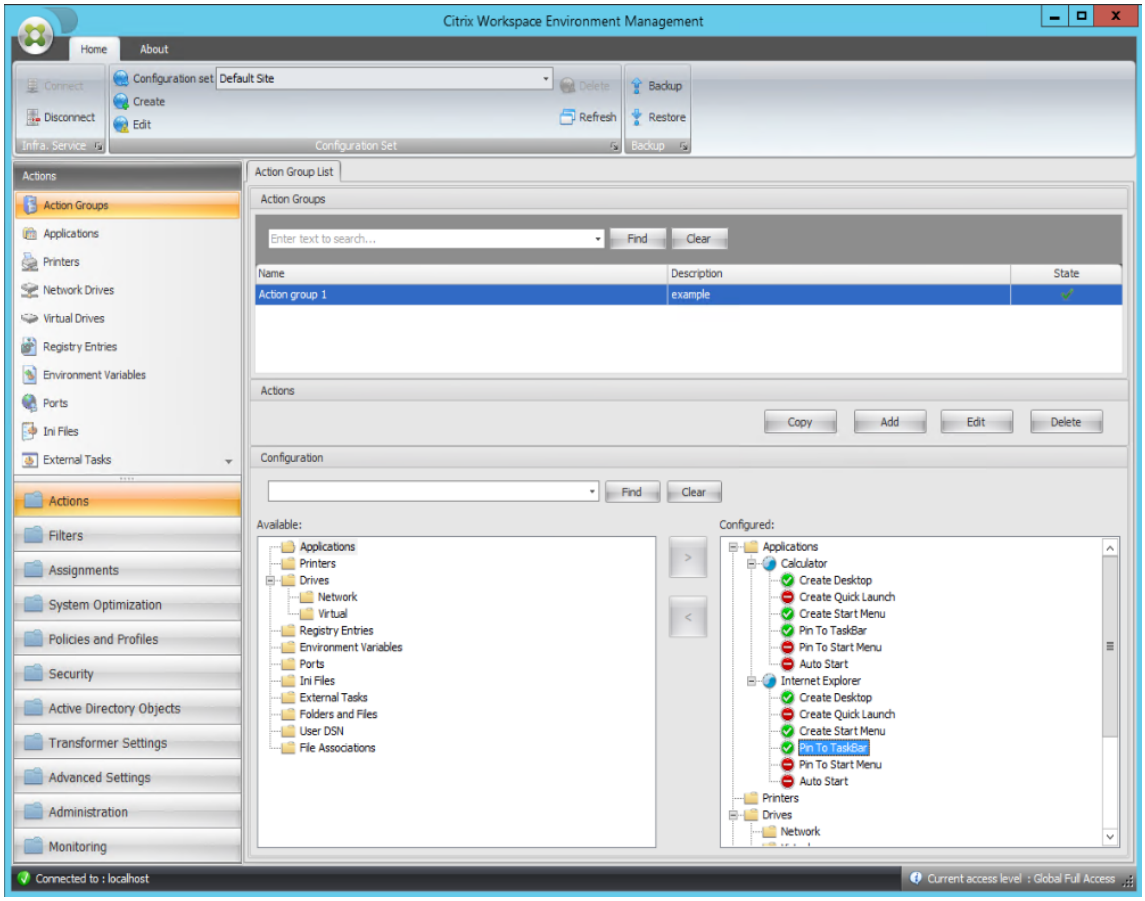
4. In the **Available** pane, double-click each application to move it to the **Configured** pane. You can also do so by selecting the application and then clicking the right arrow.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



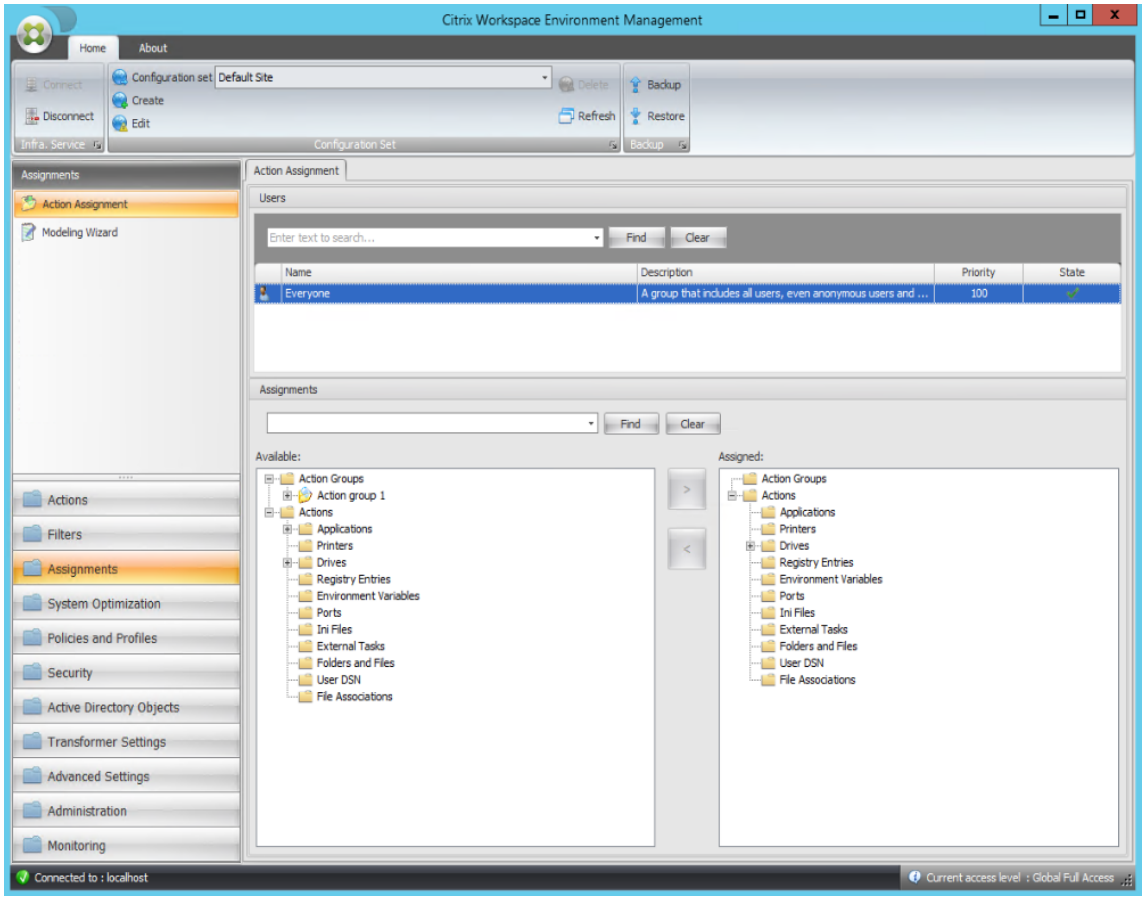
5. In the **Configured** pane, configure the options for each application. In this example, enable **Create Desktop** and **Pin To TaskBar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



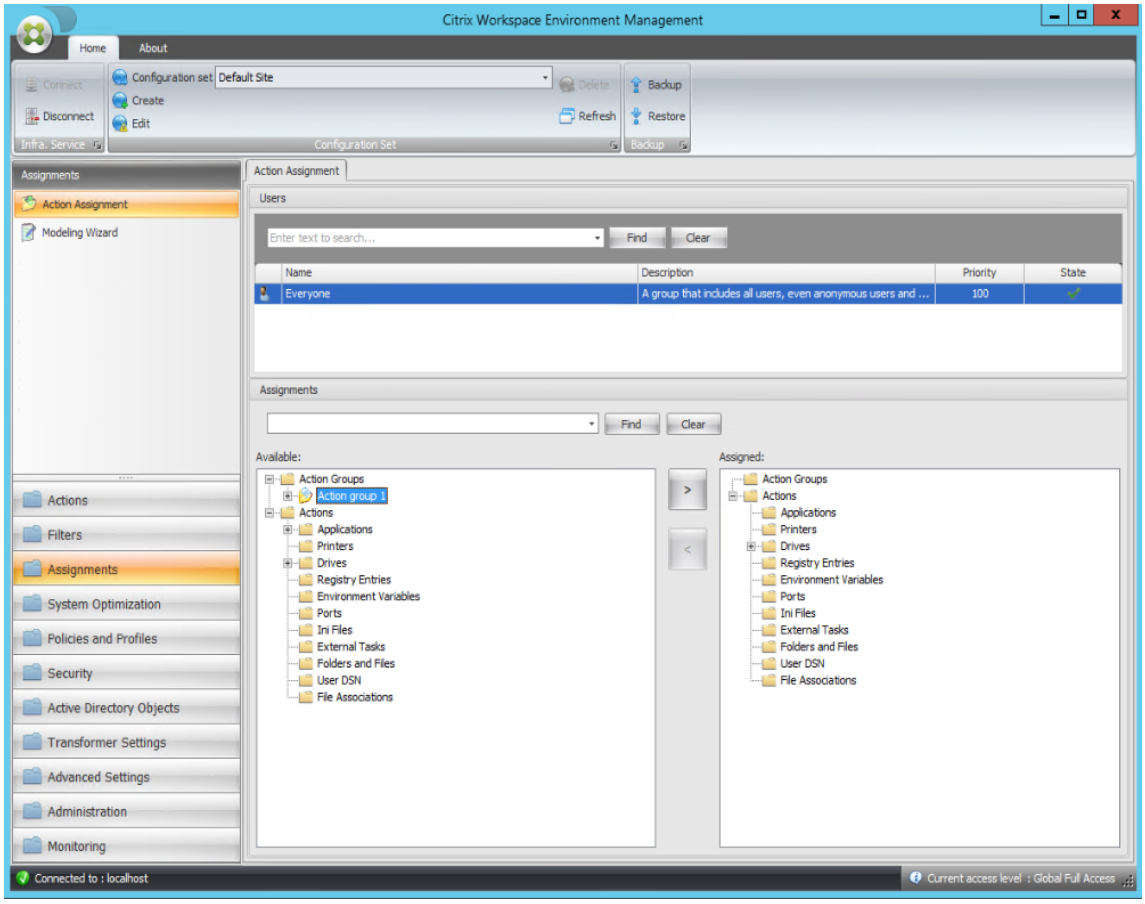
6. Go to the **Administration Console > Assignments > Action Assignment** tab and then double-click the applicable user to display the action group in the **Available** and **Assigned** panes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



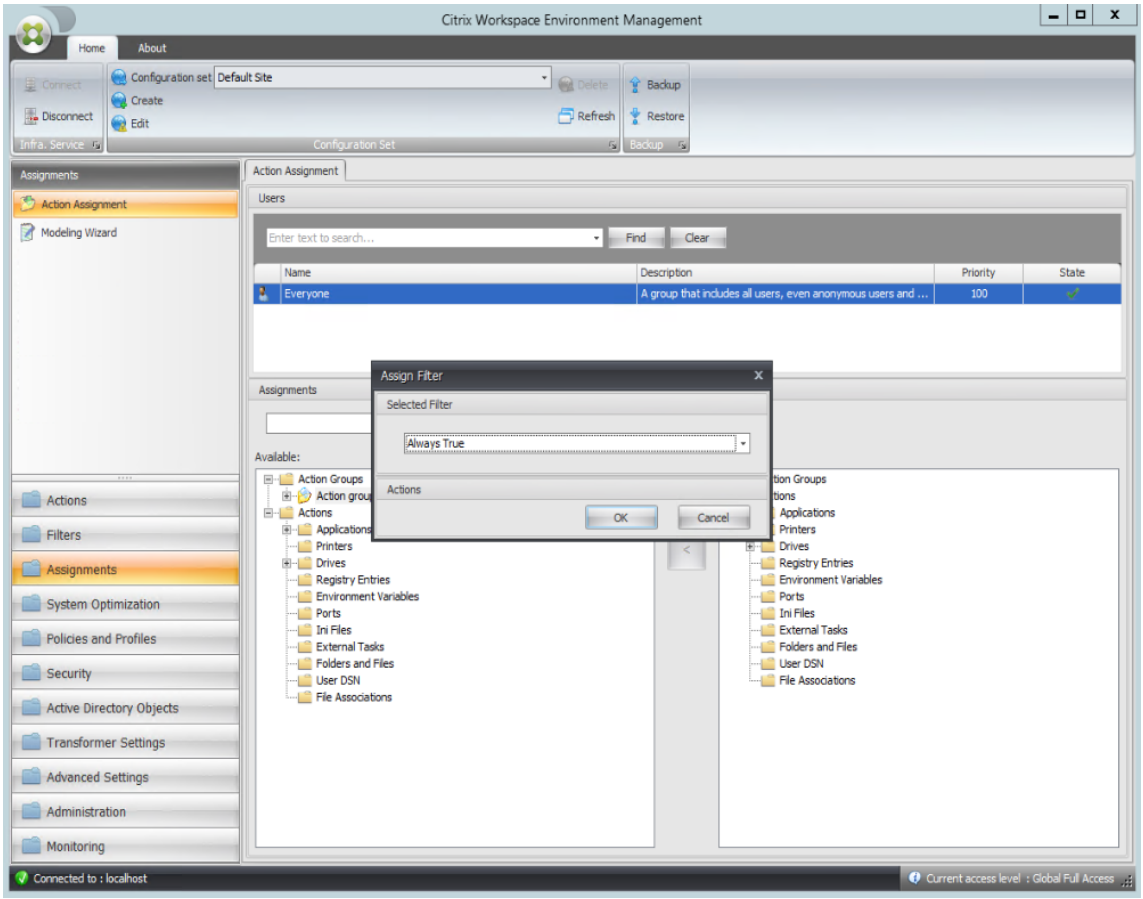
7. In the **Available** pane, double-click the action group you created (in this example, Action group 1) to move it to the **Assigned** pane. You can also do so by selecting the action group and then clicking the right arrow.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



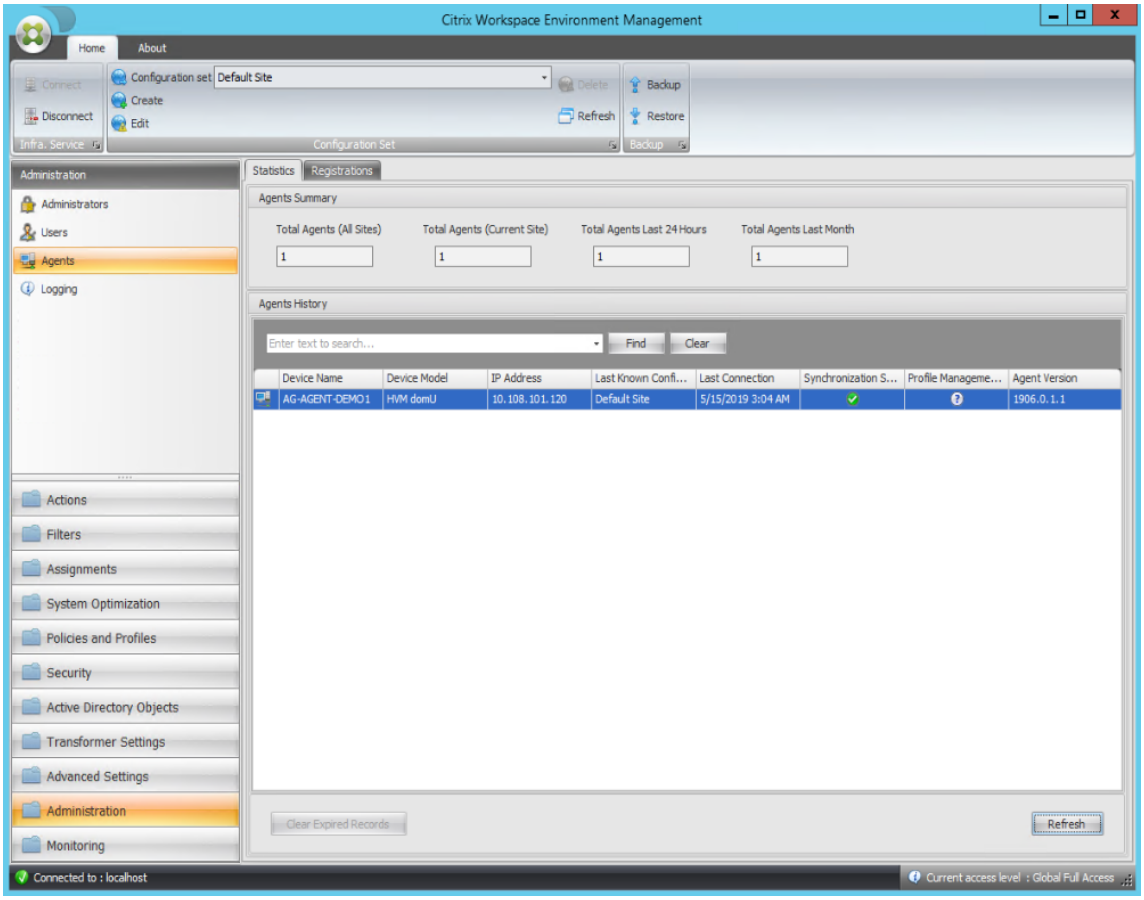
8. In the **Assign Filter** window, select **Always True** and then click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

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

Group Policy Settings

December 6, 2022

> **Important:**
>
> WEM currently supports adding and editing only Group Policy settings associated with the `HKEY_LOCAL_MACHINE` and the `HKEY_CURRENT_USER` registry hives.

In previous releases, you could migrate only Group Policy Preferences (GPP) into Workspace Environment Management (WEM). For more information, see the description of the **Migrate** wizard in Ribbon.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

You can now also import Group Policy settings (registry-based settings) into WEM.

After importing the settings, you can have an itemized view of the settings associated with each GPO before you decide which GPO to assign. You can assign the GPO to different AD groups, just like you assign other actions. If you assign GPOs to an individual user directly, the settings do not take effect. A group can contain users and machines. Machine-level settings take effect if the related machine belongs to the group. User-level settings take effect if the current user belongs to the group.

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

Group Policy settings

> **Note:**
>
> For WEM agents to process Group Policy settings properly, verify that Citrix WEM User Logon Service is enabled on them.

Enable Group Policy Settings Processing. Controls whether to enable WEM to process Group Policy settings. By default, this option is disabled. When disabled:

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

Group Policy object list

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

- **Refresh**. Refreshes the GPO list.
- **Import**. Opens the **Import Group Policy Settings** wizard, which lets you import Group Policy settings into WEM.
- **Edit**. Lets you edit an existing GPO.
- **Delete**. Deletes the GPO you select.

Import Group Policy settings

Before importing Group Policy settings, back up your Group Policy settings on your domain controller:

1. Open the Group Policy Management Console.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

Import Group Policy settings from registry files

You can convert registry values that you export using the Windows Registry Editor into GPOs for management and assignment. If you are familiar with the Import registry files option available with Registry Entries, this feature:

- Lets you import registry values under both `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`.
- Lets you import registry values of the `REG_BINARY` and `REG_MULTI_SZ` types.
- Supports converting delete operations associated with registry keys and values that you define in .reg files. For information about deleting registry keys and values by using a .reg file, see https://support.microsoft.com/en-us/topic/how-to-add-modify-or-delete-registry-subkeys-and-values-by-using-a-reg-file-9c7f37cf-a5e9-e1cd-c4fa-2a26218a1a23.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Before you start, be aware of the following:

- When importing settings from a zip file, the file can contain one or more registry files. Make sure that the size of the unzipped file is not greater than 30 M.
- Each .reg file will be converted into a GPO. You can treat each converted GPO as a set of registry settings.
- The name of each converted GPO is generated based on the name of the corresponding .reg file. Example: If the name of the .reg file is `test1.reg`, the name of the converted GPO is `test1`.
- Descriptions of converted GPOs are empty. Their state defaults to enabled (check mark icon).

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

1. In the administration console, go to **Actions > Group Policy Settings**, select **Enable Group Policy Settings Processing**, click the down arrow next to **Import**, and select **Import Registry File**.
2. In the wizard that appears, browse to the zip backup of your registry files.
    - **Overwrite existing GPOs**. Controls whether to overwrite existing GPOs when conflicts occur.
3. Click **Start Import**.
4. After the import completes, click **Finish**. GPOs converted from the registry files appear in **Group Policy Settings**.

Edit Group Policy settings

Double-click a GPO from the list for an itemized view of its settings and to edit the settings if needed.

To clone a GPO, right-click the GPO and select **Copy** from the menu. The clone is automatically created after you click **Copy**. The clone inherits the name of the original and has a suffix "-Copy."You can use **Edit** to change the name.

The **Edit Group Policy Object** window appears after you click **Edit**.

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

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

Registry Operations. Displays registry operations that the GPO contains.

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

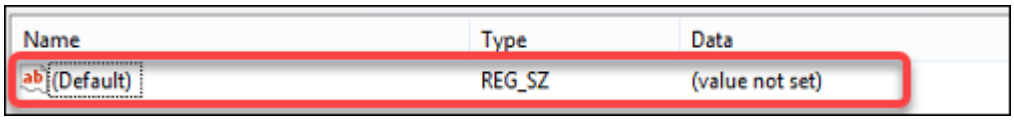
- **Add**. Lets you add a registry key.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Edit.** Lets you edit a registry key.
- **Delete.** Lets you delete a registry key.

To add a registry key, click **Add** on the right-hand side. The following settings become available:

- **Order**. Lets you specify the order of deployment for the registry key.
- **Action**. Lets you specify the type of action for the registry key.
  - **Set value**. Lets you set a value for the registry key.
  - **Delete value**. Lets you delete a value for the registry key.
  - **Create key**. Lets you create the key as specified by the combination of the root key and the subpath.
  - **Delete key**. Lets you delete a key under the registry key.
  - **Delete all values**. Lets you delete all values under the registry key.
- **Root Key**. Supported values: `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`.
- **Subpath**. The full path of the registry key without the root key. For example, if `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows` is the full path of the registry key, `Software\Microsoft\Windows` is the subpath.
- **Value**. Lets you specify a name for the registry value. The highlighted item in the following diagram as a whole is a registry value.



- **Type**. Lets you specify the data type for the value.
  - **REG_SZ**. This type is a standard string used to represent human readable text values.
  - **REG_EXPAND_SZ**. This type is an expandable data string that contains a variable to be replaced when called by an application. For example, for the following value, the string "%SystemRoot%"will be replaced by the actual location of the folder in an operating system.
  - **REG_BINARY**. Binary data in any form.
  - **REG_DWORD**. A 32-bit number. This type is commonly used for Boolean values. For example, "0"means disabled and "1"means enabled.
  - **REG_DWORD_LITTLE_ENDIAN**. A 32-bit number in little-endian format.
  - **REG_QWORD**. A 64-bit number.
  - **REG_QWORD_LITTLE_ENDIAN**. A 64-bit number in little-endian format.
  - **REG_MULTI_SZ**. This type is a multi-string used to represent values that contain lists or multiple values. Each entry is separated by a null character.
- **Data**. Lets you type data corresponding to the registry value. For different data types, you might need to type different data in different formats.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Your changes might take some time to take effect. Keep the following in mind:

- Changes associated with the `HKEY_LOCAL_MACHINE` registry hive take effect when **Citrix WEM Agent Host Service** starts or the specified **SQL Settings Refresh Delay** times out.
- Changes associated with the `HKEY_CURRENT_USER` registry hive take effect when users log on.

Contextualize Group Policy settings

You can make Group Policy settings conditional by using a filter to contextualize their assignments. A filter comprises a rule and multiple conditions. The WEM agent applies the assigned Group Policy settings only when all conditions in the rule are met in the user environment at runtime. Otherwise, the agent skips those settings when enforcing filters.

A general workflow to make Group Policy settings conditional is as follows:

1. In the administration console, navigate to **Filters > Conditions** and define your conditions. See Conditions.

   > **Important:**
   >
   > For a complete list of filter conditions available, see Filter conditions. Group Policy settings comprise user and machine settings. Some filter conditions apply only to user settings. If you apply those filter conditions to machine settings, the WEM agent ignores the filter conditions and applies the machine settings. For a complete list of filter conditions that do not apply to machine settings, see Filter conditions not applicable to machine settings.

2. Navigate to **Filters > Rules** and define your filter rule. You can include the conditions you defined in Step 1 into that rule. See Rules.
3. Navigate to **Actions > Group Policy Settings** and configure your Group Policy settings.
4. Navigate to **Administration Console > Assignments > Action Assignment** and complete the following:

   a) Double-click the user or user group to which you want to assign the settings.

   b) Select the application and click the right arrow (>) to assign them.

   c) In the **Assign Filter** window, select the rule you defined in Step 2 and then click **OK**. The settings move from the **Available** pane to the **Assigned** pane.

   d) In the **Assigned** pane, configure priority for the settings. Type an integer to specify a priority. The greater the value, the higher the priority. Settings with higher priority are processed later, ensuring that they are in effect when there is a conflict or dependency.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Filter conditions not applicable to machine settings

Filter name	Applicable to machine settings
ClientName Match	No
Client IP Address Match	No
Registry Value Match	If you configure a registry value starting with HKCU, the **Registry Value Match** filter does not work if applied to machine settings.
User Country Match	No
User UI Language Match	No
User SBC Resource Type	No
Active Directory Path Match	No
Active Directory Attribute Match	No
No ClientName Match	No
No Client IP Address Match	No
No Registry Value Match	No
No User Country Match	No
No User UI Language Match	No
No Active Directory Path Match	No
No Active Directory Attribute Match	No
Client Remote OS Match	No
No Client Remote OS Match	No
Active Directory Group Match	No
No Active Directory Group Match	No
Published Resource Name	No

Applications

March 6, 2023

Controls the creation of application shortcuts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Application list

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

To add an application

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

Fields and controls

General

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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

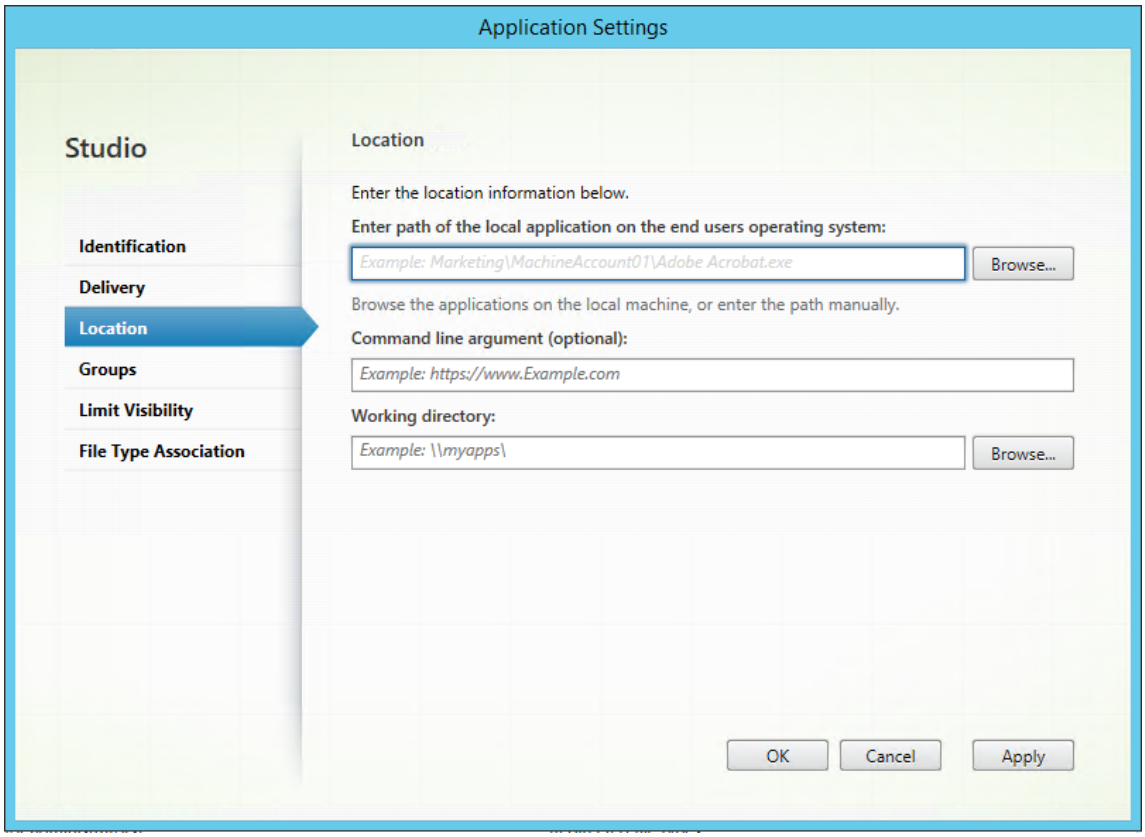
Workspace Environment Management (WEM) provides you with client-side tools to troubleshoot issues you experience. The VUEMAppCMD tool (**VUEMAppCmd.exe**) ensures that the WEM agent finishes processing an environment before Citrix Virtual Apps and Desktops published applications are started. It is located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

> **Note:**
>
> For the 64-bit OS, use `%ProgramFiles(x86)%` instead.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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%\Internet Explorer\iexplore.exe"`.

Printers

December 6, 2022

This tab controls the mapping of printers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

December 6, 2022

Controls the mapping of network drives.

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

Network drive list

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

To add a network drive

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

Fields and controls

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

December 6, 2022

Controls the mapping of virtual drives. Virtual drives are Windows virtual drives or MS-DOS device names that map local file paths to drive letters.

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

Virtual drive list

Displays a list of your existing virtual drives. You can use **Find** to filter the list by name or ID.

A general workflow to add and assign a virtual disk is as follows:

1. Go to the **Administration Console > Actions > Virtual Drives > Virtual Drives List** tab, click **Add**. Alternatively, right-click the blank area and then select **Add** in the context menu. The **New Virtual Drive** window appears.
    a) On the **General** tab, type the required information and select whether to set the virtual drive as a home drive.
    b) Click **OK** to save changes and to exit the **New Virtual Drive** window.
2. Go to the **Administration Console > Assignments > Action Assignment** tab.
    a) Double-click the user or user group to which you want to assign the virtual drive.
    b) Select the virtual drive and click the right arrow (>) to assign it.
    c) In the **Assign Filter & Driver Letter** window, select **Always True**, select a driver letter, and then click **OK**. The virtual drive moves from the **Available** pane to the **Assigned** pane.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

The assignment might take some time to take effect, depending on the value you specified for **SQL Settings Refresh Delay** on the **Advanced Settings > Configuration > Service Options** tab. Perform the following steps for the assignment to take effect immediately if needed.

1. Go to the **Administration Console > Administration > Agents > Statistics** tab and then click **Refresh**.
2. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.

Fields and controls

The General tab **Name**. The display name of the drive, as it appears in the virtual drive list.

Description. Lets you specify additional information about the virtual drive. The information appears only in the edition or creation wizard.

Target Path. Type the path to the virtual drive as it resolves in the user's environment.

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

Set as Home Drive. Lets you choose whether to set it as a home drive.

The Options tab **Action Type**. Describes what type of action this resource is.

Registry Entries

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To add a registry entry

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

Fields and controls

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

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

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

Target Path. The registry location in which the registry entry will be created. Workspace Environment Management can only create Current User registry entries, so you do not need to preface your value with %ComputerName%\HKEY_CURRENT_USER –this is done automatically.

Target Name. The name of your registry value. It will appear in the registry (for example, NoNtSecurity).

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

Target Value. The value of the registry entry once created (for example, 0 or C:\Program Files)

Run Once. By default, Workspace Environment Management creates registry entries every time the agent refreshes. Select this check box to make Workspace Environment Management create the registry entry only once - on the first refresh - rather than on every refresh. This speeds up the agent refresh process, especially if you have many registry entries assigned to your users.

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

Import registry files

You can convert your registry file into registry entries for assignment. This feature has the following limitations:

- It supports only registry values under `HKEY_CURRENT_USER`. With the registry entries feature, you can assign only registry settings under `HKEY_CURRENT_USER`.
- It does not support registry values of the `REG_BINARY` and `REG_MULTI_SZ` types.

To avoid the limitations, we recommend that you import your registry files to WEM by using the **Import Registry File** option in **Group Policy Settings**. For more information, see Import Group Policy settings from registry files.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To import a registry file, do the following:

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

Fields and controls

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

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

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

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

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

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

Environment Variables

December 6, 2022

Controls the creation of environment variables.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Environment variable list

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

To add an environment variable

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

Fields and controls

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

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

Environment Variable State. Toggles whether the environment variable is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.

Variable Name. The functional name of the environment variable.

Variable Value. The environment variable value.

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

Execution order.

Ports

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

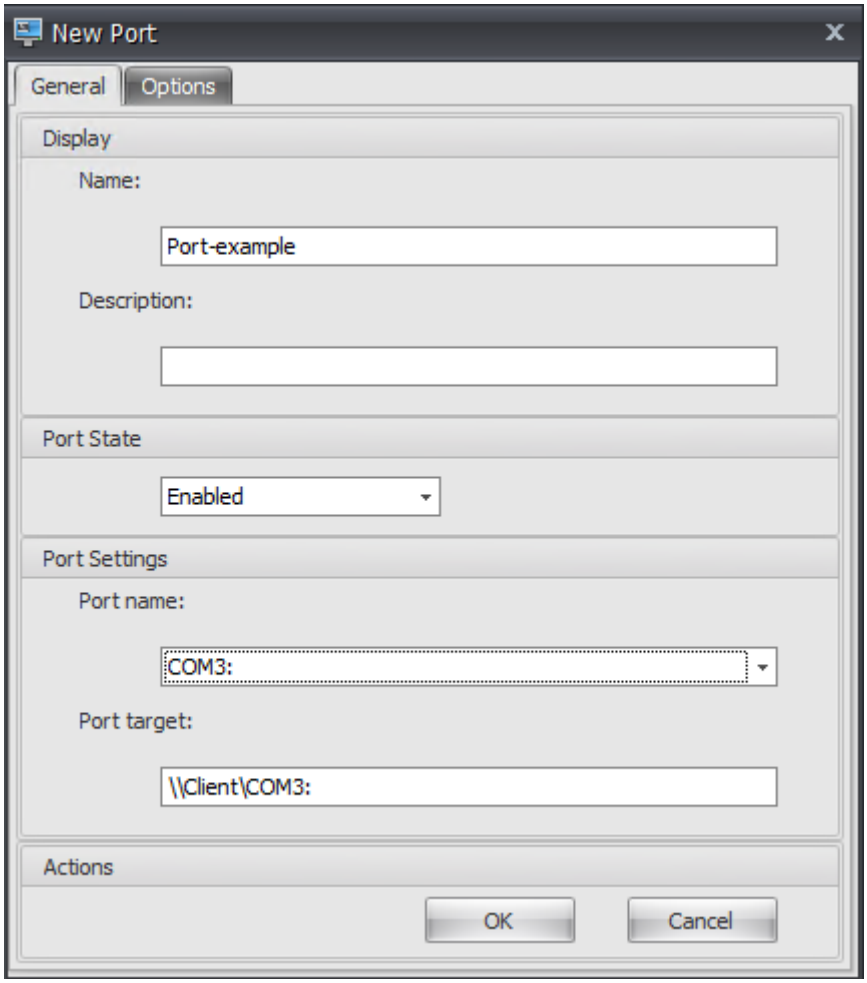
Port Target. The target port.

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:`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ini Files

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

External task list

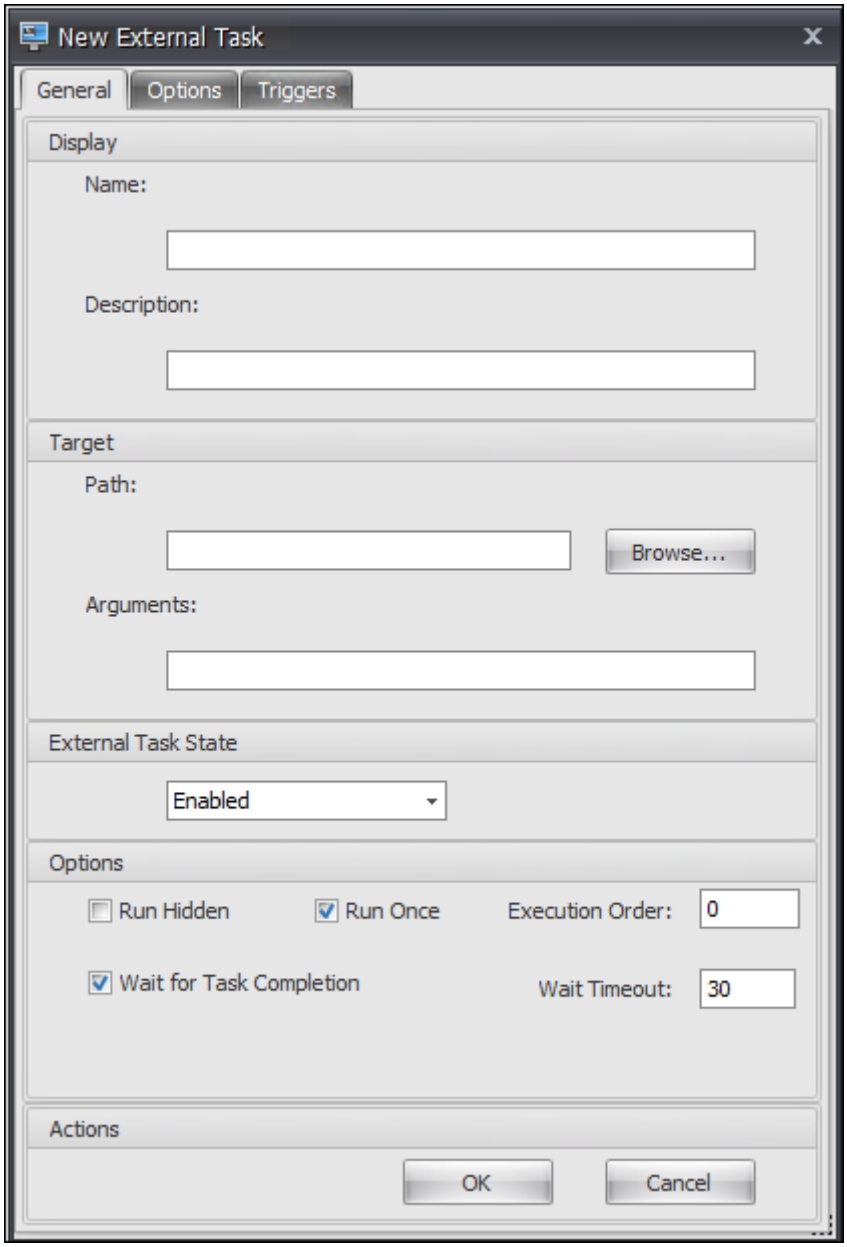
A list of your existing external tasks. You can use **Find** to filter the list.

To add an external task

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 con-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tains arguments to pass to the target script or application. For examples to use the **Path** and **Arguments** fields, see External task examples.

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

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

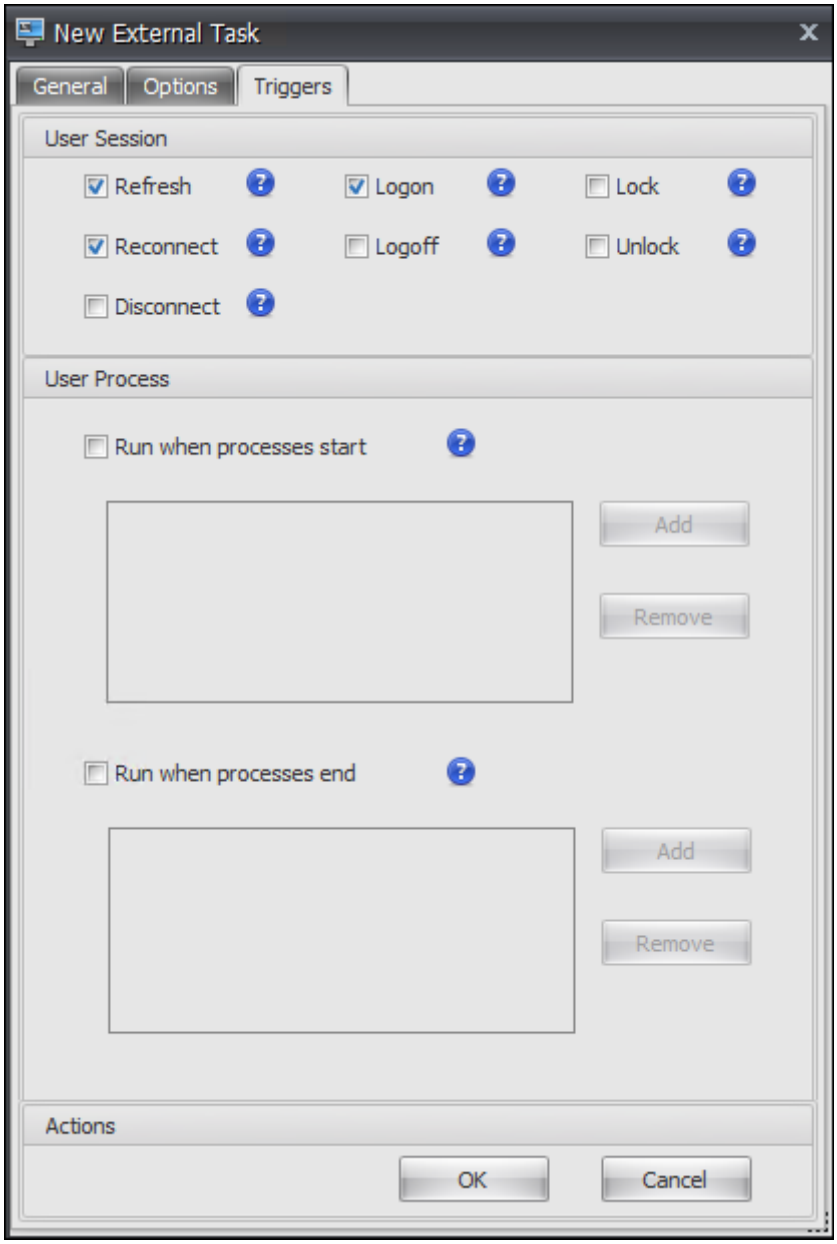
Run Once. If selected, WEM runs the task only once regardless of which options you select on the **Triggers** tab and regardless of whether agents restart. By default, this option is selected.

Execution Order. Lets you specify the running order of each task. The option can be useful when you have multiple tasks assigned to users and some of those tasks rely on others to run successfully. By default, the value is 0. Tasks with an execution order value of 0 (zero) run first, then those with a value of 1, then those with a value of 2, and so on.

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



User session triggers. This feature lets you configure the following session activities as triggers for external tasks:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Logoff**. Controls whether to run the external task when users log off. This option does not work unless Citrix User Logon Service is running. By default, the option is not selected.
- **Disconnect**. Controls whether to run the external task when a user disconnects from a machine where the agent is running. By default, the option is not selected.
- **Lock**. Controls whether to run the external task when a user locks a machine where the agent is running. By default, the option is not selected.
- **Unlock**. Controls whether to run the external task when a user unlocks a machine where the agent is running. By default, the option is not selected.

When using disconnect, lock, and unlock options, consider the following constraints:

- The implementation of these options is based on Windows events. In some environments, these options might not work as expected. For example, in desktops running on Windows 10 or Windows 11 single-session VDAs, the disconnect option does not work. Instead, use the lock option. (In this scenario, the action we receive is "lock.")
- We recommend that you use these options with the UI agent. Two reasons:
  - When you use the options with the CMD agent, the agent starts in the user environment each time the corresponding event occurs, to check whether the external task runs.
  - The CMD agent might not work optimally in concurrent task scenarios.

User process triggers. This feature lets you configure user processes as triggers for external tasks. Using this feature, you can define external tasks to supply resources only when certain processes are running and to revoke those resources when the processes end. Using processes as triggers for external tasks lets you manage your user environments more precisely compared with processing external tasks on logon or logoff.

- Before you use this feature, verify that the following prerequisites are met:
  - The WEM agent launches and runs in UI mode.
  - The specified processes run in the same user session as the logged-on user.
  - To keep the configured external tasks up to date, be sure to select **Enable Automatic Refresh** on the **Advanced Settings > Configuration > Advanced Options** tab.
- **Run when processes start**. Controls whether to run the external task when specified processes start.
- **Run when processes end**. Controls whether to run the external task when specified processes end.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Troubleshooting

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

External task examples

For a script (for example, PowerShell script):

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

  Alternatively, you can type the path to the script file directly in the **Path** field. For example: `C:\<folder path>\<script name>.ps1`. In the **Arguments** field, specify arguments if needed. However, whether the script file is run or opens with a different program depends on file type associations configured in the user environment. For information about file type associations, see File Associations.
- If the folder path or the script name contains blank spaces:
  - In the **Path** field, type the following: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.
  - In the **Arguments** field, type the following: `-file C:\<folder path>\<script name>.ps1`.

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

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

File System Operations

December 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Controls the copying of folders and files into the user's environment.

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

File system operations list

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

To add a file system operation

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

Fields and controls

Name. The display name of the file or folder operation, as it appears in the list.

Description. Lets you specify additional information about the resource. This field appears only in the edition or creation wizard.

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

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

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

Overwrite Target if Existing. Controls whether the file or folder operation overwrites existing files or folders with the same names in the target location. If cleared, and a file or folder with the same name already exists at the target location, the affected files are not copied.

Run Once. By default, Workspace Environment Management runs a file system operation every time the agent refreshes. Select this option to let Workspace Environment Management run the operation only once, rather than on every refresh. This speeds up the agent refresh process, especially if you have many file system operations assigned to your users.

Action Type. Describes what type of action this file or folder action is: **Copy**, **Delete**, **Move**, **Rename** or **Symbolic Link** operation. For symbolic link creation, you need to give users the `SeCreateSymbolicLinkPrivilege` privilege for Windows to allow symbolic link creation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Execution order. Determines the running order of operations, letting certain operations run before others. Operations with an execution order value of 0 (zero) run first, then those with a value of 1, then those with a value of 2, and so on.

User DSN

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Run Once. By default, Workspace Environment Management will create a user DSN every time the agent refreshes. Tick this box to make Workspace Environment Management only create the user DSN once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many DSNs assigned to your users.

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

File Associations

December 6, 2022

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

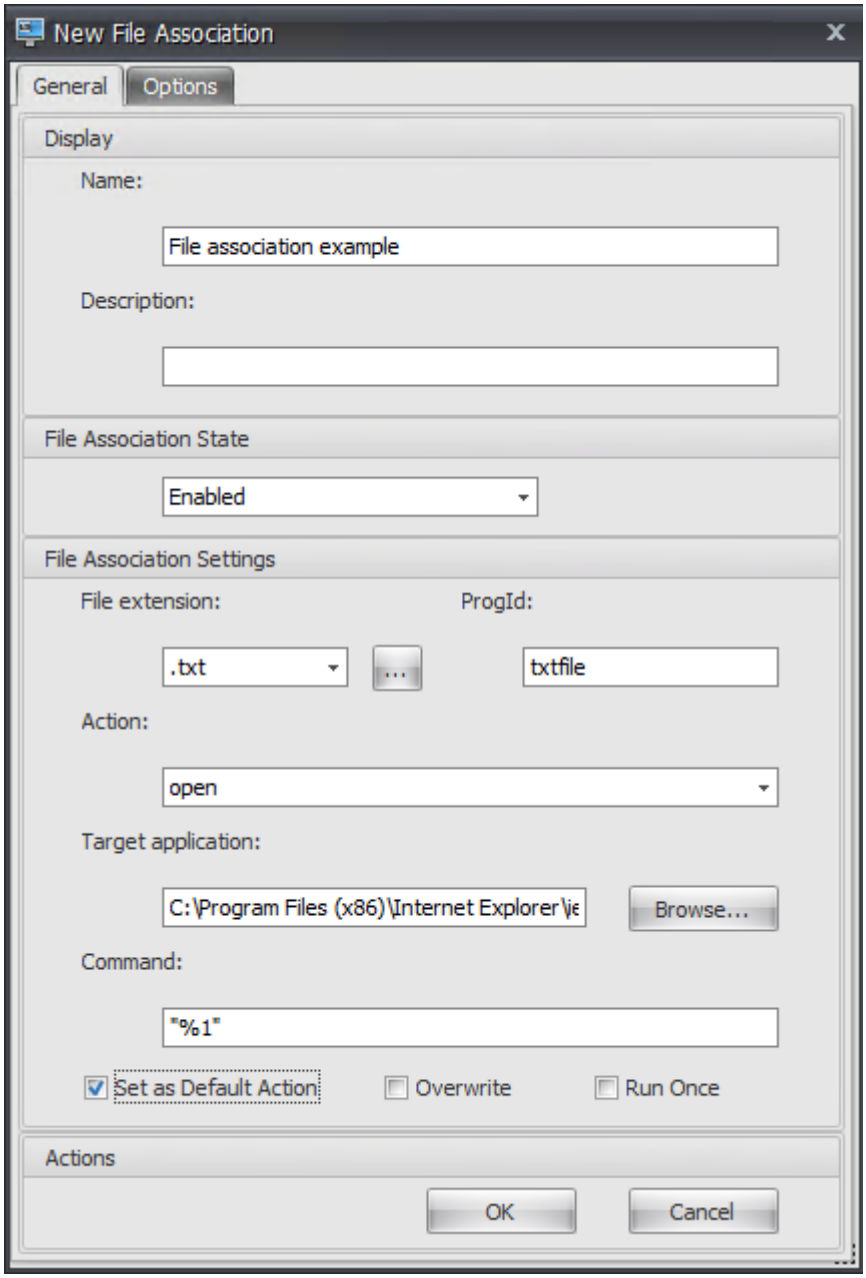
Run Once. By default, Workspace Environment Management (WEM) creates a file association every time the agent refreshes. Select this option to create the file association once, rather than on every refresh. This speeds up the agent refresh process, especially if you have many file associations assigned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

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

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

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **File Association State**. Select **Enabled**.
- **File extension**. Type the file name extension. In this example, type .txt.
- **Action**. Select **Open**.
- **Target application**. Click **Browse** to navigate to the applicable executable (.exe file). In this example, browse to iexplore.exe located in the C:\Program Files (x86)\Internet Explorer folder.
- **Command**. Type "%1"and make sure to wrap %1 in double quotes.
- Select **Set as Default Action**.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Good to know

Browser association

WEM supports creating an association for these browsers:

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

When creating browser associations, keep the following in mind:

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

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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

December 6, 2022

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To add a filter rule

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

Fields and controls

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

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

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

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

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

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

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

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To add a filter condition

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

Fields and controls

Name. The display name of the condition, as it appears in the condition list and in the rule creation/edition wizard.

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

Filter Condition State. Toggles whether the filter is enabled or disabled. When disabled, it will not appear in the rule creation/edition wizard.

Filter Condition Type. The type of filter condition type to use. See Filter conditions. Note: rules using the Always True condition will always trigger.

Settings. These are the specific settings for individual conditions. See Filter conditions.

> **Note:**
>
> When entering an IP address, you can either specify individual addresses or ranges.
>
> If you specify a range, both bounds must be specified in full. Use the dash character (**-**) to separate IP range bounds (for example **192.168.10.1-192.168.10.5**). Separate multiple ranges or addresses using the semicolon character (**;**) . For example, **192.168.10.1-192.168.10.5;192.168.10.8-192.168.10;192.168.10.17** is a valid value which includes the ranges **.1-.5** and **.8-.10**, plus the individual address **.17**.

Assignments

December 6, 2022

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> For the **Pin To Start Menu** option to work, make sure that the application shortcut exists in the Start menu folder. If unsure, enable the **Create Start Menu** option as well.

For example, say you assign an action to start Notepad. In the Assigned list, the option "Autostart"is provided and set to "Disabled"by default. If you use the **Enable** option to enable Autostart, Notepad (local Notepad on the VDA) automatically launches when the user launches a published desktop session (local Notepad automatically starts when the desktop completes loading).

Modeling wizard

The **Actions Modeling Wizard** displays the resultant actions for a given user only (it does not work for groups).

Fields and controls

Actions Modeling Target User. The account name for the user you want to model.

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

User Groups. The groups the user belongs to.

System Optimization

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

March 29, 2023

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." Unlike in **CPU Clamping**, only its priority is reduced.

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To add a process

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

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

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

To edit a process

Select the process and click **Edit**.

To remove a process

Select the process and click **Remove**.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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

December 6, 2022

These settings let you optimize application memory usage through Workspace Environment Management (WEM).

Memory management

If these settings are enabled, WEM calculates how much memory a process is using and the minimum amount of memory a process needs without losing stability. WEM considers the difference as excess memory. When the process becomes idle, WEM releases the excess memory that the process consumes to the page file, and optimizes the process for subsequent launches. Usually, an application becomes idle when it is minimized to the task bar.

When applications are restored from the task bar, they initially run in their optimized state but can continue to consume additional memory as needed.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Optimize Memory Usage for Idle Processes. Forces processes that remain idle for a specified time to release excess memory until they are no longer idle.

Idle Sample Time (min). Lets you specify the length of time that a process is considered idle after which it is forced to release excess memory. During this time, WEM calculates how much memory a process is using and the minimum amount of memory a process needs without losing stability. The default value is 120 minutes.

Idle State Limit (percent). Lets you specify the percentage of CPU usage below which a process is considered idle. The default is 1%. We recommend that you do not use a value greater than 5%. Otherwise, a process being actively used can be mistaken for idle, causing its memory to be released.

Do Not Optimize When Total Available Memory Exceeds (MB). Lets you specify a threshold limit below which WEM optimizes memory usage for idle applications.

Exclude Processes from Memory Usage Optimization. Lets you exclude processes from memory usage optimization. Specify the process name, for example, notepad.exe.

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

- `rdpshell`
- `wfshell`
- `rdpclip`
- `wmiprvse`
- `dllhost`
- `audiodg`
- `msdtc`
- `mscorsvw`
- `spoolsv`
- `smss`
- `winlogon`
- `svchost`
- `taskmgr`
- `System Idle Process`
- `System`
- `LSASS`
- `wininit`
- `msiexec`
- `services`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `csrss`
- `MsMpEng`
- `NisSrv`
- `Memory Compression`

Memory usage limit

Enable Memory Usage Limit for Specific Processes. Lets you limit the memory usage of a process by setting an upper limit for the memory the process can consume.

> **Warning:**
>
> Applying memory usage limits to certain processes might have unintended effects, including slow system responsiveness.

- **Add**. Lets you add a process to which you want to apply a memory usage limit.
- **Remove**. Lets you delete an item.
- **Edit**. Lets you edit an item.
- **Dynamic Limit**. Lets you apply a dynamic limit to the specified process. This setting dynamically limits the amount of memory allocated to the specified process. If applied, enforces memory usage limits depending on available memory. Therefore, the memory that the specified process consumes might exceed the specified amount.
- **Static Limit**. Lets you apply a static limit to the specified process. This setting always limits the amount of memory allocated to the specified process. If applied, restricts the process from consuming more than the specified amount of memory regardless of the amount of available memory. As a result, the memory that the specified process consumes is capped at the specified amount.

To add a process:

1. On the **Administration Console > System Optimization > Memory Management > Memory Usage Limit** tab, click **Add**.
2. In the **Add Process** window, type the name of the process you want to add (for example, notepad.exe.), configure the memory usage limit, select a limit mode from the drop-down menu, and then click **OK**.

To edit an item, select the item and click **Edit**.

To remove an item, select the item and click **Remove**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To apply a dynamic limit to an item, select the item and click **Dynamic Limit**.

To apply a static limit to an item, select the item and click **Static Limit**.

I/O Management

December 6, 2022

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

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

I/O priority

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

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fast Logoff

December 6, 2022

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

December 6, 2022

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

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

To get a template that you can customize, use either of the following approaches:

- Use the template builder feature that the standalone Citrix Optimizer offers. Download the standalone Citrix Optimizer at https://support.citrix.com/article/CTX224676. The template builder feature lets you build your own custom templates to be uploaded to WEM.
- On an agent host (machine where the WEM agent is installed), navigate to the `<C:\Program Files (x86)>\Citrix\Workspace Environment Management Agent\Citrix Optimizer\Templates` folder, select a default template file, and copy it to a convenient

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

folder. Customize the template file to reflect your specifics and then upload the custom template to WEM.

Settings

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

Run Weekly. If selected, WEM runs optimizations on a weekly basis. If **Run Weekly** is not selected, WEM behaves as follows:

- The first time you add a template to WEM, WEM runs the corresponding optimization. WEM runs the optimization only once unless you make changes to that template later. Changes include applying a different template to OS and moving optimization entries around between the **Available** and **Configured** panes.
- Each time you make changes to a template, WEM runs the optimization once.

> **Note:**
>
> For a non-persistent VDI environment, WEM follows the same behavior –all changes to the environment are lost when the machine restarts. In the case of Citrix Optimizer, WEM runs optimizations each time the machine restarts.

Automatically Select Templates to Use. If you are unsure which template to use, use this option to let WEM select the best match for each OS.

- **Enable Automatic Selection of Templates Starting with Prefixes**. Use this option if custom templates with different name formats are available. Type a comma-separated list of prefixes. Custom template follows this name format:
  - `prefix_<os version>_<os build>`
  - `prefix_Server_<os version>_<os build>`

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

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

To add a custom template:

1. On the **Administration Console > System Optimization > Citrix Optimizer > Citrix Optimizer** tab, click **Add**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. In the **New Custom Template** window, click **Browse** to select the applicable template, select the applicable OS from the list, configure groups contained in the template, and then click **OK**.

> **Important:**
>
> - Citrix optimizer does not support exporting custom templates. Retain a local copy of your custom template after you add it.

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

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

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

Fields and controls

Template Name. The display name of the selected template.

Applicable OSs. A list of operating systems. Select one or more operating systems to which the template applies. You can add custom templates applicable to Windows 10 OSs that are not available on the list. Add those OSs by typing their build numbers. Be sure to separate the OSs with semicolons (;). For example, 2001;2004.

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

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

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Multi-session Optimization

December 6, 2022

Multi-session OS machines run multiple sessions from a single machine to deliver applications and desktops to users. A disconnected session remains active and its applications continue to run. The disconnected session can consume resources needed for connected desktops and applications that run on the same machine. These settings let you optimize multi-session OS machines with disconnected sessions for better user experience with connected sessions.

Settings

Enable Multi-session Optimization. If enabled, optimizes multi-session OS machines where disconnected sessions are present. By default, this option is disabled. This option improves the user experience of connected sessions by limiting the number of resources disconnected sessions can consume. After a session stays disconnected for one minute, the WEM agent lowers the CPU and the I/O priorities of processes or applications associated with the session. The agent then imposes limits on the amount of memory resources the session can consume. If the user reconnects to the session, WEM restores the priorities and removes the limitations.

Exclude Specified Groups. Lets you specify which groups to exclude from multi-session optimization. Specify at least one group.

Exclude Specified Processes. Lets you specify which processes to exclude from multi-session optimization. Type the name of the process you want to exclude. Specify at least one process.

Policies and Profiles

December 6, 2022

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Environmental Settings

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

December 6, 2022

These settings allow you to optimize Microsoft User State Virtualization (USV).

Roaming profiles configuration

These settings allow you to configure Workspace Environment Management's integration with Microsoft roaming profiles.

Process User State Virtualization Configuration. Controls whether the agent processes USV settings. If disabled, no USV settings are processed.

Exclude Administrators. If enabled, USV settings you configure do not apply to administrators. When using this option, consider the following:

- Settings on the **Roaming Profiles Configuration** and **Roaming Profiles Advanced Configuration** tabs are machine-level and still apply regardless of whether the option is enabled.
- Settings on the **Folder Redirections** tabs are user-level. The option controls whether the settings apply to administrators.

Set Windows Roaming Profile Path. Lets you specify the path to your Windows profiles.

Set RDS Roaming Profiles Path. Lets you specify the path to your RDS roaming profiles.

Set RDS Home Drive Path. Lets you specify the path to your RDS home drive and the drive letter it appears with in the user environment.

Roaming profiles advanced configuration

The following are the advanced roaming profile optimization options.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Delete Cached Copies of Roaming Profiles. If enabled, the agent deletes cached copies of the roaming profiles.

Add Administrators Security Group to Roaming User Profiles. If enabled, the Administrators group is added as owner to roaming user profiles.

Do Not Check for User Ownership of Roaming Profiles Folders. If enabled, the agent does not check to see if the user owns the roaming profiles folder before acting.

Do Not Detect Slow Network Connections. If enabled, connection speed detection is skipped.

Wait for Remote User Profile. If enabled, the agent waits for the remote user profile to be fully downloaded before processing its settings.

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

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

Cleanse Profiles. This button cleans the selected profiles per the Folder Exclusion settings.

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

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

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

Folder redirection

Process Folder Redirection Configuration. This check box toggles whether the agent processes folder redirections. If it is cleared, no folder redirections are processed. Select the options to control whether and where the user's folders are redirected.

Delete Local Redirected Folders. If enabled, the agent deletes the local copies of the folders selected for redirection.

Citrix Profile Management Settings

July 26, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

In addition to using WEM to configure Citrix Profile Management features, you can use Active Directory GPOs, Citrix Studio policies, or .ini files on the VDA. We recommend that you use the same method consistently.

Main Citrix Profile Management settings

Get started with Profile Management by applying basic settings. Basic settings include processed groups, excluded groups, user store, and more.

Enable Profile Management Configuration. When enabled, you can configure and apply your settings. Enabling this option creates Profile Management related registries in the user environment. The option controls whether WEM deploys Profile Management settings you configure in the console to the agent. If disabled, none of the Profile Management settings are deployed to the agent.

Enable Profile Management. Controls whether to enable the Profile Management service on the agent machine. If disabled, the Profile Management service does not work.

You might want to disable Profile Management completely so that settings already deployed to the agent will no longer be processed. To achieve the goal, do the following:

1. Clear the **Enable Profile Management** check box and wait for the change to apply automatically or apply the change manually for immediate effect.

   > **Note:**
   >
   > The change takes some time to take effect, depending on the value you specified for **SQL Settings Refresh Delay** in Advanced Settings. For the change to take effect immediately, refresh agent host settings and then reset Profile Management settings for all related agents. See Administration.

2. After the change takes effect, clear the **Enable Profile Management Configuration** check box.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Set excluded groups. Lets you specify which groups are excluded from Profile Management.

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

Set path to user store. Lets you specify the path to the user store folder.

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

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

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

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

Profile container settings

These options control Profile Management profile container settings.

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

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

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

Enable Local Cache for Profile Container. If enabled, each local profile serves as a local cache of its profile container. If profile streaming is in use, locally cached files are created on demand. Otherwise, they are created during user logons. To use this setting, put an entire user profile in its profile container. This setting applies only to Citrix Profile Management profile containers.

Profile handling

These settings control Profile Management profile handling.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Set delay before deleting cached profiles. Lets you specify a delay (in seconds) before cached profiles are deleted on logoff.

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

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

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

Enable template profile. If enabled, 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.

Set directory of the MFT cache file. Lets you specify the MFT cache file directory. This option has been *deprecated* and will be *removed* in the future.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Replicate user stores. If enabled, Profile Management replicates a user store to multiple paths on each logon and logoff, in addition to the path that the Set path to user store option specifies. To synchronize to the user stores files and folders modified during a session, enable active write-back. Enabling the option can increase system I/O and might prolong logoffs.

Customize storage path for VHDX files. Lets you specify a separate path to store VHDX files. By default, VHDX files are stored in the user store. Policies that use VHDX files include the following: Profile container, Search index roaming for Outlook, and Accelerate folder mirroring. If enabled, VHDX files of different policies are stored in different folders under the storage path.

Enable OneDrive container. If enabled, Profile Management roams OneDrive folders with users by storing the folders on a VHDX disk. The disk is attached during logons and detached during logoffs.

Log settings

These options control Profile Management logging.

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Streamed user profiles

These options control streamed user profile settings.

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

Enable Profile Streaming for Folders. If enabled, folders are fetched only when they are being accessed. This setting eliminates the need to traverse all folders during user logons, thus saving bandwidth and reducing the time to synchronize files.

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

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

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

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

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Security

April 20, 2023

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

Application security

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

These settings let you control the applications users are permitted to run by defining rules. This functionality is similar to Windows AppLocker.

When you use Workspace Environment Management to manage Windows AppLocker rules, the agent processes (converts) Application Security tab rules into Windows AppLocker rules on the agent host. If you stop the agent processing rules, they are preserved in the configuration set and AppLocker continues running by using the last set of instructions processed by the agent.

Application security

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

- The **Overwrite** and **Merge** settings let you determine how the agent processes application security rules.
  - **Overwrite**. Lets you overwrite existing rules. When selected, the rules that are processed last overwrite rules that were processed earlier. We recommend that you apply this mode only to single-session machines.
  - **Merge**. Lets you merge rules with existing rules. When conflicts occur, the rules that are processed last overwrite rules that were processed earlier. If you need to modify the rule enforcement setting during merging, use overwrite mode because merge mode will keep the old value if it differs.

Rule collections

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

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

When you filter the rule list to a collection, the **Rule enforcement** option is available to control how

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

AppLocker enforces all rules in that collection on the agent host. The following rule enforcement values are possible:

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

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

Audit. Rules are created and set to "audit," which means they are on the agent host in an inactive state. When a user runs an app that violates an AppLocker rule, the app is allowed to run and the information about the app is added to the AppLocker event log.

To import AppLocker rules

You can import rules exported from AppLocker into Workspace Environment Management. Imported Windows AppLocker settings are added to any existing rules in the **Security** tab. Any invalid application security rules are automatically deleted and listed in a report dialog.

1. In the ribbon, click **Import AppLocker Rules**.
2. Browse to the XML file exported from AppLocker containing your AppLocker rules.
3. Click **Import**.

The rules are added to the Application Security rules list.

To add a rule

1. Select a rule collection name in the sidebar. For example, to add an executable rule select the "Executable Rules" collection.
2. Click **Add Rule**.
3. In the **Display** section, type the following details:
    - **Name**. The display name of the rule as it appears in the rule list.
    - **Description**. Additional information about the resource (optional).
4. In the **Type** section, click an option:
    - **Path**. The rule matches a file path or folder path.
    - **Publisher**. The rule matches a selected publisher.
    - **Hash**. The rule matches a specific hash code.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Tip:**
>
> - You can use the usual Windows selection modifier keys to make multiple selections, or use **Select All** to select all rows.
> - Users must already be in the Workspace Environment Management Users list.
> - You can assign rules after the rule is created.

7. Click **Next**.
8. Specify the criteria that the rule matches, depending on the rule type you choose:
    - **Path**. Specify a file path or folder path that you want the rule to match. When you choose a folder, the rule matches all files inside and below that folder.
    - **Publisher**. Specify a signed reference file that you want to use as a reference for the rule, and then use the Publisher Info slider to tune the level of property matching.
    - **Hash**. Specify a file or folder from which you want to create a hash. The rule matches the hash code of the file.
9. Click **Next**.
10. Add any exceptions you require (optional). In Add exception, choose an exception type then click **Add**. (You can **Edit** and **Remove** exceptions as required.)
11. To save the rule, click **Create**.

To assign rules to users

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

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

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 add specific processes to the allow list or block list.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Process management

Enable Process Management. Toggles whether process on the allow list or block list are in effect. If disabled, none of the settings on the **Process BlackList** and **Process WhiteList** tabs are taken into account.

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

Process block list

These settings let you add specific processes to the block list.

Enable Process Blacklist. Enable processing of processes on the block list. You must add processes by using their executable name (for example, cmd.exe).

Exclude Local Administrators. Excludes local administrator accounts.

Exclude Specified Groups. Lets you exclude specific user groups.

Process allow list

These settings let you add specific processes to the allow list. Process block lists and process allow lists are mutually exclusive.

Enable Process Whitelist. Enable processing of processes on the allow list. You must add processes by using their executable name (for example, cmd.exe). **Note** If enabled, **Enable Process Whitelist** automatically adds all processes not in the allow list to the block list.

Exclude Local Administrators. Excludes local administrator accounts (they are able to run all processes).

Exclude Specified Groups. Lets you exclude specific user groups (they are able to run all processes).

Privilege elevation

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> This feature does not apply to Citrix virtual apps.

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

Privilege elevation

When you select the **Privilege Elevation** pane in **Security**, the following options appear:

- **Process Privilege Elevation Settings**. Controls whether to enable the privilege elevation feature. When selected, enables agents to process privilege elevation settings and other options on the **Privilege Elevation** tab become available.
- **Do Not Apply to Windows Server OSs**. Controls whether to apply privilege elevation settings to Windows Server operating systems. If selected, rules assigned to users do not work on Windows Server machines. By default, this option is selected.
- **Enforce RunAsInvoker**. Controls whether to force all executables to run under the current Windows account. If selected, users are not prompted to run executables as administrators.

This tab also displays the complete list of rules that you have configured. Click **Executable Rules** or **Windows Installer Rules** to filter the rule list to a specific rule type. You can use **Find** to filter the list. The **Assigned** column displays a check mark icon for assigned users or user groups.

Supported rules

You can apply privilege elevation using two types of rules: executable rules and Windows installer rules.

- **Executable Rules**. Rules that include files with .exe and .com extensions associated with an application.
- **Windows Installer Rules**. Rules that include installer files with.msi and .msp extensions associated with an application. When you add Windows installer rules, keep the following scenario in mind:
  - Privilege elevation applies only to Microsoft's msiexec.exe. Make sure that the tool you use to deploy `.msi` and `.msp` Windows installer files is msiexec.exe.
  - Suppose that a process matches a specified Windows installer rule and its parent process matches a specified executable rule. The process cannot get elevated privileges unless the **Apply to Child Processes** setting is enabled in the specified executable rule.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

After you click the **Executable Rules** or the **Windows Installer Rules** tab, the **Actions** section displays the following actions available to you:

- **Edit**. Lets you edit an existing executable rule.
- **Delete**. Lets you delete an existing executable rule.
- **Add Rule**. Lets you add an executable rule.

To add a rule

1. Navigate to **Executable Rules** or **Windows Installer Rules** and click **Add Rule**. The **Add Rule** window appears.
2. In the **Display** section, type the following:
    - **Name**. Type the display name of the rule. The name appears in the rule list.
    - **Description**. Type additional information about the rule.
3. In the **Type** section, select an option.
    - **Path**. The rule matches a file path.
    - **Publisher**. The rule matches a selected publisher.
    - **Hash**. The rule matches a specific hash code.
4. In the **Settings** section, configure the following if needed:
    - **Apply to Child Processes**. If selected, applies the rule to all child processes that the executable starts. To manage privilege elevation at a more granular level, use the following options:
        - **Apply only to executables in the same folder**. If selected, applies the rule only to executables that share the same folder.
        - **Apply only to signed executables**. If selected, applies the rule only to executables that are signed.
        - **Apply only to executables of the same publisher**. If selected, applies the rule only to executables that share the same publisher information. This setting does not work with Universal Windows Platform (UWP) apps.

        > **Note:**
        >
        > When you add Windows install rules, the **Apply to Child Processes** setting is enabled by default and you cannot edit it.

    - **Start Time**. Lets you specify a time for agents to start applying the rule. The time format is HH:MM. The time is based on the agent time zone.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **End Time**. Lets you specify a time for agents to stop applying the rule. The time format is HH:MM. From the specified time onward, agents no longer apply the rule. The time is based on the agent time zone.
- **Add Parameter**. Lets you restrict privilege elevation to executables that match the specified parameter. The parameter works as a match criterion. Make sure that the parameter you specify is correct. For an example of how to use this feature, see Executables running with parameters. If this field is empty or contains only blank spaces, the agent applies privilege elevation to relevant executables whether or not they run with parameters.
- **Enable Regular Expressions**. Lets you control whether to use regular expressions to further expand the criterion.

5. In the **Assignments** section, select users or user groups to which you want to assign the rule. If you want to assign the rule to all users and user groups, select **Select All**.

   Tip:

   - You can use the usual Windows selection modifier keys to make multiple selections.
   - Users or user groups must already be in the list displayed on the **Administration > Users** tab.
   - You can choose to assign the rule later (after the rule is created).

6. Click **Next**.
7. Do either of the following. Different actions are needed depending on the rule type you selected in the preceding page.

   Important:

   WEM provides you with a tool named **AppInfoViewer** to obtain the following information and more from executable files: publisher, path, and hash. The tool can be useful if you want to provide relevant information for applications to be configured in the management console. For example, you can use the tool to extract relevant information from applications when using the application security feature. The tool is located in the agent installation folder.

   - **Path**. Type the path to the file or folder to which you want to apply the rule. The WEM agent applies the rule to an executable according to the executable file path.
   - **Publisher.** Fill out the following fields: **Publisher**, **Product name**, **File name**, and **File version**. You cannot leave any of the fields empty, but you can type an asterisk (*) instead. The WEM agent applies the rule according to publisher information. If applied, users can run executables that share the same publisher information.

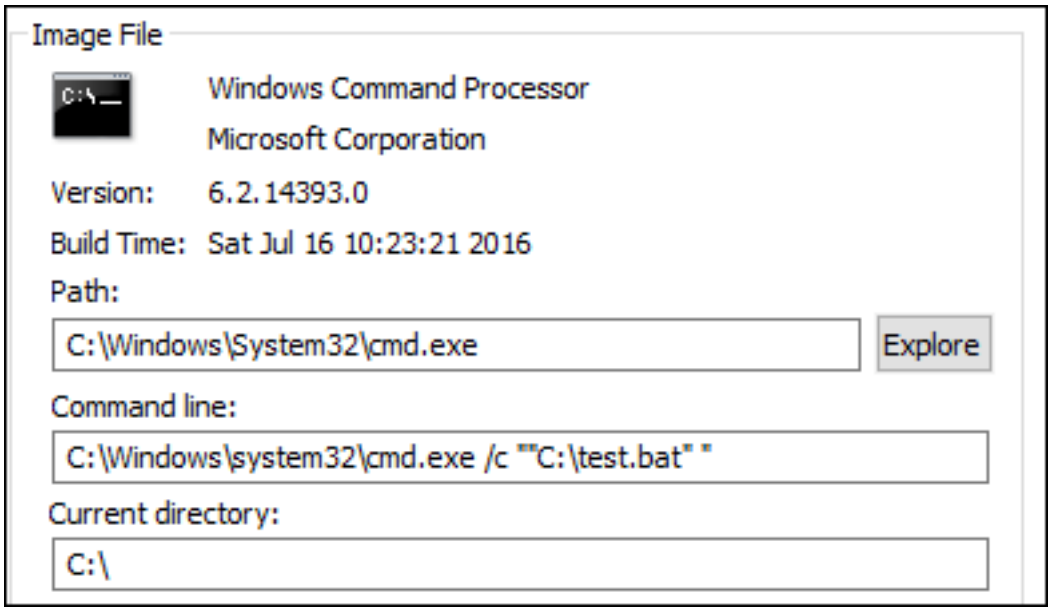
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Hash**. Click **Add** to add a hash. In the **Add Hash** window, type the file name and the hash value. You can use the **AppInfoViewer** tool to create a hash from a selected file or folder. The WEM agent applies the rule to identical executables as specified. As a result, users can run executables that are identical to the specified one.

8. Click **Create** to save the rule and to exit the window.

Executables running with parameters You can restrict privilege elevation to executables that match the specified parameter. The parameter works as a match criterion. To see parameters available to an executable, use tools such as Process Explorer or Process Monitor. Apply the parameters that appear in those tools.

Suppose you want to apply the rule to an executable (for example, cmd.exe) according to the executable file path. You want to apply privilege elevation only to `test.bat`. You can use Process Explorer to get the parameters.



In the **Add Parameter** field, you can type the following:

- `/c ""C:\test.bat""`

You then type the following in the **Path** field:

- `C:\Windows\System32\cmd.exe`

In this case, you elevate the privilege of the specified users to an administrator level only for `test.bat`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To assign rules to users Select one or more rules in the list and then click **Edit** in the **Actions** section. In the **Edit Rule** window, select users or user groups to which you want to assign the rule and then click **OK**.

To delete rules Select one or more rules in the list and then click **Delete** in the **Actions** section.

To back up privilege elevation rules You can back up all privilege elevation rules in your current configuration set. All rules are exported as a single XML file. You can use **Restore** to restore the rules to any configuration set.

To complete the backup, use the **Backup** wizard, available in the ribbon. For more information about using the **Backup** wizard, see Ribbon.

To restore privilege elevation rules You can restore privilege elevation rules from XML files exported through the Workspace Environment Management Backup wizard. The restore process replaces the rules in the current configuration set with those rules in the backup. When you switch to or refresh the **Security > Privilege Elevation** pane, any invalid privilege elevation rules are detected. Invalid rules are automatically deleted and listed in a report that you can export. For more information about using the **Restore** wizard, see Ribbon.

Self-elevation

With self-elevation, you can automate privilege elevation for certain users without the need to provide the exact executables beforehand. Those users can request self-elevation for any applicable file simply by right-clicking the file and then selecting **Run with administrator privileges** in the context menu. After that, a prompt appears, requesting that they provide a reason for the elevation. The WEM agent does not validate the reason. The reason for the elevation is saved to the database for auditing purposes. If the criteria are met, the elevation is applied, and the files run successfully with administrator privileges.

The feature also gives you flexibility to choose the best solution for your needs. You can create allow lists for files you permit users to self-elevate or block lists for files you want to prevent users from self-elevating.

Self-elevation applies to files of the following formats: `.exe`, `.msi`, `.bat`, `.cmd`, `.ps1`, and `.vbs`.

> **Note:**
>
> By default, certain applications are used to run some files. For example, cmd.exe is used to run .cmd files and powershell.exe is used to run .ps1 files. In those scenarios, you cannot change the default behavior.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

When you select **Security > Self-elevation**, the following options appear:

- **Enable self-elevation**. Controls whether to enable the self-elevation feature. Select the option to:
  - Enable agents to process self-elevation settings.
  - Make other options on the **Self-elevation** tab available.
  - Make the **Run with administrator privileges** option available in the context menu when users right-click a file. As a result, users can request self-elevation for files that match the conditions you specify on the **Self-elevation** tab.
- **Permissions**. Lets you create allow lists for files you permit users to self-elevate or block lists for files you want to prevent users from self-elevating.
  - **Allow**. Creates allow lists for files you permit users to self-elevate.
  - **Deny**. Creates block lists for files you want to prevent users from self-elevating.
- You can perform the following operations:
  - **Edit**. Lets you edit an existing condition.
  - **Delete**. Lets you delete an existing condition.
  - **Add**. Lets you add a condition. You can create a condition based on a path, a selected publisher, or a specific hash code.
- **Settings**. Lets you configure additional settings that control how agents apply self-elevation.
  - **Apply to Child Processes**. If selected, applies self-elevation conditions to all child processes that the file starts.
  - **Start Time**. Lets you specify a time for agents to start applying conditions for self-elevation. The time format is HH:MM. The time is based on the agent time zone.
  - **End Time**. Lets you specify a time for agents to stop applying conditions for self-elevation. The time format is HH:MM. From the specified time onward, agents no longer apply the conditions. The time is based on the agent time zone.
- **Assignments**. Lets you assign the self-elevation condition to applicable users or user groups. To assign the condition to all users and user groups, click **Select All** or select **Everyone**. The **Select All** check box is useful in scenarios where you want to clear your selection and reselect users and user groups.

Auditing privilege elevation activities

WEM supports auditing activities related to privilege elevation. For more information, see Auditing user activities.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Process hierarchy control

The process hierarchy control feature controls whether certain child processes can be started from their parent processes in parent-child scenarios. You create a rule by defining parent processes and then designating an allow list or a block list for their child processes. Review this entire section before using the feature.

> **Note:**
>
> - This feature applies only to Citrix virtual apps.

To understand how the rule works, keep the following in mind:

- A process is subject to only one rule. If you define multiple rules for the same process, only the rule with the highest priority is enforced.
- The rule you defined is not restricted only to the original parent-child hierarchy but also applies to each level of that hierarchy. Rules applicable to a parent process prevail over rules applicable to its child processes regardless of the priority of the rules. For example, you define the following two rules:
  - Rule 1: Word cannot open CMD.
  - Rule 2: Notepad can open CMD.

  With the two rules, you cannot open CMD from Notepad by first opening Word and then opening Notepad from Word regardless of the priority of the rules.

This feature relies on certain process-based parent-child relationships to work. To visualize the parent-child relationships in a scenario, use the process tree feature of the Process Explorer tool. For more information about Process Explorer, see https://docs.microsoft.com/en-us/sysinternals/downloads/procmon.

To avoid any potential issues, we recommend that you add an executable file path that points to **VUEMAppCmd.exe** in Citrix Studio. **VUEMAppCmd.exe** ensures that the WEM agent finishes processing settings before published applications start. In Citrix Studio, complete the following steps:

1. In **Application**, select the application, click **Properties** in the action pane, and then go to the **Location** page.
2. Type the path of the local application on the end-user operating system.
   - Under the **Path to the executable file** field, type the following: <%ProgramFiles%>\Citrix\Workspace Environment Management Agent\VUEMAppCmd.exe.
3. Type the command-line argument to specify an application to open.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Under the **Command-line argument** field, type the full path to the application that you want to launch through **VUEMAppCmd.exe**. Make sure that you wrap the command line for the application in double quotes if the path contains blank spaces.
- For example, suppose you want to launch iexplore.exe through **VUEMAppCmd.exe**. You can do so by typing the following: `%ProgramFiles(x86)%\"Internet Explorer"\iexplore.exe`.

Considerations

For the feature to work, you need to use the **AppInfoViewer** tool on each agent machine to enable the feature. (The tool is located in the agent installation folder.) Every time you use the tool to enable or disable the feature, a machine restart is required. With the feature enabled, you must restart the agent machine after upgrading or uninstalling the agent.

To verify that the process hierarchy control feature is enabled, open the **Registry Editor** on the agent machine. The feature is enabled if the following registry entry exists:

- 32-bit OS
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\WEM Hook`
- 64-bit OS
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\WEM Hook`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_Dlls\WEM Hook`

Prerequisites

To use the feature, make sure that the following prerequisites are met:

- A Citrix virtual apps deployment.
- The agent is running on Windows 10 or Windows Server.
- The agent host has been restarted after in-place upgrade or fresh install.

Process hierarchy control

When you select **Process Hierarchy Control** in **Security**, the following options appear:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Enable Process Hierarchy Control**. Controls whether to enable the process hierarchy control feature. When selected, other options on the **Process Hierarchy Control** tab become available and configured settings there can take effect. You can use this feature *only* in a Citrix virtual apps deployment.
- **Hide Open With from Context Menu**. Controls whether to show or hide the **Open With** option from the Windows right-click context menu. When enabled, the menu option is hidden from the interface. When disabled, the option is visible and users can use it to start a process. The process hierarchy control feature does not apply to processes started through the **Open With** option. We recommend that you enable this setting to prevent applications from starting processes through system services that are unrelated to the current application hierarchy.

The **Process Hierarchy Control** tab also displays the complete list of rules that you have configured. You can use **Find** to filter the list. The **Assigned** column displays a check mark icon for assigned users or user groups.

The **Actions** section displays the following actions:

- **Edit**. Lets you edit a rule.
- **Delete**. Lets you delete a rule.
- **Add Rule**. Lets you add a rule.

To add a rule

1. Navigate to **Process Hierarchy Control** and click **Add Rule**. The **Add Rule** window appears.
2. In the **Display** section, type the following:
    - **Name**. Type the display name of the rule. The name appears in the rule list.
    - **Description**. Type additional information about the rule.
3. In the **Type** section, select an option.
    - **Path**. The rule matches a file path.
    - **Publisher**. The rule matches a selected publisher.
    - **Hash**. The rule matches a specific hash code.
4. In the **Mode** section, select either of the following options:
    - **Add Child Processes to Block List**. If selected, lets you define a block list for applicable child processes after configuring a rule for their parent processes. A block list prohibits only the processes you specified from running and other processes are allowed to run.
    - **Add Child Processes to Allow List**. If selected, lets you define an allow list for applicable child processes after configuring a rule for their parent processes. An allow list allows only the processes you specified to run and other processes are prohibited from running.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> A process is subject to only one rule. If you define multiple rules for the same process, the rules are enforced in order of priority.

5. In the **Priority** section, set the priority for the rule. When configuring the priority, consider the following: The priority determines the order in which the rules you configured are processed. The greater the value, the higher the priority. Type an integer. If there is a conflict, the rule with the higher priority prevails.
6. In the **Assignments** section, select users or user groups to which you want to assign the rule. If you want to assign the rule to all users and user groups, select **Select All**.

   > **Note:**
   >
   > - You can use the usual Windows selection keys to make multiple selections.
   > - Users or user groups must already be in the list displayed on the **Administration > Users** tab.
   > - You can choose to assign the rule later (after the rule is created).

7. Click **Next**.
8. Do either of the following to configure the rule for parent processes. Different actions are needed depending on the rule type you selected on the previous page.

   - **Path**. Specify a file path or folder path that you want the rule to match. If you specify a folder path, the rule applies to all files and subfolders in that folder. The WEM agent applies the rule to an executable according to the executable file path. We do not recommend that you type only asterisk (*) to indicate a path match. Doing that might cause unintended performance issues.
   - **Publisher**. Specify a signed reference file that you want to use as a reference for the rule. Use the Publisher Info slider to tune the level of property matching. Move the slider up or down to make the rule less or more specific. If you move the slider to the Any publisher position, the rule applies to all signed files. The WEM agent applies the rule to parent processes according to publisher information. If applied, users can run executables that share the same publisher information. If necessary, you can select **Use custom values** to customize information.
   - **Hash**. Specify a file or folder from which you want to create a hash. The rule matches the hash code of the file. The WEM agent applies the rule to identical executables as specified. As a result, users can run executables that are identical to the specified one.

9. Click **Next** to configure child process settings.
10. Do either of the following to define an allow list or a block list for applicable child processes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) Select a rule type from the menu and then click **Add**. The **Child Process** window appears.
b) In the **Child Process** window, configure settings as needed. The user interface of the **Child Process** window is different depending on the rule type you selected. For a child process, the following rule types are available: **Path**, **Publisher**, and **Hash**.
c) Click **OK** to return to the **Add Rule** window. You can add more child processes or click **Create** to save the rule and to exit the window.

To assign rules to users Select one rule in the list and then click **Edit** in the **Actions** section. In the **Edit Rule** window, select users or user groups to which you want to assign the rule and then click **OK**.

To delete rules Select one or more rules in the list and then click **Delete** in the **Actions** section.

To back up rules You can back up all process hierarchy control rules in your current configuration set. All rules are exported as a single XML file. You can use **Restore** to restore the rules to any configuration set.

To complete the backup, use the **Backup** wizard, available in the ribbon. For more information about using the **Backup** wizard, see Ribbon.

To restore rules You can restore process hierarchy control rules from XML files exported through the Workspace Environment Management Backup wizard. The restore process replaces the rules in the current configuration set with those rules in the backup. When you switch to or refresh the **Security > Process Hierarchy Control** pane, any invalid rules are deleted and listed in a report that you can export. For more information about using the **Restore** wizard, see Ribbon.

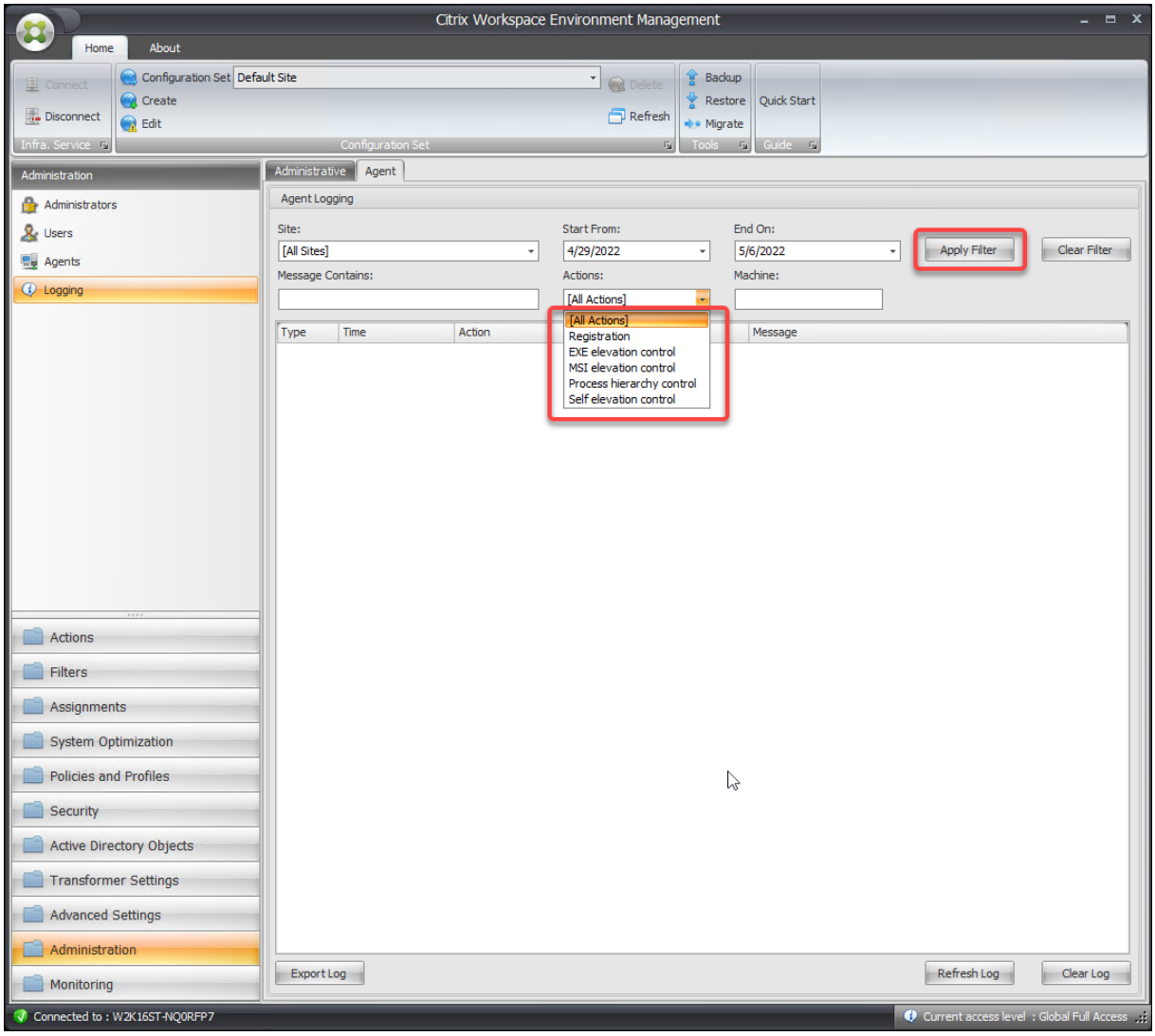
Auditing process hierarchy control activities

WEM supports auditing activities related to process hierarchy control. For more information, see Auditing user activities.

Auditing user activities

WEM supports auditing activities related to privilege elevation and process hierarchy control. To view the audits, go to the **Administration > Logging > Agent** tab. On the tab, configure logging settings, select **ElevationControl**, **Self-elevation**, or **ProcessHierarchyControl** in the **Actions** field, and then click **Apply Filter** to narrow the logs to specific activities. You can view the entire history of privilege elevation or process hierarchy control.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Active Directory Objects

December 6, 2022

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

> **Note:**
>
> Add users, computers, groups, and OUs to WEM so that the agent can manage them.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Users

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

To add a user

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

Name. The name of the user or group.

Description. Only shown in the **Edit Item** dialog. Lets you specify additional information about the user or group.

Item Priority. Lets you configure priority between different groups and user accounts. The priority determines the order in which the actions you assign are processed. Type an integer to specify a priority. The greater the value, the higher the priority. If there is a conflict (for example, when mapping different network drives with the same drive letter), the group or user account with the higher priority prevails.

> **Important:**
>
> When assigning Group Policy settings, the priority you configure here does not work. To set the priority for them, use **Administration console > Assignments**. For more information, see Contextualize Group Policy settings.

Item State. Lets you choose whether a user or group is enabled or disabled. If disabled, you cannot assign actions to it.

To add multiple users

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

Machines

A list of computers which have been added to the current site (configuration set). Only computers listed here are managed by Workspace Environment Management. When agents on these computers

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. This allows you to configure priority between different groups and user accounts. The priority determines the order in which the actions you assign are processed. The greater the value, the higher the priority. Type an integer. If there is a conflict (for example, when mapping different network drives with the same drive letter), the group or user account with the higher priority prevails.

* Read-only details reported from Active Directory.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

Site settings

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

Tool settings

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

Advanced

Process launcher

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

Advanced & administration settings

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 and power settings

Enable Autologon Mode. If enabled, users automatically log on to the desktop environment by the agent, bypassing the Windows logon screen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

December 6, 2022

These settings modify how and when the agent processes actions.

Configuration

These options control basic agent behavior.

Main configuration

Agent Actions. These settings determine whether the agent processes actions configured in the Actions tab. These settings apply on logon, and on refresh - automatic or manual refresh (user or administrator triggered).

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

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

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

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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, without awaiting the completion of the processing of other actions.

Asynchronous Network Drive Processing. If enabled, the agent processes network drives asynchronously, without awaiting the completion of the processing of other actions.

Initial Environment Cleanup. If enabled, the agent cleans up the user environment during the first logon. Specifically, it deletes the following items:

- User network printers.
  - With **Preserve Auto-created Printers** on the **Cleanup Actions** tab enabled, the agent does not delete auto-created printers.
  - With **Preserve Specific Printers** on the **Cleanup Actions** tab enabled, the agent does not delete any of the printers specified in the list.
- All network drives except the network drive that is the home drive.
- All non-system desktop, Start menu, Quick Launch, and Start-button-context-menu shortcuts.
- All taskbar and Start menu pinned shortcuts.

Initial Desktop UI Cleanup. If enabled, the agent cleans up the session desktop during the first logon. Specifically, it deletes the following items:

- All non-system desktop, Start menu, Quick Launch, and Start-button-context-menu shortcuts.
- All taskbar and Start menu pinned shortcuts.

Check Application Existence. If enabled, the agent does not create a shortcut unless it confirms that the application exists on the machine the user signs in to.

Expand App Variables. If enabled, variables are expanded by default (see Environment variables for normal behavior when the agent encounters a variable).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Allow drive letter reuse in assignment process. If enabled, a drive letter used in an assignment is still available for use by other assignments.

StoreFront

Use this tab to add a StoreFront store to Workspace Environment Management. You can then navigate to the **Actions > Applications > Application List** tab to add applications available in those stores. Do-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ing 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

UI agent options

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

Custom Background Image Path. If specified, displays a custom splash screen instead of the Citrix Workspace Environment Management logo when the agent launches or refreshes. The image must be accessible from the user environment. We recommend that you use a 400*200 px .bmp file.

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

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

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

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

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

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

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

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

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

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

> **Note:**
>
> Shortcuts created in self-healing mode cannot be deleted using this menu.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> The QuickLaunch option is available only in Windows XP and Windows Vista.

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

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

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

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

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

Helpdesk options

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

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

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

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

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

Enable Send to Support Option. Controls whether to display the **Send to support** option in the screen capture tool. If enabled, users can use the option to send screenshots and log files directly to

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

the specified support email address, in the specified format. This setting requires a working, configured email client.

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

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

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

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

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

Power saving

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

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

Administration

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Assist change management and track configurations.
- Report administrative activities.

Administrators

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

Configured administrators list

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

To add an administrator

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

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

Description. Additional information about the user or group.

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

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

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

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

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

Action Creators can create and manage actions.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Users Summary. Displays a count of total users who have reserved a Workspace Environment Management license, for both the current site (configuration set) and all sites (configuration sets). Also displays a count of new users in the last 24 hours and in the last month.

Users History. This displays connection information for all the users associated with the current site (configuration set), including the last connection time, the name of the machine from which they last connected and the session agent type (UI or CMD) and version. You can use **Find** to filter the list by name or ID against a text string.

Agents

This page displays statistics about the agents in your Workspace Environment Management deployment.

Statistics

This page displays a summary of the Workspace Environment Management agents recorded in the Workspace Environment Management database.

Agents Summary. Displays a count of total agents that have reserved a Workspace Environment Management license, for both the current configuration set and all configuration sets. It also reports agents added in the last 24 hours and in the last month.

Agents History. Displays connection information for all agents registered with the configuration set, including the last connection time, the name of the device from which they last connected, and the agent version. You can use **Find** to filter the list by name or ID.

In the **Synchronization State** column, the following icons indicate the result of the last synchronization of the agent cache with the Workspace Environment Management database.

- Successful (check mark icon). Indicates that the last synchronization was successful, with the synchronization result reported to the administration console.
- Unknown (question mark icon). Indicates that synchronization is in progress, synchronization has not started yet, or the synchronization result is not reported to the administration console.
- Failed (X icon). Indicates that the last synchronization failed.

In the **Profile Management Health Status** column, you can view the health status of Profile Management in your deployment.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

checks to identify specific issues from the output file on each agent host (`%systemroot%\temp\UpmConfigCheckOutput.xml`). The feature performs status checks every day or each time the WEM agent host service starts. To perform the status checks manually, right-click the selected agent in the administration console, and then select the **Refresh Profile Management Configuration Check** in the context menu. Each status check returns a status. To view the most recent status, click **Refresh**. The icon in the **Profile Management Health Status** column provides general information about the health status of Profile Management:

- Good (check mark icon). Indicates that Profile Management is in good shape.
- Warning (triangle exclamation point icon). Informs about a suboptimal state of Profile Management. The suboptimal settings might affect the user experience with Profile Management in your deployment. This status does not necessarily require action on your part.
- Error (X icon). Indicates that Profile Management is configured incorrectly, causing Profile Management not to function properly.
- Unavailable (question mark icon). Appears when Profile Management is not found or not enabled.

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

In the **Recently Connected** column, the following icon indicates that the agent uploaded statistics to the Workspace Environment Management database within a certain interval. The agent is online. A blank column field indicates that the agent is offline.

- Online (check mark icon)

Clear Expired Records. Lets you delete the expired records from the Workspace Environment Management database. If a user's last logon time dates back more than 24 hours, the corresponding record expires.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

July 3, 2023

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Profile container insights

This feature monitors profile containers for Profile Management and FSLogix. It provides insights into the basic usage data of the profile containers, the status of sessions using the profile containers, the issues detected, and more.

Use this feature to stay on top of space usage for profile containers and to identify problems that prevent profile containers from working.

Summary

Includes two doughnut charts:

- **Used Space**. The chart on the left side shows the space usage of profile containers over the specified time period.
- **Session Status**. The chart on the right side shows results of attaching profile containers for sessions established over the specified time period.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

After specifying the time period (for example, last 6 days), click **Refresh** to trigger a refresh of the charts.

High when used space is more than (GB). Lets you type a threshold value above which to treat the space usage of the profile containers as high. Type a positive integer.

Low when used space is less than (GB). Lets you type a threshold value below which to treat the space usage of the profile containers as low. Type a positive integer.

> **Note:**
>
> - The high threshold value must be greater than the low threshold value.
> - After specifying the high and the low threshold values, click **Refresh** to trigger a refresh of the **Used Space** chart.
> - After specifying the high and the low threshold values, space usage in between defaults to **Medium**.

Profile container status

Displays a list of status records for profile containers over a specified time period. After specifying the time period (for example, last 6 days), click the **Refresh** button to filter records.

You can trigger the collection of data for the container the selected record pertains to. Doing so brings you up to date with the user's container status. To achieve that, right-click a status record and then select **Refresh**. The refresh operation results in a sequence of tasks. First, a task is immediately sent to the associated agent host. The agent receives the task and then collects status-related data if the container is in use on the agent host. Then, the latest attach record is updated with the collected data. It might take a while for the status to be updated. Click the **Refresh** button for the up-to-date record to appear.

The **Status** column displays information about status and error codes. For information about error codes, see the Microsoft documentation at https://docs.microsoft.com/en-us/fslogix/fslogix-error-codes-reference.

Configuration

Report options

These options allow you to control the reporting period and work days. You can also specify minimum **Boot Time** and **Login Time** (in seconds) below which values are not reported.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Agent in CMD and UI mode

December 6, 2022

The Workspace Environment Management agent can run in CMD mode and UI mode.

When you configure the agent to run on logon, you can control whether to start it in CMD mode or UI mode. To do that, use the **Agent Type** setting, available on the **Administration Console > Advanced Settings > Configuration > Main Configuration** tab. For more information, see Advanced settings.

If you do not configure the agent to run automatically on logon, you (administrators or end users) can start the agent in CMD mode or UI mode on the agent machine. To do that, navigate to the agent installation folder and identify the following two .exe files:

- **VUEMCmdAgent.exe**. Lets you run the agent in CMD mode.
- **VUEMUIAgent.exe**. Lets you run the agent in UI mode.

Differences between CMD mode and UI mode

For CMD mode, be aware of the following considerations:

- When running automatically on logon, CMD mode displays a command prompt. CMD mode exits automatically after startup.
- On startup, CMD mode applies the user-assigned actions to the agent. Those actions include network drives, printers, applications, and more.
- Currently, CMD mode does not support any command-line operations.

For UI mode, be aware of the following considerations:

- When running automatically on logon, UI mode displays an agent splash screen.
- UI mode can present the following options:
  - **My Applications**. Lets you view applications assigned to you.
  - **Capture Screen**. Lets you open a screen capture tool. This option requires **Enable Screen Capture** on the **Administration Console > Advanced Settings > UI Agent Personalization > Helpdesk Options** tab to be enabled. For more information, see Helpdesk Options.
  - **Reset Actions**. Lets you open the **Reset actions** tool to specify what actions to reset in the environment.

  This option requires **Allow Users to Reset Actions** on the **Administration Console > Advanced Settings > UI Agent Personalization > UI Agent Options** tab to be enabled. For more information, see UI Agent Options.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Manage Applications**. Lets you open the **Manage applications** tool to manage applications.

  This option requires **Allow Users to Manage Applications** on the **Administration Console > Advanced Settings > UI Agent Personalization > UI Agent Options** tab to be enabled. For more information, see UI Agent Options.

  - **Manage Printers**. Lets you open the **Manage printers** tool to configure a default printer and modify printing preferences.

  This option requires **Allow Users to Manage Printers** on the **Administration Console > Advanced Settings > UI Agent Personalization > UI Agent Options** tab to be enabled. For more information, see UI Agent Options.

  - **Refresh**. Refreshes the agent, applying the user-assigned actions to the agent. Those actions include network drives, printers, applications, and more.
  - **Help**. Lets you open a website through which you can ask for help.

  This option requires **Help Link Action** on the **Administration Console > Advanced Settings > UI Agent Personalization > Helpdesk Options** tab to be specified. For more information, see Helpdesk Options.

  - **About**. Displays information about the agent version.
  - **Exit**. Lets you close the agent.

To reset actions and manage applications and printers, you can directly use the following tools (available in the agent installation folder) without the need to use the agent in UI mode:

- **ResetActionsUtil.exe**. Lets you open the **Reset actions** tool.
- **AppsMgmtUtil.exe**. Lets you open the **Manage applications** tool.
- **PrnsMgmtUtil.exe**. Lets you open the **Manage printers** tool.

Key differences between CMD mode and UI mode:

- The CMD agent applies settings and then exits. You can configure the WEM agent service (Citrix WEM Agent Host Service or Citrix WEM User Logon Service) to start the CMD agent at a particular point in time (for example, logon or reconnect). If necessary, administrators can invoke the CMD agent manually.
- The UI agent keeps running. The Citrix WEM Agent Host Service starts or stops the UI agent. The UI agent provides self-service options to end users. We recommend that administrators do not launch the UI agent manually.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> You cannot run the CMD agent and the UI agent at the same time in a session.

Common Control Panel applets

December 6, 2022

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

February 13, 2023

You can use dynamic tokens in any Workspace Environment Management actions to make them more powerful.

You can use dynamic tokens in the following fields:

- Applications
  - With **Installation application** as the application type: **Command Line**, **Working Directory**, and **Parameters**
  - With **File/Folder** as the application type: **Target**
  - With **URL** as the application type: **Shortcut URL**
  - **Icon File**
- Printers
  - **Target Path**
- Network drives
  - **Target Path** and **Display Name**
- Virtual drives
  - **Target Path**
- Registries

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Target path**, **Target name**, and **Target value**

> **Note:**
>
> The **Target value** field does not support environment variable expansion. If you use environment variables, they do not work as expected.

- Environment variables
  - **Variable value**
- Ports
  - **Port Target**
- Ini files
  - **Target path**, **Target section**, **Target value name**, and **Target value**

> **Note:**
>
> The **Target section**, **Target value name**, and **Target value** fields do not support environment variable expansion. If you use environment variables, they do not work as expected.

- External tasks
  - **Path** and **Arguments**
- File system operations
  - **Source Path** and **Target Path**
- Certain filter conditions
  - Example: With **Active Directory Attribute Match** as the condition type: **Tested Active Directory Attribute** and **Matching Result**

> **Note:**
>
> For a complete list of supported fields for filter conditions, see Supportability matrix for filter conditions.

String operations

Sometimes you need to manipulate strings within a script to map drives or launch applications. The following string operations are accepted by the Workspace Environment Management agent:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modal	Description	Example
#Left(string,length)#	Returns the specified number of characters on the left.	#Left(abcdef,2)# returns ab
#Right(string,length)#	Returns the specified number of characters on the right.	#Right(abcdef,2)# returns ef
#Truncate(string,length)#	If the length of the string is less than or equal to the specified length, returns the entire string. If the length of the string is greater than the specified length, returns the specified number of characters on the left.	#Truncate(abcdef,3)# returns abc
&Trim(string)&	Removes all leading and trailing blank spaces of the string.	&Trim(a b c)& returns a b c
&RemoveSpaces(string)&	Removes all blank spaces of the string.	&RemoveSpaces(a b c)& returns abc
&Expand(string)&	If the string contains an environment variable that is enclosed with \%, expands the variable.	&Expand(%userprofile%\destop)& returns C:\Users\Jill\desktop
$Split(string,[splitter],index)$	Splits the string into substrings based on the splitter that is enclosed with [] and returns the indexed substring.	$Split(abc-def-hij,[-],2)$ returns hij
#Mid(string,startindex)#	Starts at the specified index in the string and returns all characters after it.	#Mid(abcdef,2)# returns cdef
!Mid(string,startindex,length)!	Starts at the specified index in the string and returns the specified number of characters.	!Mid(abcdef,1,2)! returns bc
!Substring(string,startindex,length)!	Starts at the specified index in the string and returns the specified number of characters.	!Substring(abcdef,1,2)! returns bc

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modal	Description	Example
#Mod(string,length)#	Divides the string by the length and returns the remainder. The string must be able to be converted to an integer.	`#Mod(7,3)#` returns 1

> **Note:**
>
> - String operations are also supported with hashtags and Active Directory attributes. For example: `#Left([ADAttribute:NAME],2)#` where the name attribute of the current domain user is `Administrator` returns `Ad`, and `$Split(##ClientIPAddress##,[\.],2)$` returns `157`.
> - `!Mid(string,startindex,length)!` and `!Substring(string,startindex,length)!` operations are always performed last.

Hashtags

Hash-tags are a replacement feature widely used in the processing of Workspace Environment Management items. The following example illustrates how you use hash-tags:

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

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

See the following table for examples:

Modal	Description	Example
##UserName##	Returns the expanded environment variable "%username%"	Jill
##UserProfile##	Returns the expanded environment variable "%userprofile%"	C:\Users\Jill
##FullUserName##	Returns the user's full name in Active Directory	Jill Chou

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modal	Description	Example
##UserInitials##	Returns the user name initials in Active Directory	JC
##UserAppData##	Returns the actual path of the special folder - RoamingAppData	C:\Users\Jill\AppData\Roaming
##UserPersonal##	Returns the actual path of the special folder - Documents	C:\Users\Jill\Documents
##UserDocuments##	Returns the actual path of the special folder - Documents	C:\Users\Jill\Documents
##UserDesktop##	Returns the actual path of the special folder - Desktop	C:\Users\Jill\Desktop
##UserFavorites##	Returns the actual path of the special folder - Favorites	C:\Users\Jill\Favorites
##UserTemplates##	Returns the actual path of the special folder - Templates	C:\Users\Jill\AppData\Roaming\Microsoft\W
##UserStartMenu##	Returns the actual path of the special folder - StartMenu	C:\Users\Jill\AppData\Roaming\Microsoft\W Menu
##UserStartMenuPrograms##	Returns the actual path of the special folder - Programs	C:\Users\Jill\AppData\Roaming\Microsoft\W Menu\Programs
##UserLocalAppData##	Returns the actual path of the special folder - LocalAppData	C:\Users\Jill\AppData\Local
##UserMusic##	Returns the actual path of the special folder - Music	C:\Users\Jill\Music
##UserPictures##	Returns the actual path of the special folder - Pictures	C:\Users\Jill\Pictures
##UserVideos##	Returns the actual path of the special folder - Videos	C:\Users\Jill\Videos
##UserDownloads##	Returns the actual path of the special folder - Downloads	C:\Users\Jill\Downloads
##UserLinks##	Returns the actual path of the special folder - Links	C:\Users\Jill\Links
##UserContacts##	Returns the actual path of the special folder - Contacts	C:\Users\Jill\Contacts
##UserSearches##	Returns the actual path of the special folder - SavedSearches	C:\Users\Jill\Searches

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modal	Description	Example
##commonprograms##	Returns the actual path of the special folder - CommonPrograms	C:\ProgramData\Microsoft\Windows\Start Menu\Programs
##ComputerName##	Returns the machine's name	WIN10EN-LR3B66L
##ClientName##	Returns the client machine's name	W2K16ST-5IS28JP
##ClientIPAddress##	Returns the client machine's IP address	10.150.153.138
##IpAddress##	Returns the machine's IP address	10.150.153.213
##ADSite##	Returns the Active Directory site that the machine is a member of	NKG
##DefaultRegValue##	-	Always string.Empty
##UserLDAPPath##	Returns the current user's distinguished name	CN=Jill Chou,OU=User Accounts,OU=APAC,DC=citrite,DC=net
##VUEMAgentFolder##	Returns the agent folder	C:\Program Files (x86)\Citrix\Workspace Environment Management Agent
##RDSSessionID##	Returns the remote desktop session ID	2
##RDSSessionName##	Returns the remote desktop session name	RDP-Tcp#72
##ClientRemoteOS##	Returns the operating system of the machine used to connect to the virtual desktop	Windows
##ClientOSInfos##	Returns the machine's OS information	Windows 10 Enterprise 64-bit

Hash-tag **##UserScreenCaptureComment##** is implemented for use in specific parts of the product. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Active Directory attributes

To work with Active Directory attributes, WEM replaces the **[ADAttribute:attrName]** value with the related Active Directory attribute. [ADAttribute:attrName] is the dynamic token for any Active Directory attributes. There is a related filter that checks the value of the specified attributes.

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

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

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

> **Note:**
>
> - You can substitute the digit "0"with the number that corresponds to the level you want to reach in the OU structure.
> - You can append variables to the path. To do this, ensure that you have an exact folder structure that matches your OU layout.

You can also use Active Directory attributes for filtering purposes. On the **Administration > Filters > Conditions > Filter Condition List** tab, you can open the New Filter Condition window after you click **Add**. In the New Filter Condition window, you can see the following four filter condition types associated with Active Directory attributes:

- Active Directory Attribute Match
- Active Directory Group Match
- Active Directory Path Match
- Active Directory Site Match

For Active Directory Attribute Match, the dynamic token is [ADAttribute:attrName].
There is no dynamic token available for Active Directory Group Match because that condition type is used to check a group membership.
For Active Directory Path Match, the dynamic token for the full LDAP path is ##UserLDAPPath##.
For Active Directory Site Match, the dynamic token is ##ADSite##.

See the following table for examples:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modal	Description	Example
[ADAttribute:attrName]	Returns the specified attribute of the domain user	[ADAttribute:name] returns Administrator
[PrinterAttribute:printername|attrName]	Returns the specified attribute of the specified domain printer	[PrinterAttribute:printer1|name] returns printer1
[UserParentOU: level]	Returns the specified level of the current user's parent OU	[UserParentOU:1] in CN=Jill Chou,OU=User Accounts,OU=APAC,DC=citrite,DC=net returns APAC

Registries

To work with a registry, WEM replaces the [RegistryValue:<Registry path>] value with the related registry value. For example, you can specify the following value:

- [RegistryValue:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Norskale\Agent Host\AgentLocation]

XML files

To work with an XML file, WEM replaces the [GetXmlValue:<XML path>|<tag name>] value with the specific tag value in the XML file. The XML path can be an actual path or an environment variable that resolves to a path. You must enclose the environment variable with %. For example, you can specify the following value:

- [GetXmlValue:C:\citrix\test.xml|summary] or
- [GetXmlValue:%xmlpath%|summary]

INI files

To work with an .ini file, WEM replaces the [GetIniValue:<INI path>|<section name in the .ini file>|<key name in the .ini.file>] with the key value. The INI path can be an actual path or an environment variable that resolves to a path. You must enclose the environment variable with %. For example, you can specify the following value:

- [GetIniValue:C:\citrix\test.ini|PLD_POOL_LIC_NODE_0_0|LicExpTime] or
- [GetIniValue:%inipath%|PLD_POOL_LIC_NODE_0_0|LicExpTime]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

More information

Supportability matrix for filter conditions

The following table lists all condition types whose tested value or matching result supports dynamic tokens.

Condition type	Tested value	Matching result
ComputerName Match	-	Yes
ClientName Match	-	Yes
Environment Variable Match	No	Yes
Registry Value Match	Yes	Yes
WMI Query Result Match	-	Yes
XenApp Farm Name Match	-	Yes
XenApp Zone Name Match	-	Yes
XenDesktop Farm Name Match	-	Yes
XenDesktop Desktop Group Name Match	-	Yes
Active Directory Attribute Match	Yes	Yes
Name or Value is in List	Yes	Yes
No ComputerName Match	-	Yes
No ClientName Match	-	Yes
No Environment Variable Match	No	Yes
No Registry Value Match	Yes	Yes
No WMI Query result Match	-	Yes
No XenApp Farm Name Match	-	Yes
No XenApp Zone Name Match	-	Yes
No XenDesktop Farm Name Match	-	Yes
No XenDesktop Desktop Group Name Match	-	Yes
No Active Directory Attribute Match	Yes	Yes
Name or Value is not in List	Yes	Yes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

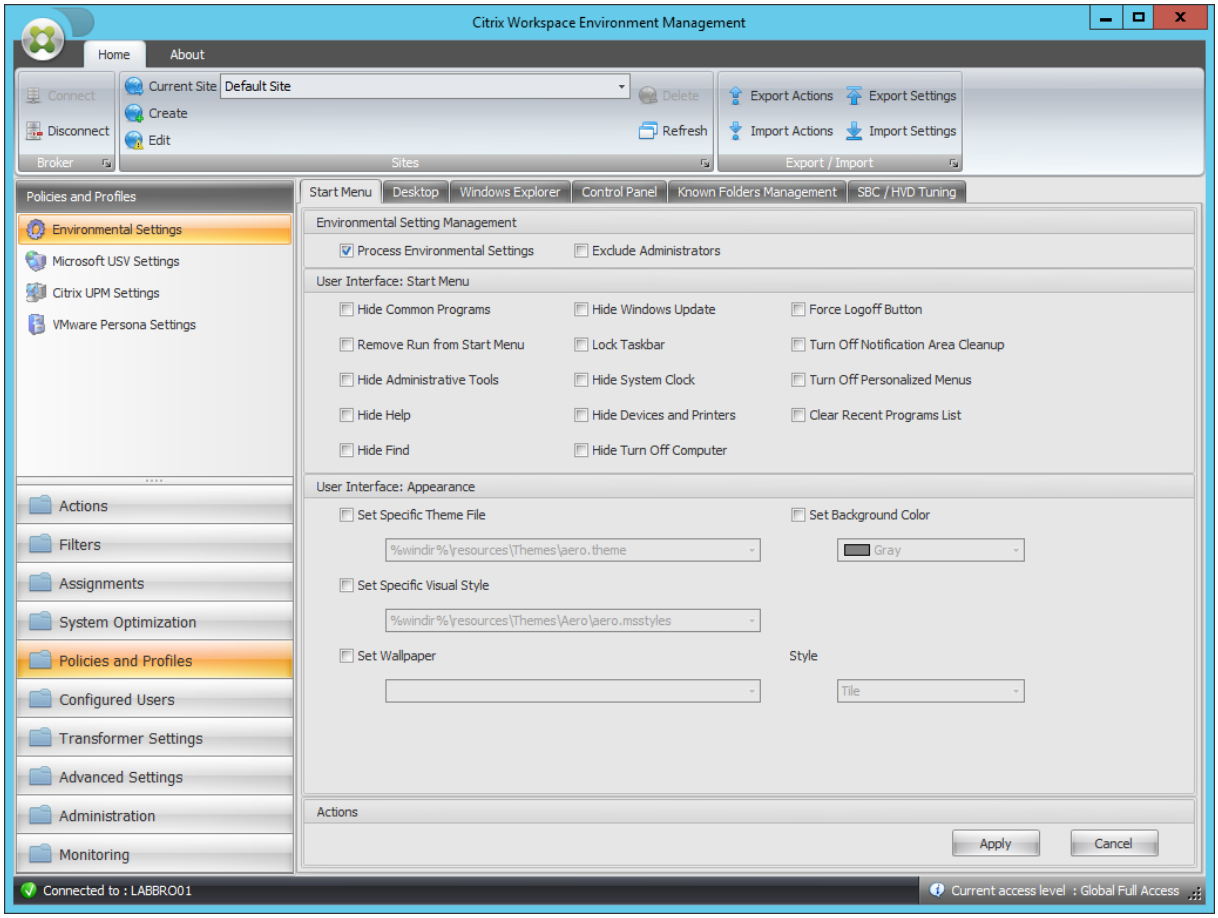
Condition type	Tested value	Matching result
Dynamic Value Match	Yes	Yes
No Dynamic Value Match	Yes	Yes
File Version Match	Yes	Yes
No File Version Match	Yes	Yes
Published Resource Name	-	Yes
Name is in List	Yes	Yes
Name is not in List	Yes	Yes
File/Folder exists	-	Yes
File/Folder does not exist	-	Yes

Environmental Settings registry values

December 6, 2022

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Hide Common Programs

Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoCommonGroups
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Remove Run from Start Menu

Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoRun
Value Type	DWORD

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Remove Run from Start Menu	
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Hide Administrative Tools	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\
Value Name	Start_AdminToolsRoot
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service called by agent

Hide Help	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hide Find	
Processing	Service called by agent

Hide Windows Update	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoWindowsUpdate
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Lock Taskbar	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	LockTaskbar
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Hide System Clock	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	HideClock
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hide Devices and Printers	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\
Value Name	Start_ShowPrinters
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service called by agent

Hide Turn Off Computer	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoClose
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Force Logoff Button	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	ForceStartMenuLogoff
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Turn Off Notification Area Cleanup	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoAutoTrayNotify

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Turn Off Notification Area Cleanup	
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Turn Off Personalized Menus	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	Intellimenus
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service at logon

Clear Recent Programs List	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	ClearRecentProgForNewUserInStartMenu
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Set Specific Theme File	
Parent Key	HKCU\Software\Policies\Microsoft\Windows\Personalization
Value Name	ThemeFile
Value Type	REG_SZ
Enabled Value	Path specified in console

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Set Specific Theme File	
Disabled Value	Value is absent
Processing	Service at logon

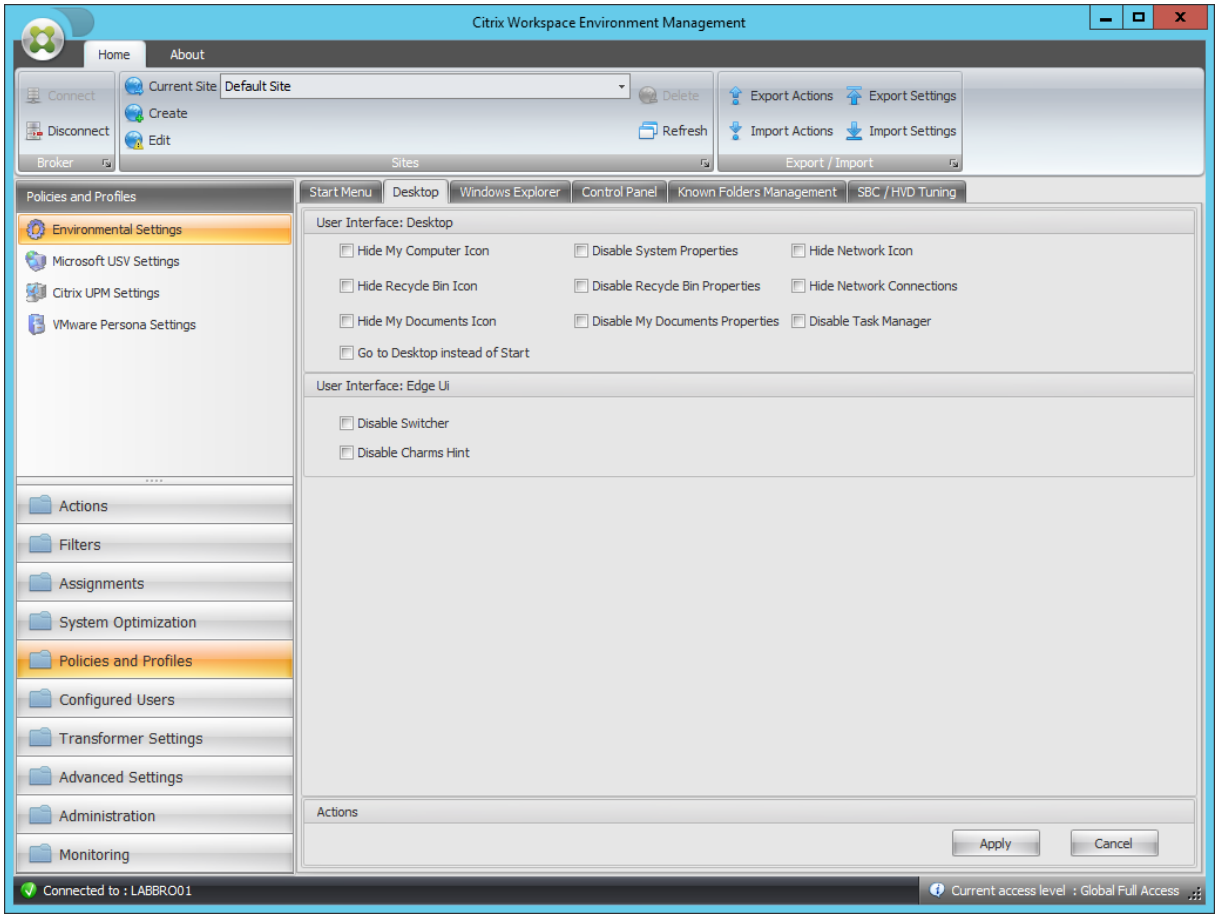
Set Background Color	
Parent Key	HKCU\Control Panel\Colors
Value Name	Background
Value Type	REG_SZ
Enabled Value	Configured color (R G B)
Disabled Value	Value does not exist or 0 0 0 if previously configured value
Processing	Service called by agent

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

Set Wallpaper	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	Wallpaper
Value Type	REG_SZ
Enabled Value	Path specified in console
Disabled Value	Value is absent
Processing	Service at logon

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Set Wallpaper	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	WallpaperStyle
Value Type	REG_SZ
Enabled Value	Depends on Style value
Disabled Value	Value is absent
Processing	Service at logon
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	TileWallpaper
Value Type	REG_SZ
Enabled Value	Depends on Style value
Disabled Value	Value is absent
Processing	Service at logon



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hide My Computer Icon	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	{20D04FE0-3AEA-1069-A2D8-08002B30309D}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Hide Recycle Bin Icon	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	{645FF040-5081-101B-9F08-00AA002F954E}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Hide My Documents Icon	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	{450D8FBA-AD25-11D0-98A8-0800361B1103}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Go to Desktop instead of Start	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\
Value Name	OpenAtLogon

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Go to Desktop instead of Start	
Value Type	DWORD
Enabled Value	0
Disabled Value	1
Processing	Service at logon

Disable System Properties	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoPropertiesMyComputer
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Disable Recycle Bin Properties	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoPropertiesRecycleBin
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Disable My Documents Properties	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoPropertiesMyDocuments
Value Type	DWORD
Enabled Value	1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Disable My Documents Properties	
Disabled Value	0
Processing	Service called by agent

Hide Network Icon	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Hide Network Connections	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoNetworkConnections
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

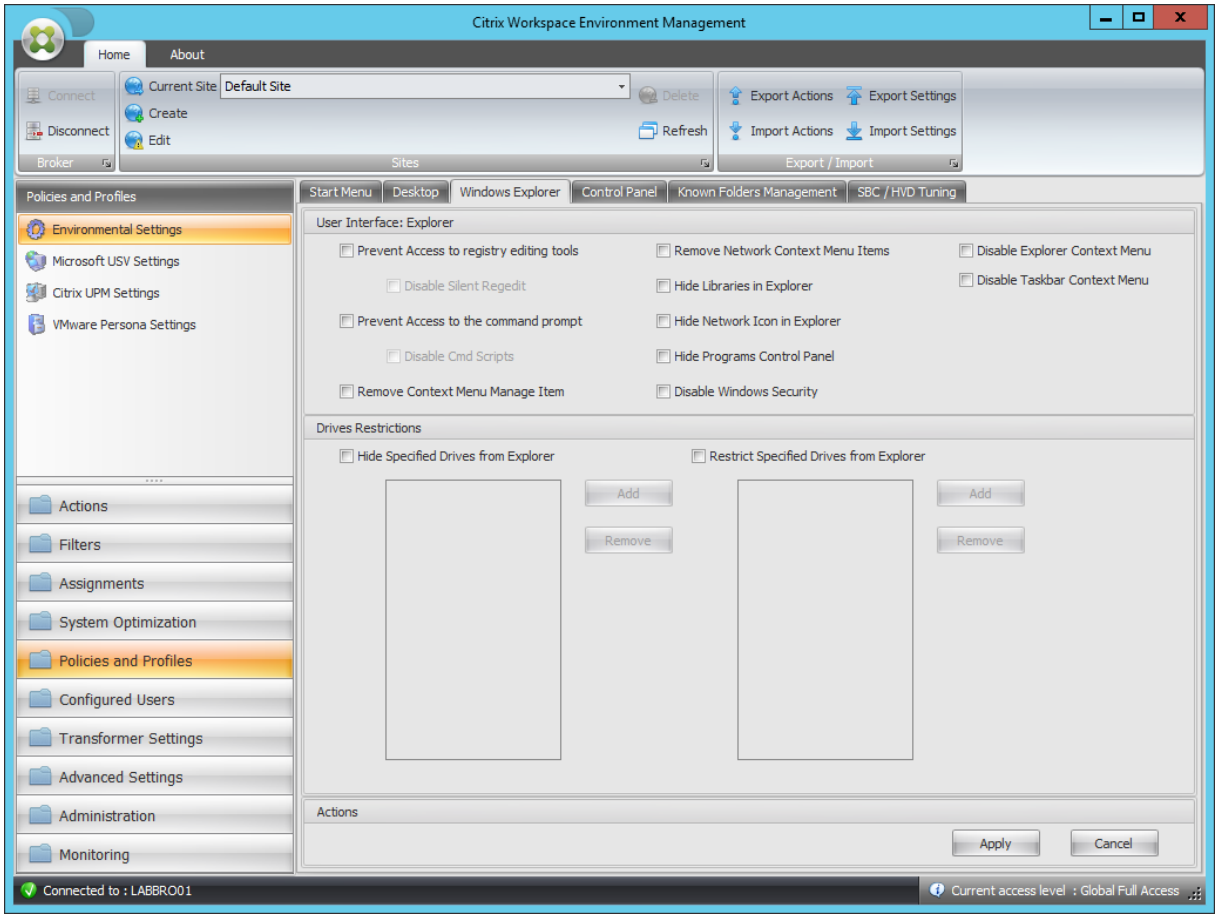
Disable Task Manager	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	DisableTaskMgr
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Disable Switcher	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Immersiv
Value Name	DisableTLcorner
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Disable Charm Hints	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Immersiv
Value Name	DisableCharmsHint
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Prevent Access to Registry Editing Tools

Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	DisableRegistryTools
Value Type	DWORD
Enabled Value	Disable Silent Regedit ? 2 : 1
Disabled Value	0
Processing	Service called by agent

Prevent Access to the Command Prompt

Parent Key	HKCU\Software\Policies\System
Value Name	DisableCMD
Value Type	DWORD

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Prevent Access to the Command Prompt	
Enabled Value	Disable Silent Cmd Scripts ? 2 : 1
Disabled Value	0
Processing	Service called by agent

Remove Context Menu Manage Item	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoManageMyComputerVerb
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Remove Network Context Menu Items	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoNetworkConnections
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Hide Libraries in Explorer	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	{031E4825-7B94-4dc3-B131-E946B44C8DD5}
Value Type	DWORD
Enabled Value	1
Disabled Value	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hide Libraries in Explorer	
Processing	Service at logon

Hide Network Icon in Explorer	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service at logon

Hide Programs Control Panel	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoProgramsCPL
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Disable Windows Security	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoNtSecurity
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Disable Explorer Context Menu	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoViewContextMenu
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

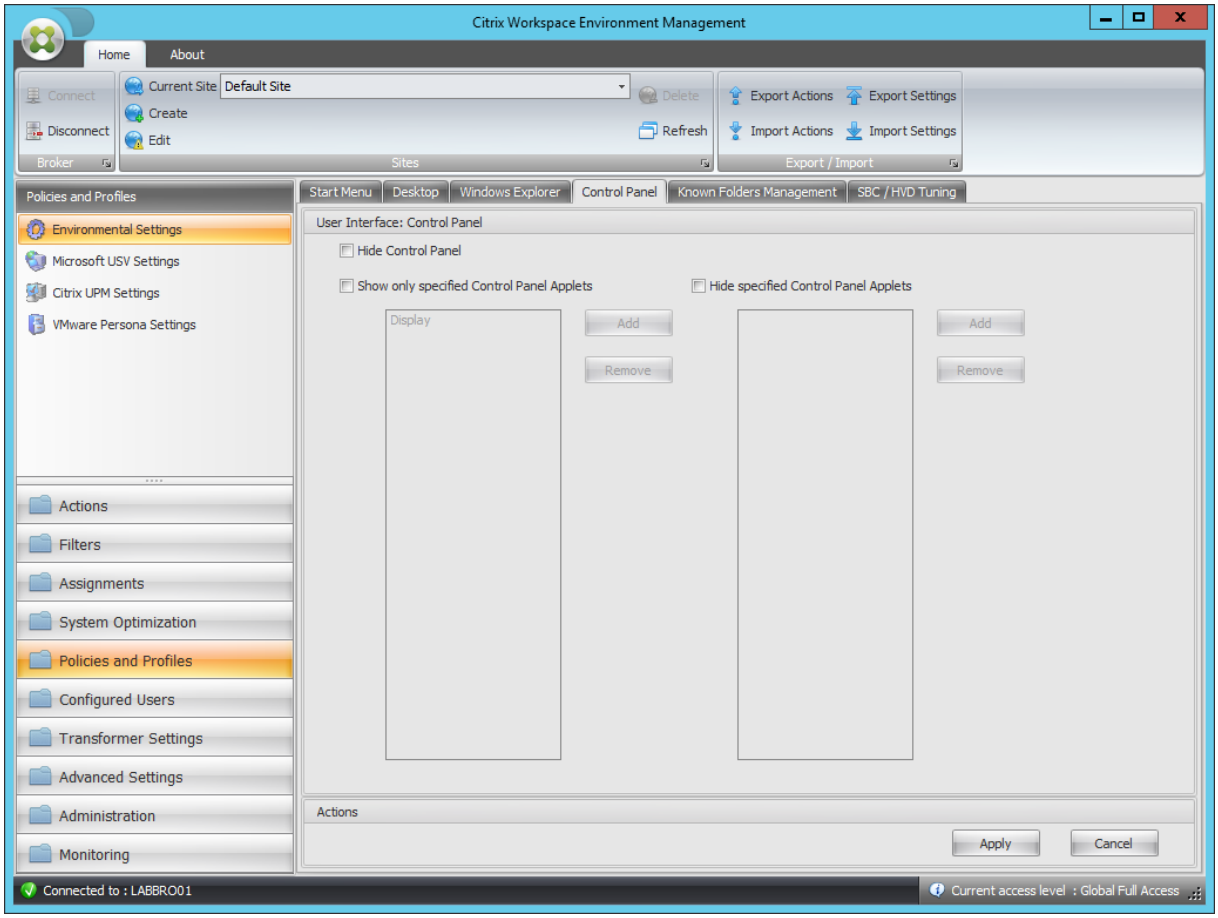
Disable Taskbar Context Menu	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoTrayContextMenu
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

Hide specified Drives from Explorer	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoDrives
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon

Restrict Specified Drives from Explorer	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoViewOnDrive

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Restrict Specified Drives from Explorer	
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon



Hide Control Panel	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	NoControlPanel
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hide Control Panel	

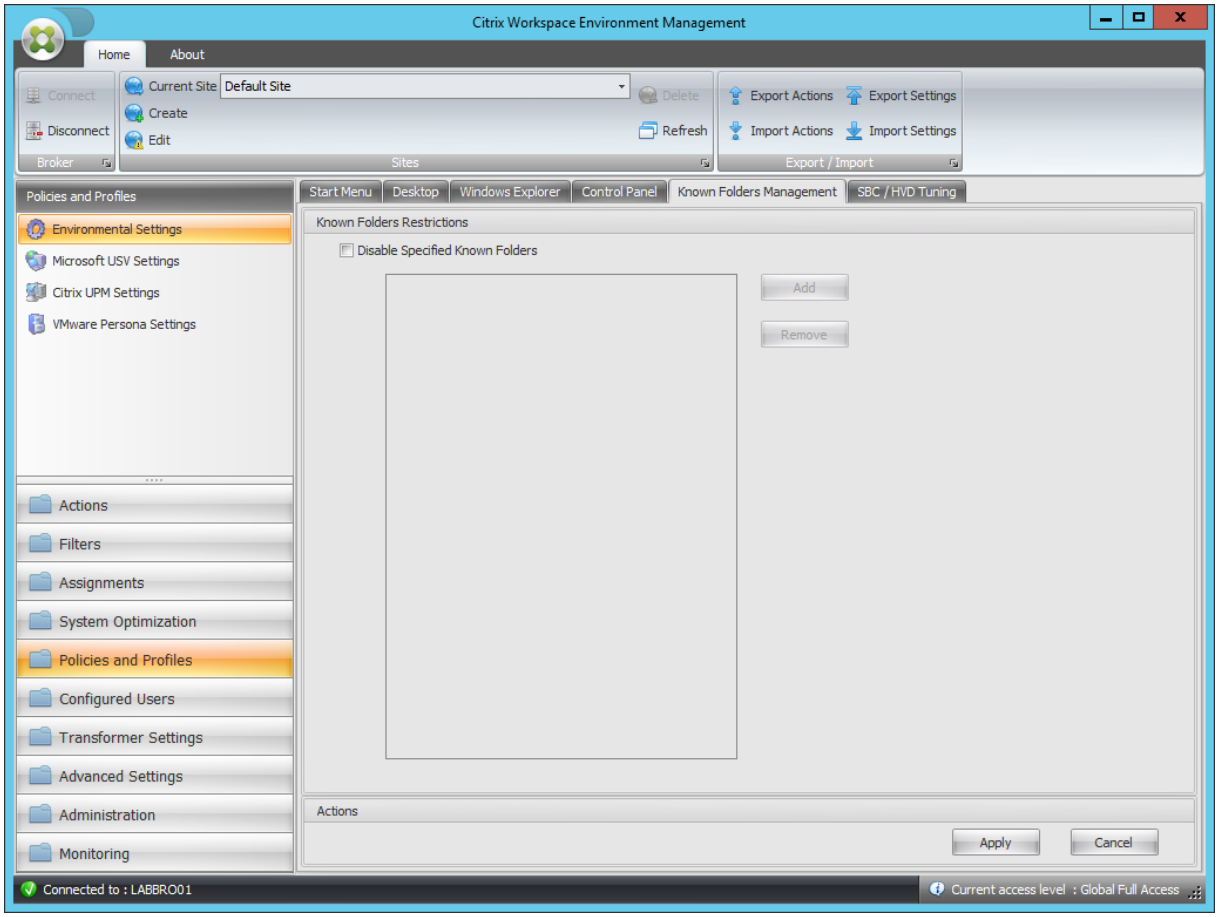
Show only specified Control Panel Applets	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Value Name	RestrictCpl
Value Type	DWORD
Enabled Value	1
Disabled Value	0
Processing	Service called by agent

For each allowed applet	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ RestrictCpl
Value Name	Applet index (starting at 1 and automatically incremented)
Value Type	REG_SZ
Enabled Value	AppletName
Disabled Value	Null / Removed
Processing	Service called by agent

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For each disallowed applet	
Parent Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\DisallowCpl
Value Name	Applet index (starting at 1 and automatically incremented)
Value Type	REG_SZ
Enabled Value	AppletName
Disabled Value	Null / Removed
Processing	Service called by agent



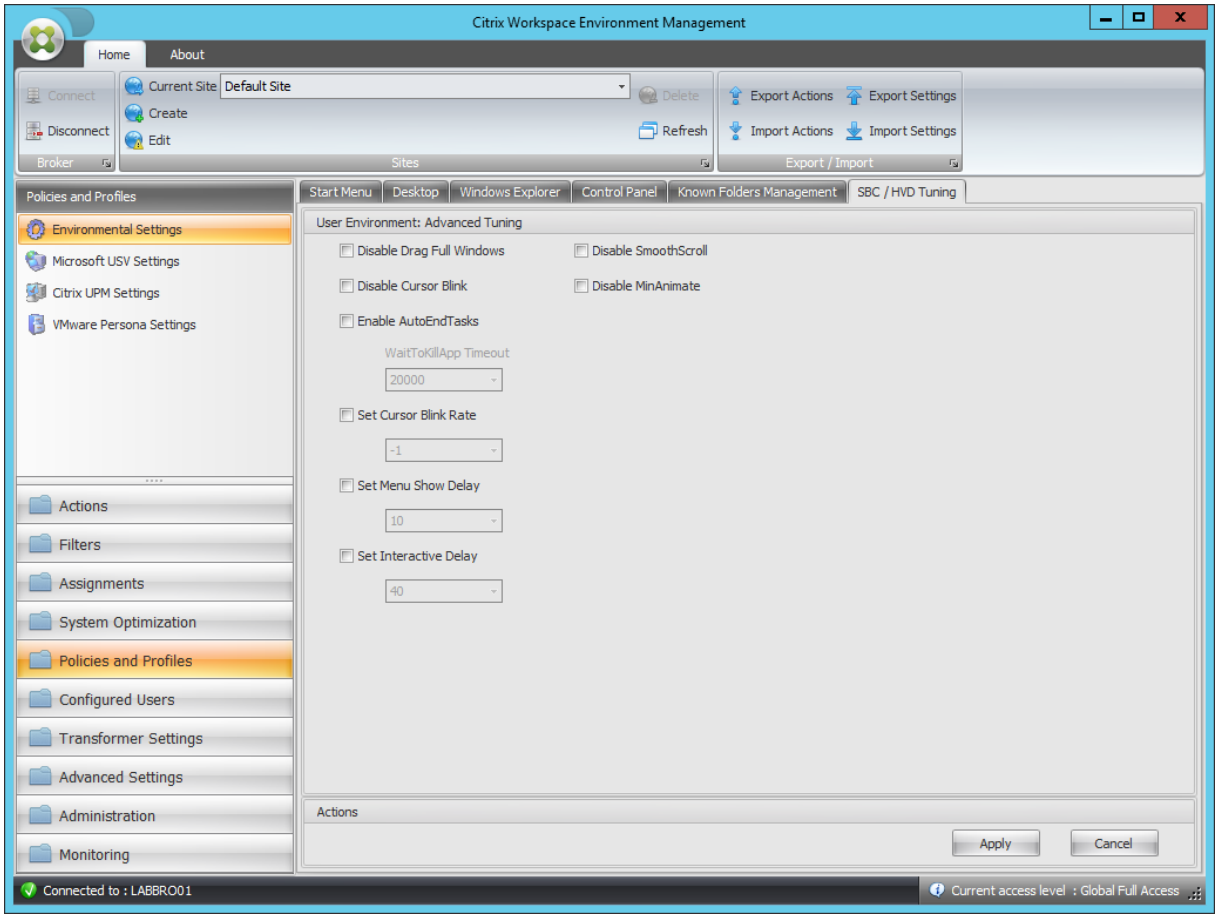
Disable Specified Known Folders	
Parent Key	HKCU\Software\Policies\Microsoft\Windows\Explorer
Value Name	DisableKnownFolders

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Disable Specified Known Folders	
Value Type	DWORD
Enabled Value	Value depends on selected drive letters
Disabled Value	Null (value should be removed)
Processing	Service at logon

For each disabled folder	
Parent Key	HKCU\Software\Policies\Microsoft\Windows\Explorer\DisableKnownFolders
Value Name	Disabled folder name
Value Type	REG_SZ
Enabled Value	Disabled folder name
Disabled Value	Null / Removed
Processing	Service at logon

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Disable Drag Full Windows

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

Disable Cursor Blink

Parent Key	HKCU\Control Panel\Desktop
Value Name	DisableCursorBlink
Value Type	DWORD

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Disable Cursor Blink	
Enabled Value	1
Disabled Value	0
Processing	Service at logon

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Set Cursor Blink Rate	
Processing	Service at logon

Set Menu Show Delay	
Parent Key	HKCU\Control Panel\Desktop
Value Name	MenuShowDelay
Value Type	DWORD
Enabled Value	Configured value
Disabled Value	400 (decimal)
Processing	Service at logon

Set Interactive Delay	
Parent Key	HKCU\Control Panel\Desktop
Value Name	InteractiveDelay
Value Type	DWORD
Enabled Value	Configured value
Disabled Value	Null / Removed
Processing	Service at logon

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Filter conditions

December 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Condition Name	**ComputerName Match**
Expected value type	N/A
Expected result type	String.
Expected syntax	Single name test: Computername Multiple tests (OR): Computername1;Computername2 Wildcard (also works with multiples): ComputerName*
Returns	True if the current computer name matches the tested value, false otherwise.

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Condition Name	**Client IP Address Match**
Expected result type	IP address.
Expected syntax	Single name test: ClientIpAddress Multiple tests (OR): ClientIpAddress1;ClientIpAddress2 Wildcard (also works with multiples): ClientIpAddress* Range (also works with multiples): IpAddress1-IpAddress2
Returns	True if the current client IP address matches the tested value, false otherwise.

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Condition Name	**User UI Language Match**
Returns	True if user UI ISO language name matches the specified value, false otherwise.

Condition Name	**User SBC Resource Type**
Expected value type	N/A
Expected result type	Select from list.
Expected syntax	N/A
Returns	True if user context (published desktop or application) matches the selected value, false otherwise.

Condition Name	**OS Platform Type**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if machine platform type (x64 or x86) matches the selected value, false otherwise.

Condition Name	**Connection State**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if connection state (online or offline) matches the selected value, false otherwise.

Condition Name	**Citrix Virtual Apps Version Match**
Expected value type	N/A
Expected result type	String. Citrix Virtual Apps Version. Example: 6.5

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Condition Name	**Citrix Virtual Apps Version Match**
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
Returns	True if name matches the selected value, false otherwise.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 input value is found in the name/value pairs in the specified list, false otherwise.

Condition Name	**No ComputerName Match**
Negative condition behavior	Runs **ComputerName Match** and returns the opposite result (true if false, false if true). See condition **ComputerName Match** for more information.

Condition Name	**No ClientName Match**
Negative condition behavior	Runs ClientName Match and returns the opposite result (true if false, false if true). See condition **ClientName Match** for more information.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Condition Name	**Name or Value is not in List**
Negative condition behavior	Runs Name or Value is in List and returns the opposite result (true if false, false if true). See condition **Name or Value is in List** for more information.

Condition Name	**Client Remote OS Match**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current remote client operating system matches selected value, false otherwise.

Condition Name	**No Client Remote OS Match**
Negative condition behavior	Runs Client Remote OS Match and returns the opposite result (true if false, false if true). See condition **Client Remote OS Match** for more information.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Condition Name	**No Dynamic Value Match**
Negative condition behavior	Runs Dynamic Value Match and returns the opposite result (true if false, false if true). See condition **Dynamic Value Match** for more information.

Condition Name	**Transformer Mode State**
Expected value type	N/A
Expected result type	Select from dropbox.
Expected syntax	N/A
Returns	True if current Transformer state matches selected value, false otherwise.

Condition Name	**No Client OS Match**
Negative condition behavior	Runs Client OS Match and returns the opposite result (true if false, false if true). See condition **Client OS Match** for more information.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Condition Name	**No Active Directory Group Match**
Negative condition behavior	Runs Active Directory Group Match and returns the opposite result (true if false, false if true). See condition **Active Directory Group Match** for more information.

Condition Name	**File Version Match**
Expected value type	String. Full path and name of the file to test. Example: **C:\Test\TestFile.dll**
Expected result type	String. Expected file version value of the tested file.
Expected syntax	Single name test: value Not null test: ?
Returns	True if registry value exists and value matches, false otherwise.

Condition Name	**No File Version Match**
Negative condition behavior	Runs File Version Match and returns the opposite result (true if false, false if true). See condition **File Version Match** for more information.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> the **Matching Result** field. If the published resource is a published desktop, type the published name of the desktop in the **Matching Result** field.

Condition Name	**Published Resource Name**
Expected value type	N/A
Expected result type	String. Name of the published resource (Citrix Virtual Apps/Citrix Virtual Desktops/RDS).
Expected syntax	Single name test: published resource name Multiple tests (OR): Name1;Name2 Wildcard test: Name*
Returns	True if the current published resource name matches the tested value, false otherwise.

Condition Name	**Name is in List**
Expected value type	String. Full file path of the XML list generated by the Integrity List manager utility.
Expected result type	String. Expected value of the name to look for in the list.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Condition Name	**File/Folder exists**
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.

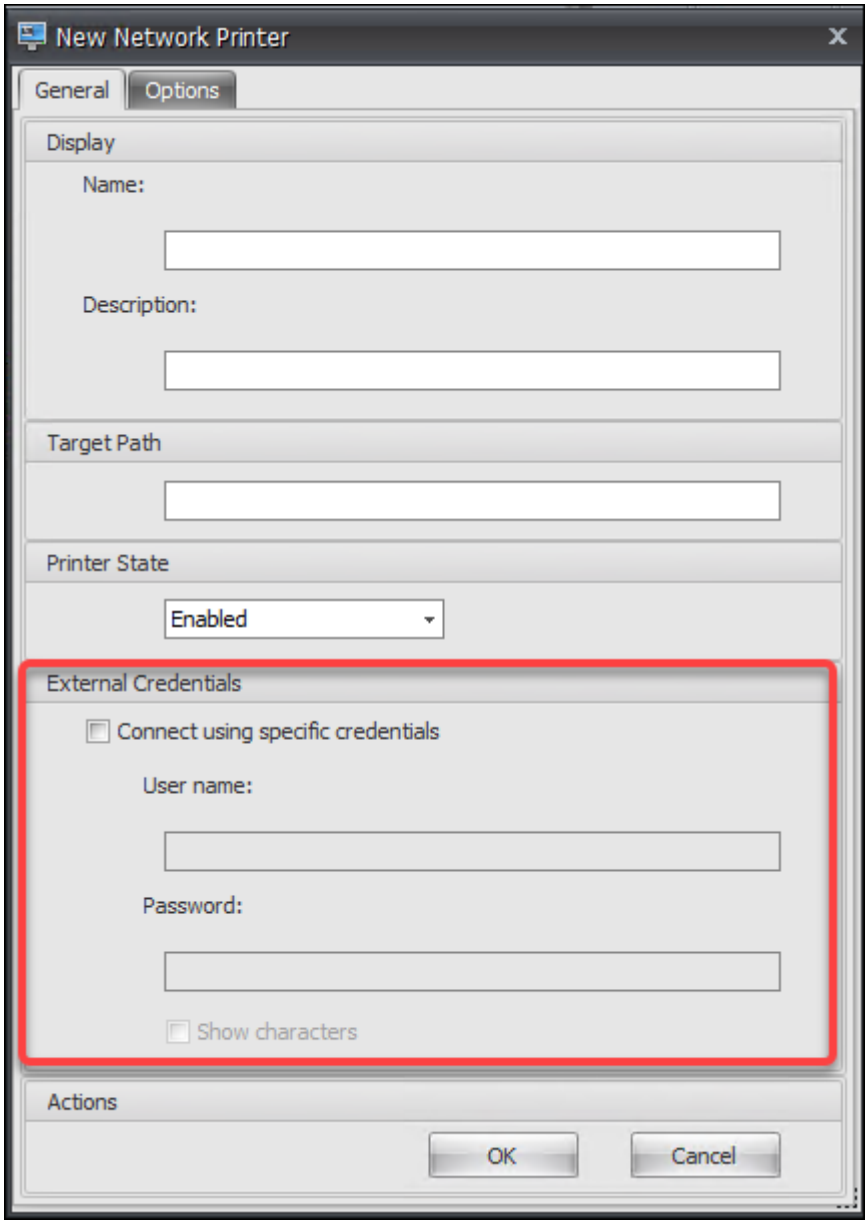
FIPS support

December 6, 2022

You can run Workspace Environment Management (WEM) in a FIPS environment. The following configurations in WEM relate to FIPS:

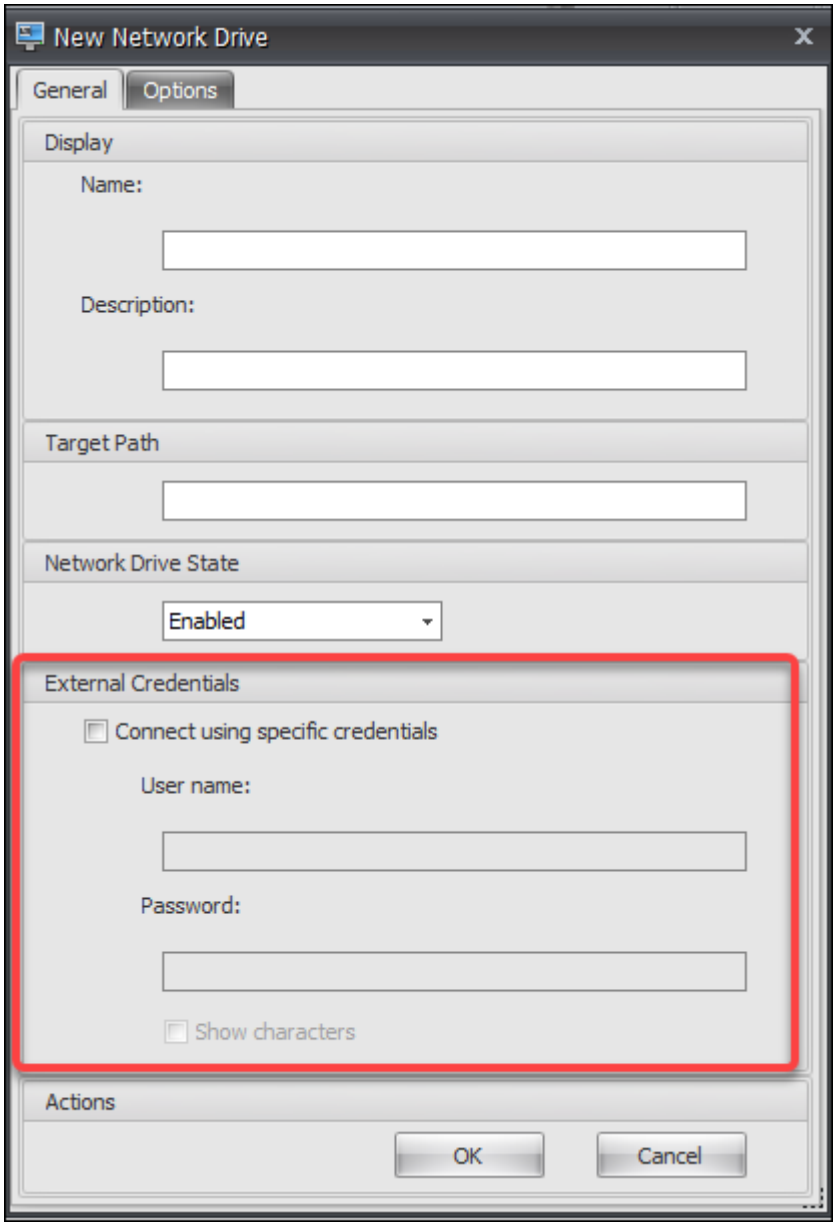
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Printer credentials in **Administration console > Actions > Printers**:



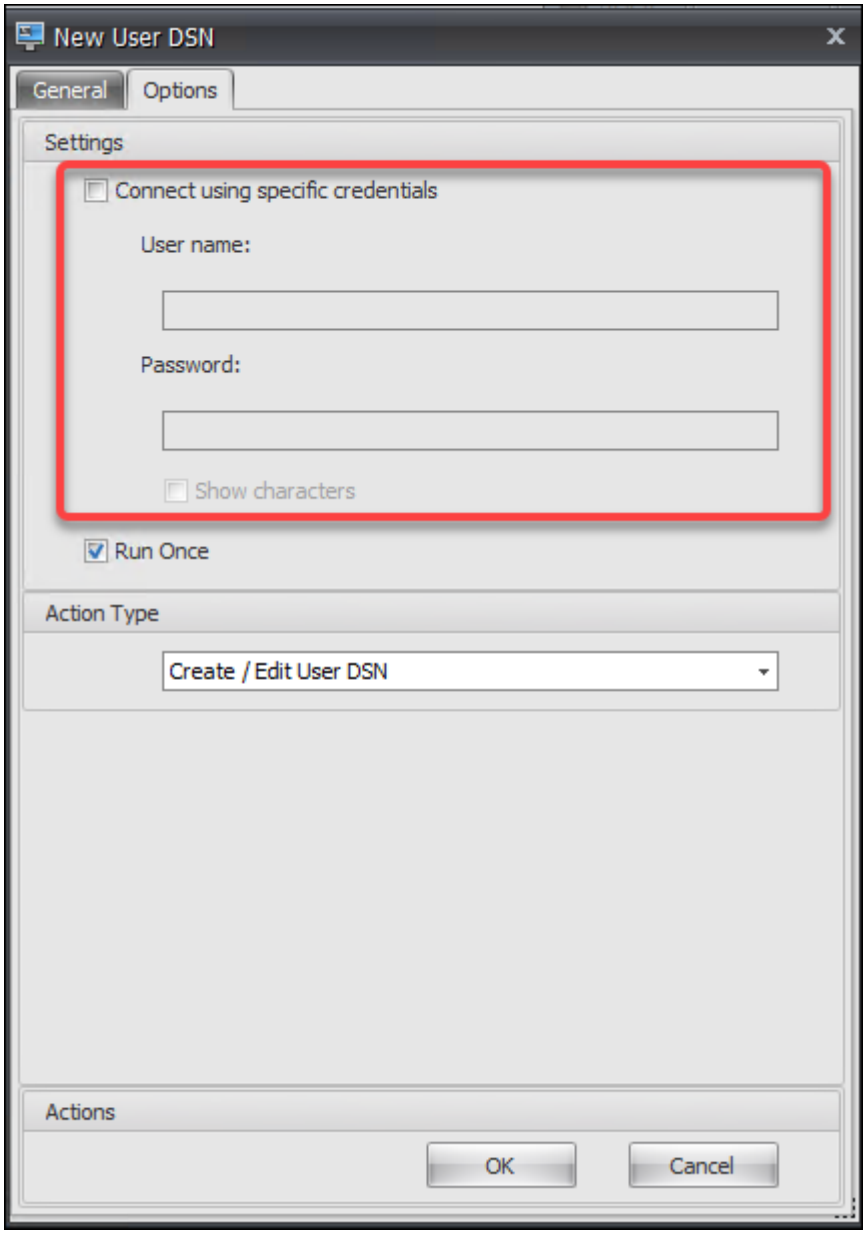
- Network drive credentials in **Administration console > Actions > Network Drives**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

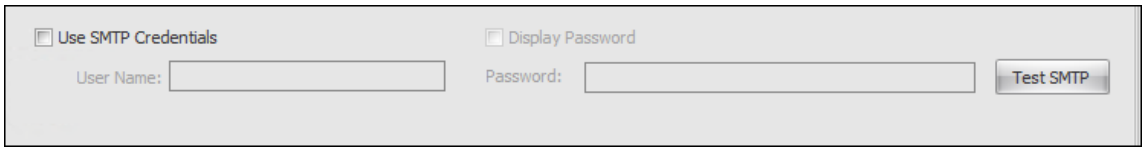


- User DSN credentials in **Administration console > Actions > User DSN**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

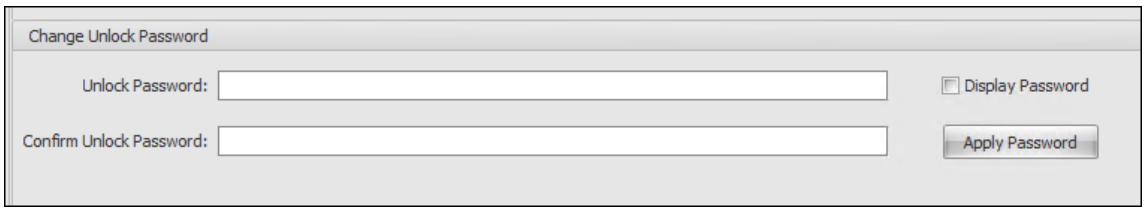


- SMTP credentials in **Administration console > Advanced Settings > UI Agent Personalization > Helpdesk Options**:

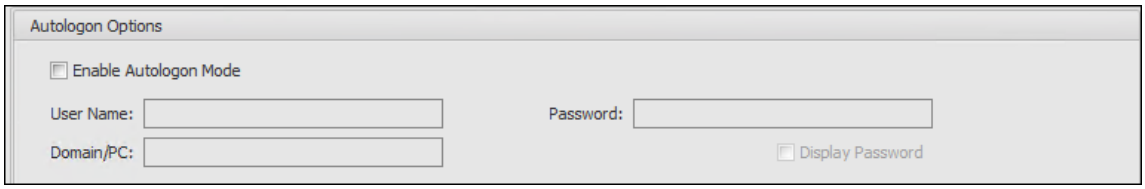


- Unlock password settings in **Administration console > Transformer Settings > General > General Settings**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Auto logon credentials in **Administration console > Transformer Settings > Advanced > Logon/Logoff & Power Settings**:



Be aware of the following consideration when running WEM in a FIPS environment.

- You cannot restore to your WEM environment the following items if they are exported from a WEM 2003 or earlier environment.
  - Actions (printers, network drives, user DSN) and action groups containing those actions
  - Settings (agent configuration settings and transformer settings)
  - Configuration sets

Upgrade considerations

If you want to run WEM in FIPS mode, be aware of the following considerations before upgrading the WEM infrastructure services and administration console:

- If you have *WEM 2006 or later* running in your environment, you can first upgrade to 2109 and then switch to FIPS mode or *the opposite way*.
- If you have *WEM 2003 or earlier* running in your environment, you must first upgrade to 2109 and then switch to FIPS mode.

Agent considerations

To run the WEM agent in a FIPS environment, make sure that the version of the agent is *2006 or later*.

Load balancing with Citrix ADC

December 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

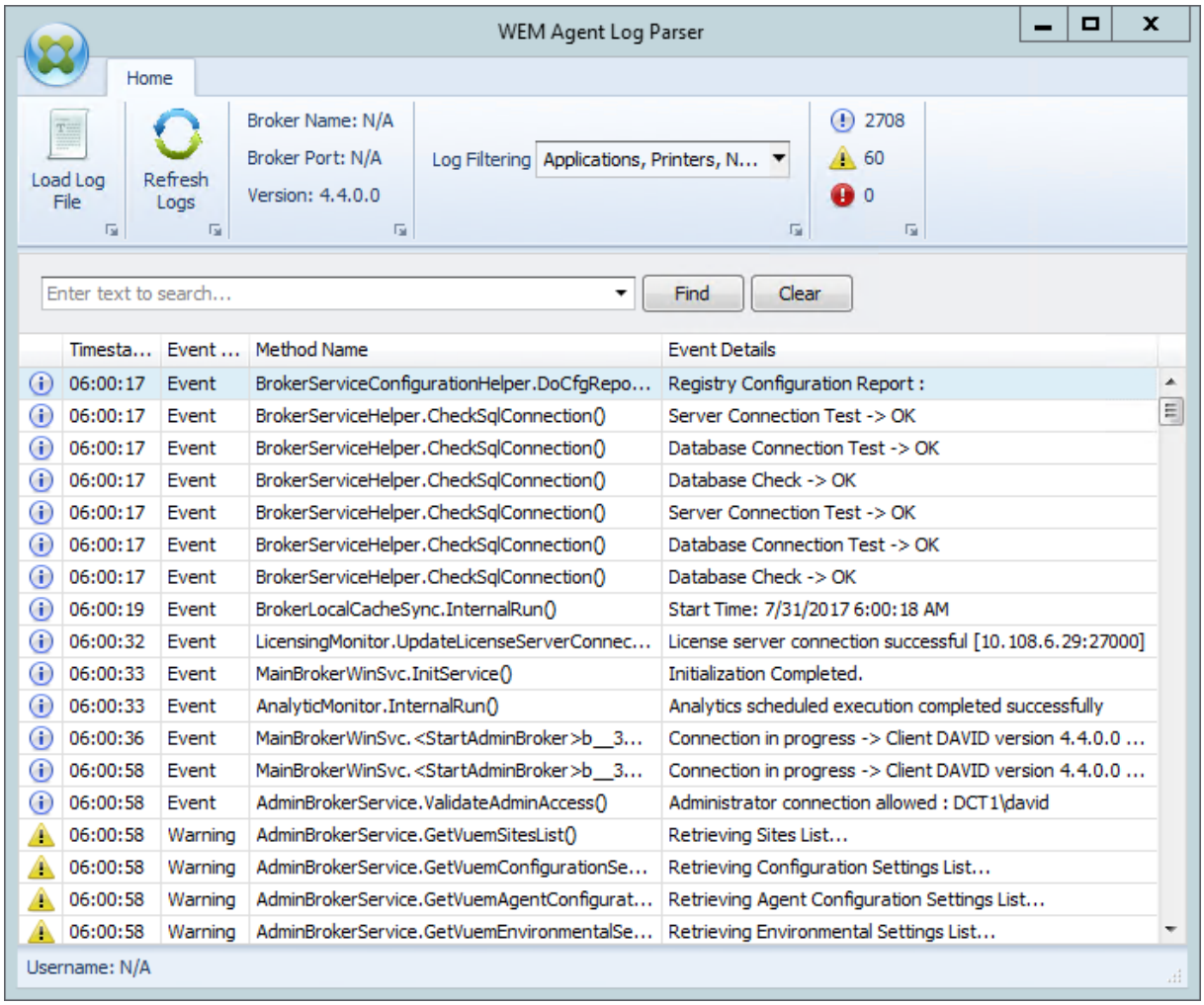
9. On the Service Group Binding page, click the right arrow, select the corresponding service group, and then click **Bind**.
10. Follow steps 7 through 9 to create virtual servers that listen on the agent service port and the cached data synchronization port.

    - **Port**. For the agent service port, type 8286. For the cached data synchronization port, type 8288.

Log parser

December 6, 2022

Workspace Environment Management includes a log parser application, which is located in the agent installation directory:



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Source	Destination	Type	Port	Details
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.

View log files

December 6, 2022

You can collect and view logs related to Workspace Environment Management (WEM). You use the logs to troubleshoot issues on your own or provide the logs when you contact Citrix Technical Support for assistance. You can collect logs related to:

- The WEM agent
- The WEM infrastructure service
- The WEM administration console
- The WEM database

Logs related to the agent

You can collect logs related to the WEM agent. Logs that you can collect on machines where the WEM agent is installed include:

- **WEM agent logs**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Citrix WEM Agent Init.log**. The initialization log that lets you troubleshoot issues with the agent in CMD or UI mode. The log is created on logon or on refresh. If the agent fails to start, view this log file for error details. Errors appear as *exceptions*. By default, this log file is created in the user's profile folder (%userprofile%).
- **Citrix WEM Agent.log**. The primary log that lets you troubleshoot issues with the agent in CMD or UI mode. The log lists what instructions the agent processed. If an action fails to be assigned to the current user, view this log file for error details. Errors appear as *exceptions*. By default, this log file is created in the user's profile folder (%userprofile%). To change the default, go to **Administration Console > Advanced Settings > Configuration > Agent Options** and then configure the **Enable Agent Logging** setting. To view more details, enable **Debug Mode** on the **Agent Options** tab. Alternatively, you can enable logging by configuring the following registry key:

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

  Name: AgentDebugModeLocalOverride

  Type: DWORD

  Value: 0

  Set the value to 1 to enable the log file and 0 to disable it. For the changes to take effect, restart the Citrix WEM Agent Host Service. By default, logging is disabled.

  > **Caution:**
  >
  > Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

- **Citrix WEM Agent Host Service Debug.log**. The log that lets you troubleshoot issues with the Citrix WEM Agent Host Service. By default, this log file is located in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Agent`. To enable logging, be sure to enable **Debug Mode** for the relevant configuration set on the **Administration Console > Advanced Settings > Configuration > Service Options** tab. Alternatively, you can enable logging by configuring the following registry key:

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

  Name: AgentServiceDebugModeLocalOverride

  Type: DWORD

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Value: 0

Set the value to 1 to enable the log file and 0 to disable it. For the changes to take effect, restart the Citrix WEM Agent Host Service. By default, logging is disabled.

> **Caution:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

- **Windows event logs**. Information written to the Windows Event Log. View logs in the **Event Viewer > Applications and Services Logs > WEM Agent Service** pane.
- **Windows Communication Foundation (WCF) traces**. Logs that are helpful when you encounter issues related to communications between the WEM agent and the WEM infrastructure service. To enable logging, you must enable WCF tracing. For more information, see Windows Communication Foundation traces.

Logs related to the infrastructure service

You can collect logs related to the WEM infrastructure service. Logs that you can collect on machines where the WEM infrastructure service is installed include:

- **Windows event logs**. Information written to the Windows Event Log. View logs in the **Event Viewer > Applications and Services Logs > Norskale Broker Service** pane.
- **Citrix WEM Infrastructure Service Debug.log**. The log that lets you troubleshoot issues with the Citrix WEM infrastructure service (Norskale Broker Service.exe). By default, this log file is located in `%PROGRAMFILES(X86)%\ Norskale\Norskale Infrastructure Services`. To enable this log file, follow these steps to enable debug mode:

  1. Open the **WEM Infrastructure Service Configuration Utility** from the Start menu.
  2. On the **Advanced Settings** tab, select **Enable debug mode**.
  3. Click **Save Configuration** and click **Yes** to start the service to apply the change.
  4. Close the **WEM Infrastructure Service Configuration Utility** window.

- **WCF traces**. Logs that are helpful when you encounter communication issues related to the WEM infrastructure service. To enable logging, you must enable WCF tracing. For more information, see Windows Communication Foundation traces.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Logs related to the administration console

You can collect logs related to the WEM administration console. Logs that you can collect on machines where the administration console is installed include:

- **Citrix WEM Console Trace.log**. The log that lets you troubleshoot issues with the WEM administration console. By default, this log file is created in the user's profile folder (%userprofile%). To enable logging, follow these steps to enable debug mode:

  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**.
  3. On the **About** tab, click **Options** and select **Enable Debug Mode**.
  4. Click **Apply** to apply the change.

- **WCF traces**. Logs that are helpful when you encounter issues related to communications between the WEM administration console and the WEM database. To enable logging, you must enable WCF tracing. For more information, see Windows Communication Foundation traces.

Logs related to the WEM database

You can collect logs related to the WEM database. Logs are created when you use the WEM database management utility to create or upgrade a database. View the following log file for details:

- **Citrix WEM Database Management Utility Debug Log.log**. The log that lets you troubleshoot issues with the WEM database. This log file is created by default and is located in `C:\Program Files (x86)\Norskale\Norskale Infrastructure Services`.

Windows Communication Foundation traces

You can view Windows Communication Foundation (WCF) traces to help you troubleshoot the following issues:

- Communications between the agent and the infrastructure service
- Communications related to the WEM infrastructure service
- Communications related to the WEM administration console

Troubleshoot communications between the agent and the infrastructure service

If the WEM agent does not communicate properly with the WEM infrastructure service, you can view WCF traces of the VUEMUIAgent.exe service. Follow these steps to enable WCF tracing:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Log on to the WEM agent machine.
2. Right-click the agent icon in the taskbar and then select **Exit** to close the agent.
3. Locate the VUEMUIAgent.exe.config file in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Agent` and then create a backup copy of the file.
4. Open the file in Notepad or WordPad and insert the following snippet into the section between the `<configuration>` and the `</configSections>` marker.
5. Save the file.

```
<system.diagnostics>
    <sources>
            <source name="System.ServiceModel"
                    switchValue="Information, ActivityTracing"
                    propagateActivity="true">
            <listeners>
            <add name="traceListener"
                type="System.Diagnostics.XmlWriterTraceListener"
                initializeData= "c:\trace\vuemUIAgent-Traces.
                    svclog" />
            </listeners>
        </source>
    </sources>
</system.diagnostics>
<!--NeedCopy-->
```

6. On the agent machine, create a root folder called “Trace”on the C drive (C:\Trace). Skip this step if the folder already exists.
7. Reproduce the issue you encountered and then end the VUEMUIAgent.exe process.
8. View the log file named `vuemUIAgent-Traces.svclog` in `C:\Trace`.

You can also view WCF traces of the Citrix.Wem.Agent.Service.exe service. Follow these steps:

1. Log on to the WEM agent machine.
2. Right-click the agent icon in the taskbar and then select **Exit** to close the agent.
3. End the Citrix WEM Agent Host Service.
4. Locate the Citrix.Wem.Agent.Service.exe.config file in `%PROGRAMFILES(X86)%\Citrix\Workspace Environment Management Agent` and then create a backup copy of the file.
5. Open the file in Notepad or WordPad and insert the following snippet into the file, starting on the fourth line right after the `</configSections>` marker.
6. Save the file.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<system.diagnostics>
    <sources>
            <source name="System.ServiceModel"
                    switchValue="Information, ActivityTracing"
                    propagateActivity="true">
            <listeners>
            <add name="traceListener"
                type="System.Diagnostics.XmlWriterTraceListener"
                initializeData= "c:\trace\NorskaleAgentHostService
                   -Traces.svclog" />
            </listeners>
        </source>
    </sources>
</system.diagnostics>
<!--NeedCopy-->
```

7. On the agent machine, create a root folder called "Trace"on the C drive (C:\Trace). Skip this step if the folder already exists.
8. Start the Windows service called Citrix WEM Agent Host Service and then reproduce the issue you encountered.
9. View the log file named `NorskaleAgentHostService-Traces.svclog` in `C:\Trace`.

Troubleshoot communications related to the WEM infrastructure service

If you encounter communication issues related to the WEM infrastructure service, you can view WCF traces of the Norskale Broker Service. Follow these steps to enable WCF tracing:

1. Log on to the machine where the WEM infrastructure service is installed.
2. End the Norskale Infrastructure Service.
3. Locate the Norskale Broker Service.exe.config file in `%PROGRAMFILES(X86)%\Norskale\Norskale Infrastructure Services` and then create a backup copy of the file.
4. Open the file in Notepad or WordPad and insert the following snippet into the file, starting on the third line right after the `<configuration>` marker.

```
<system.diagnostics>
    <sources>
            <source name="System.ServiceModel"
                    switchValue="Information, ActivityTracing"
                    propagateActivity="true">
            <listeners>
            <add name="traceListener"
                type="System.Diagnostics.XmlWriterTraceListener"
                initializeData= "c:\trace\
                   NorskaleInfrastructureBrokerService-Traces.
                   svclog" />
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
            </listeners>
        </source>
    </sources>
</system.diagnostics>
<!--NeedCopy-->
```

5. Save the file.
6. On the WEM infrastructure service machine, create a root folder called “Trace”on the C drive (C:\Trace). Skip this step if the folder already exists.
7. Start the Norskale Infrastructure Service and then reproduce the issue you encountered.
8. View the log file named `NorskaleInfrastructureBrokerService-Traces.svclog` in `C:\Trace`.

Troubleshoot communications between the WEM administration console and the WEM database

If you encounter issues related to communications between WEM administration console and the WEM database, you can view WCF traces of Norskale Administration Console.exe service. Follow these steps to enable WCF tracing:

1. Log on to the WEM administration console machine.
2. Close the WEM administration console.
3. Locate the Norskale Administration Console.exe.config file in `%PROGRAMFILES(X86)%\Norskale\Norskale Administration Console` and then create a backup copy of the file.
4. Open the file in Notepad or WordPad and add the following snippet into the file, starting on the third line right after the `<configuration>` marker.

```
<system.diagnostics>
    <sources>
            <source name="System.ServiceModel"
                    switchValue="Information, ActivityTracing"
                    propagateActivity="true">
            <listeners>
            <add name="traceListener"
                type="System.Diagnostics.XmlWriterTraceListener"
                initializeData= "c:\trace\WEMConsole-Traces.svclog
                    " />
            </listeners>
        </source>
    </sources>
</system.diagnostics>
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Save the file.
6. On the administration console machine, create a root folder called "Trace"on the C drive (C:\Trace). Skip this step if the folder already exists.
7. Open the WEM administration console and then reproduce the issue you encountered.
8. View the log file named `WEMConsole-Traces.svclog` in `C:\Trace`.

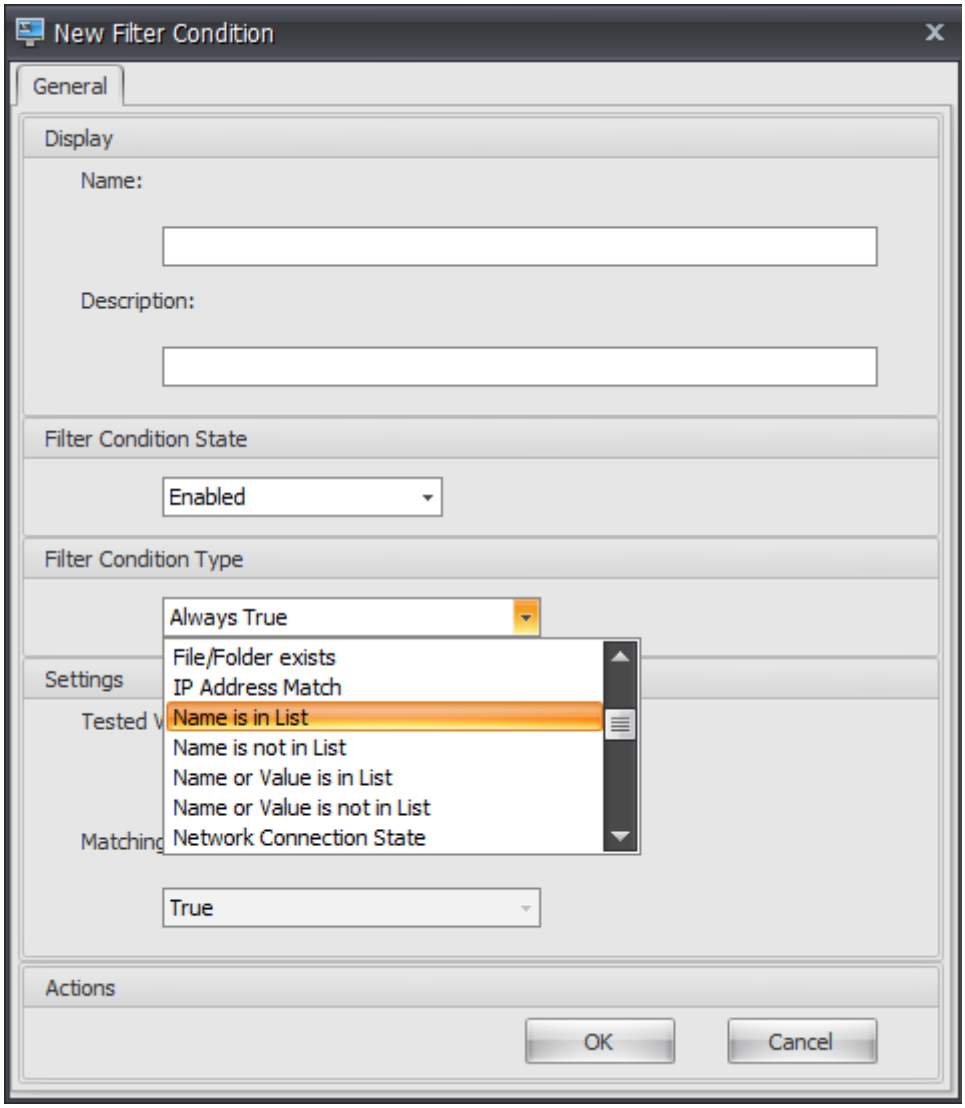
WEM Integrity Condition List Manager

December 6, 2022

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.

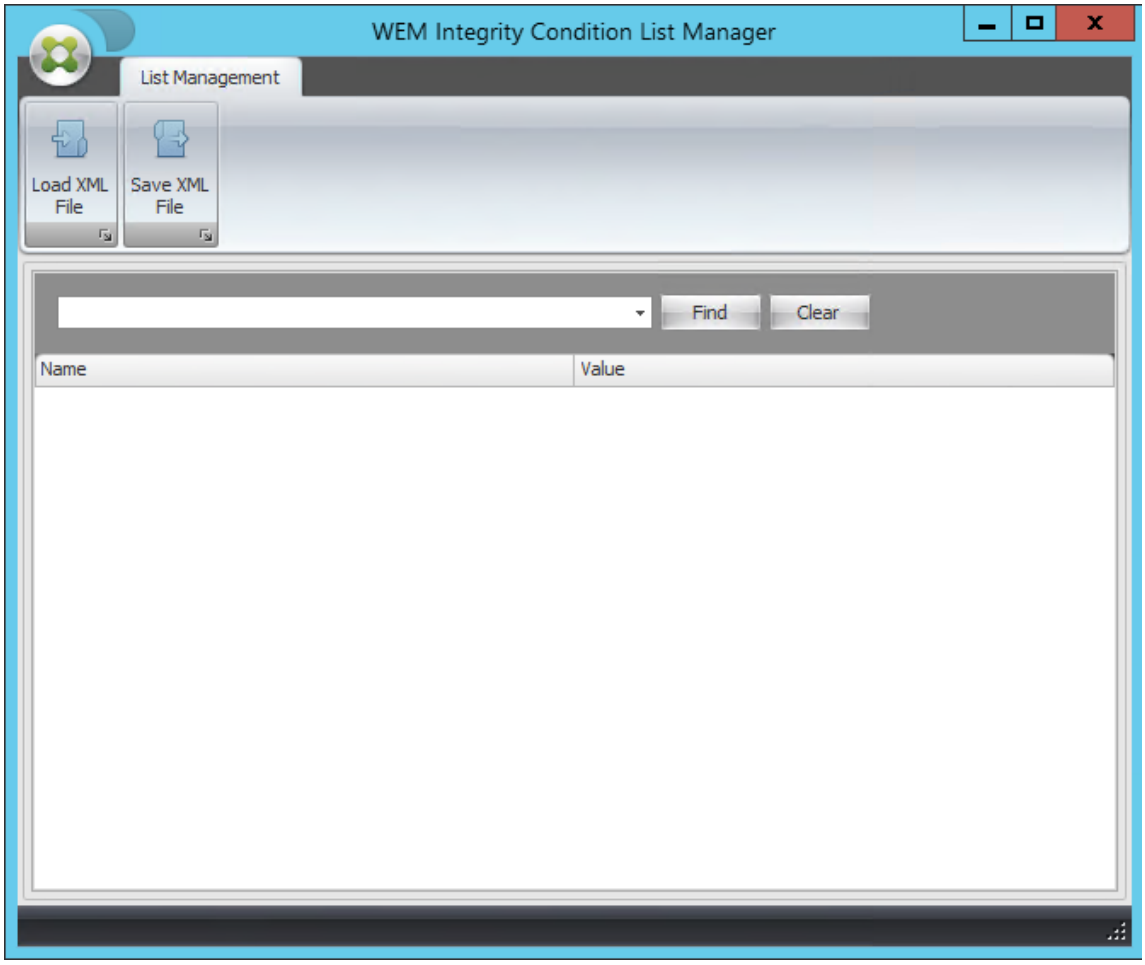
This article describes how to use the WEM Integrity Condition List Manager to create the XML file for filtering purposes. For example, suppose you want to filter the actions by using the WEM Integrity Condition List Manager in conjunction with **Name is in List**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Open WEM Integrity Condition List Manager.

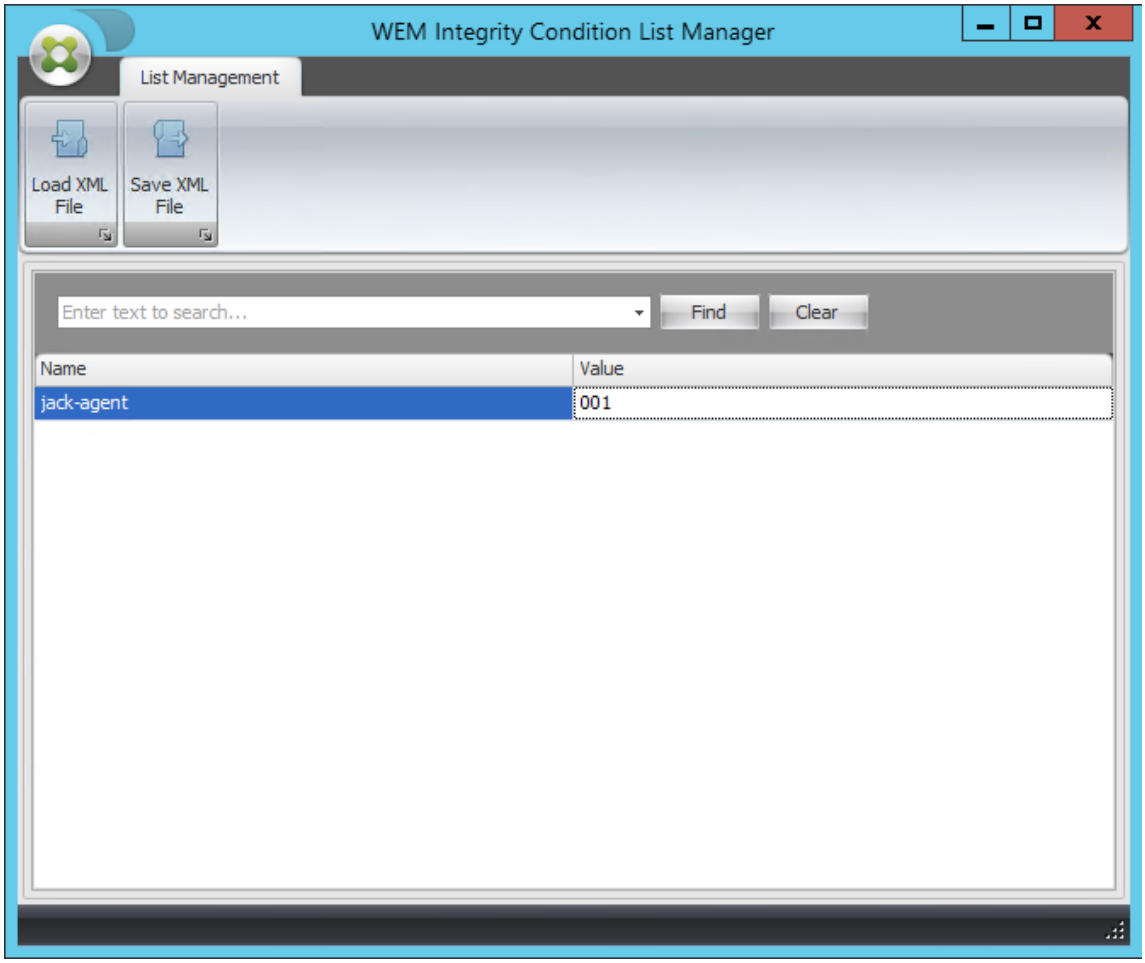
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



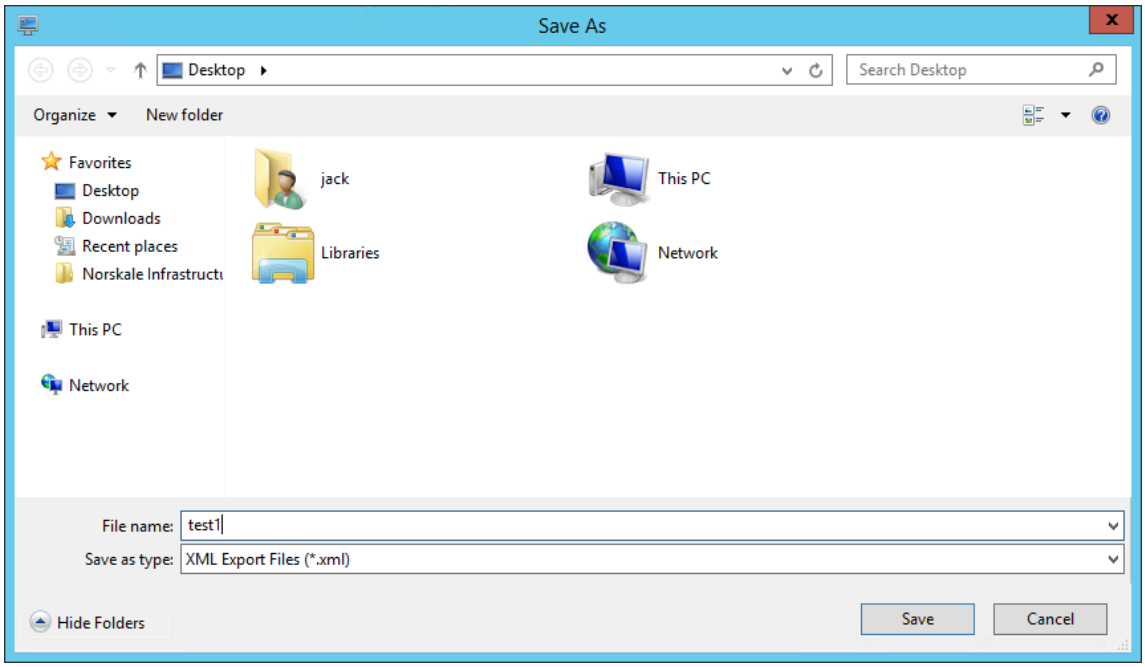
2. Right-click the blank area and then select **Add** in the context menu.
3. Type the name in the **Name** field.

> **Note:**
>
> Type the name of the machine on which the WEM agent is running (agent host).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

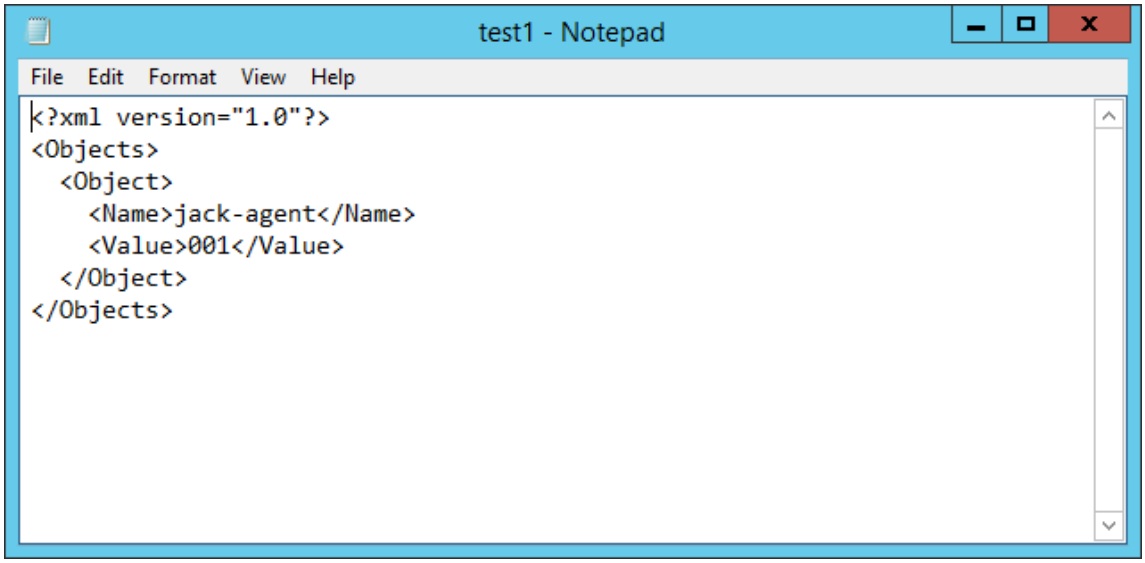


4. Click **Save XML File**, browse to the desired folder, and then click **Save**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Open the saved XML file to verify that the information you provided was saved correctly.

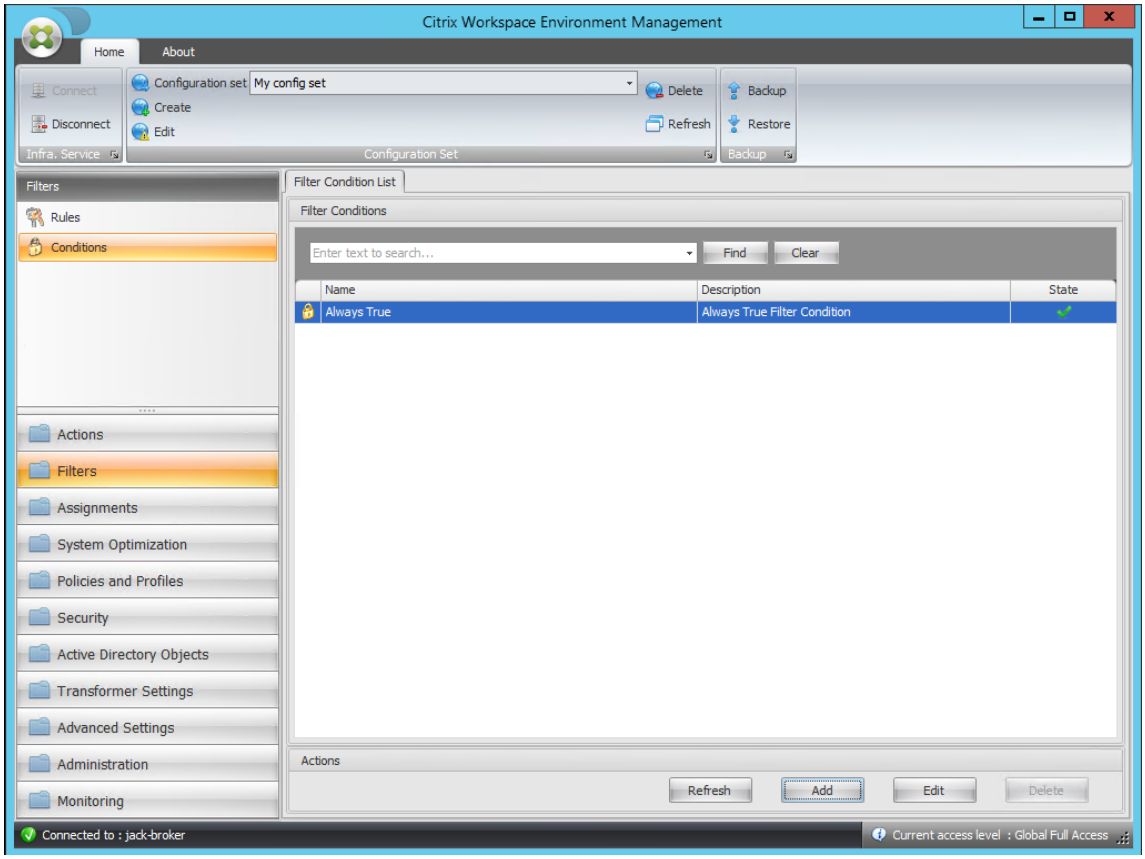


6. Copy the saved XML file to a folder on the agent host.

> **Note:**
>
> This feature does not work if you save the XML file on an administration console machine.

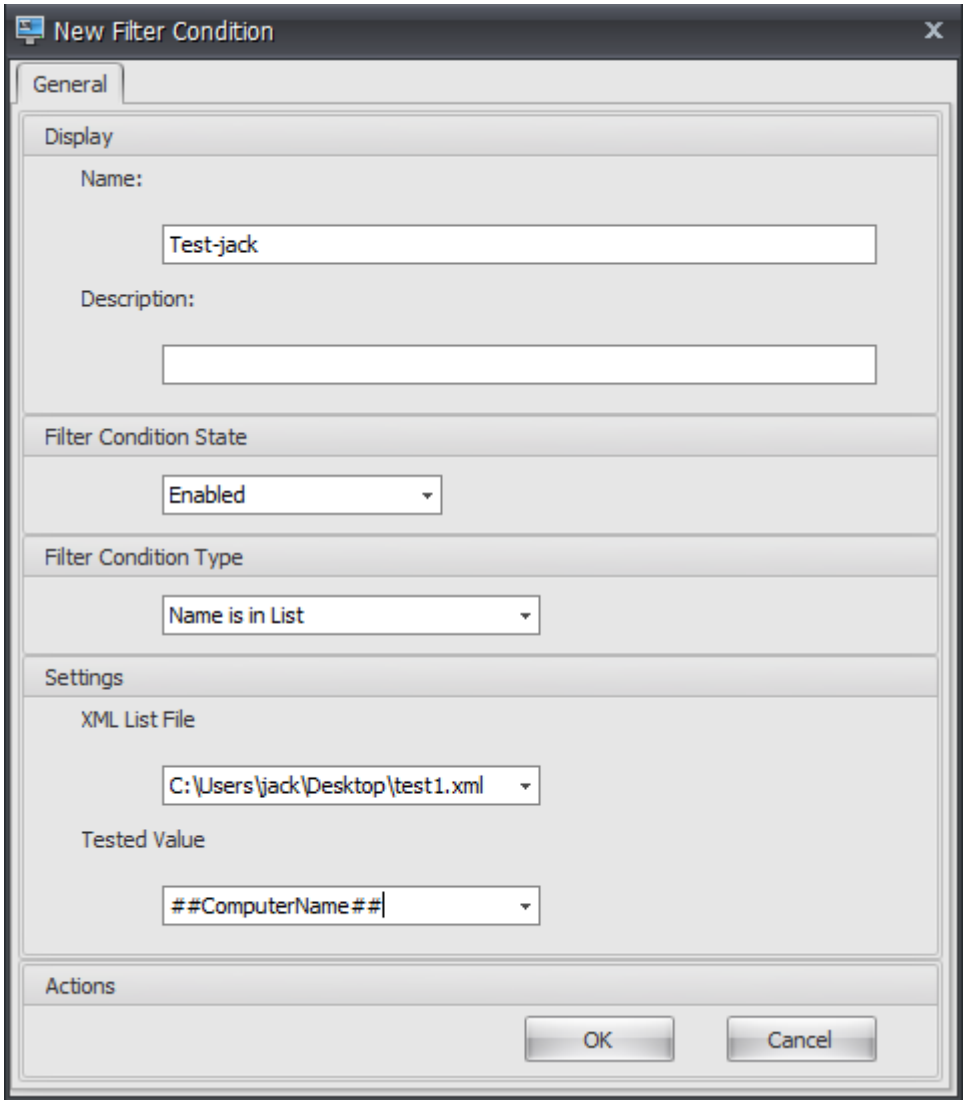
7. Go to the **Administration Console > Filters > Conditions > Filter Condition List** tab and then click **Add**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Type the information and then click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

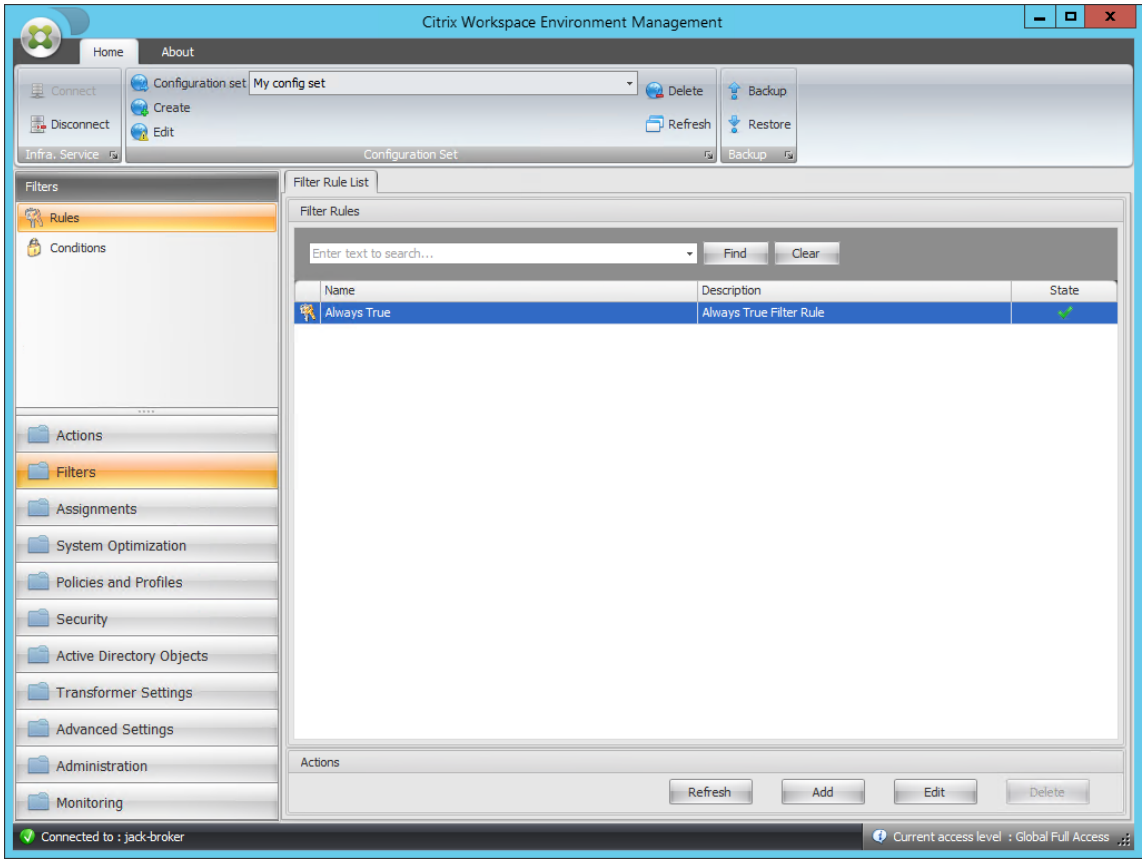


Note:

- **Filter Condition Type**. Select **Name is in List**.
- **XML List File**: C:\Users\<user1>\Desktop\test1.xml (file address on the agent host)
- **Tested Value**. Type the dynamic token that corresponds to the name you typed in the **Name** field in the WEM Integrity Condition List Manager. In this example, you typed the name of the machine on which the agent is running (agent host). Therefore, you must use the dynamic token "##ComputerName##."For more information about using dynamic tokens, see Dynamic tokens.

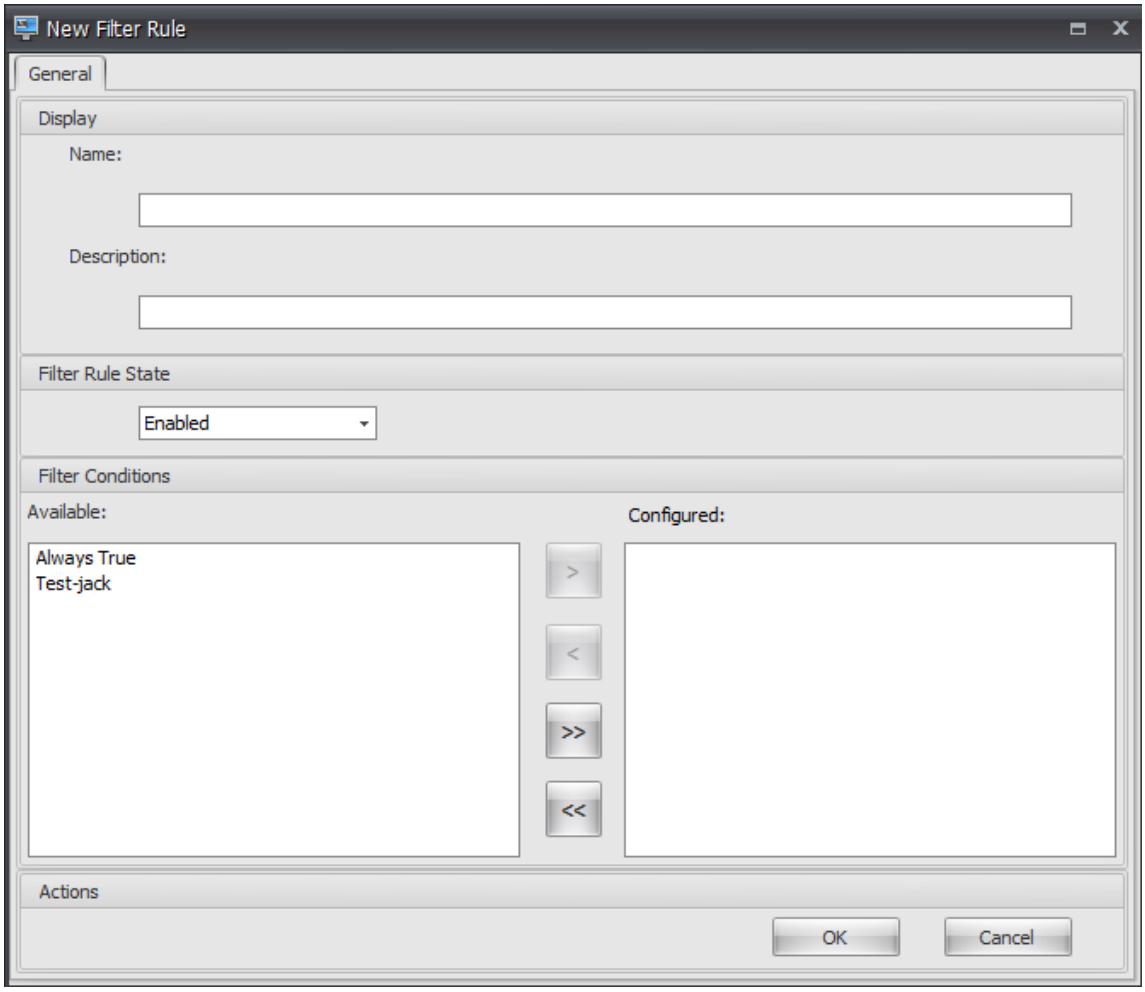
9. Go to the **Administration Console > Filters > Rules > Filter Rule List** tab and then click **Add**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



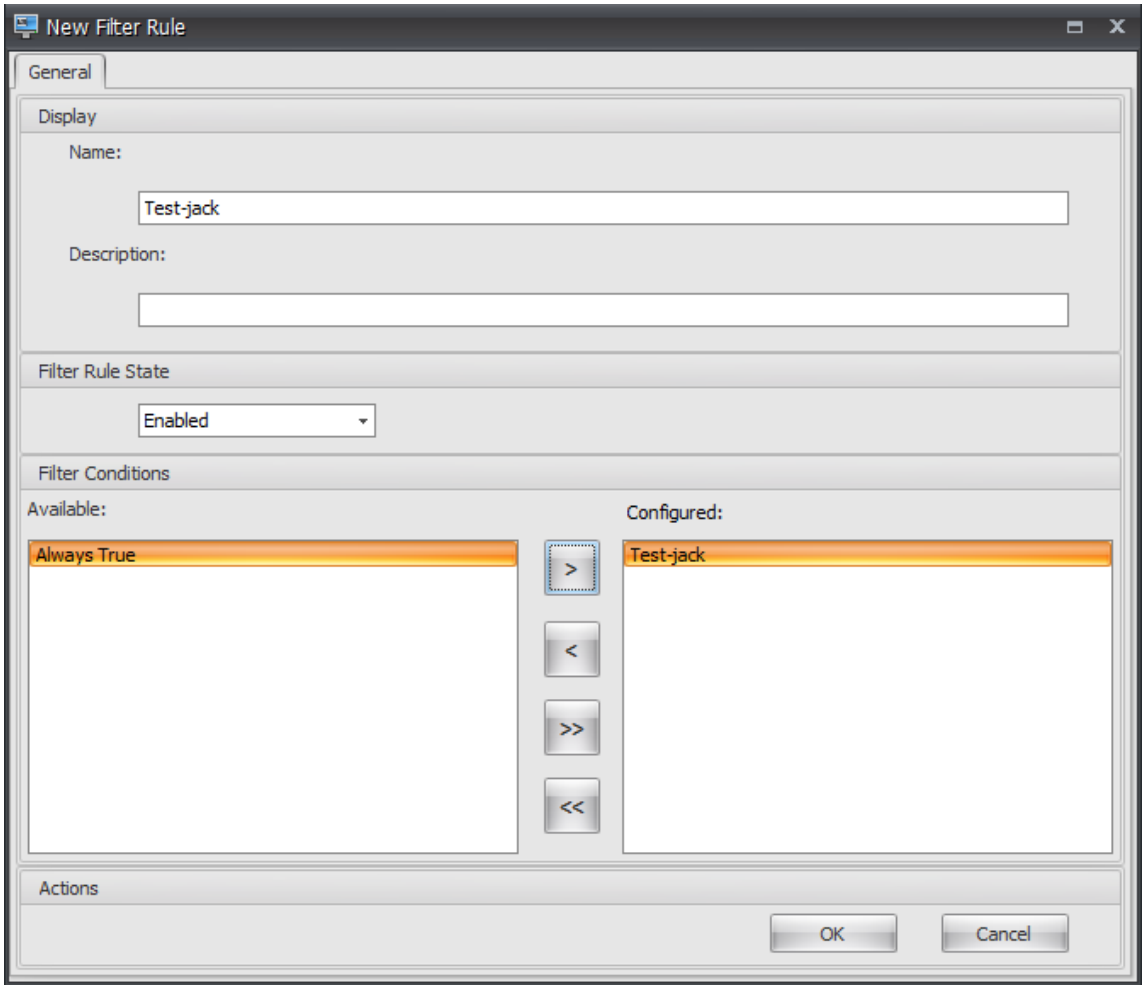
10. Type the filter name in the **Name** field.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



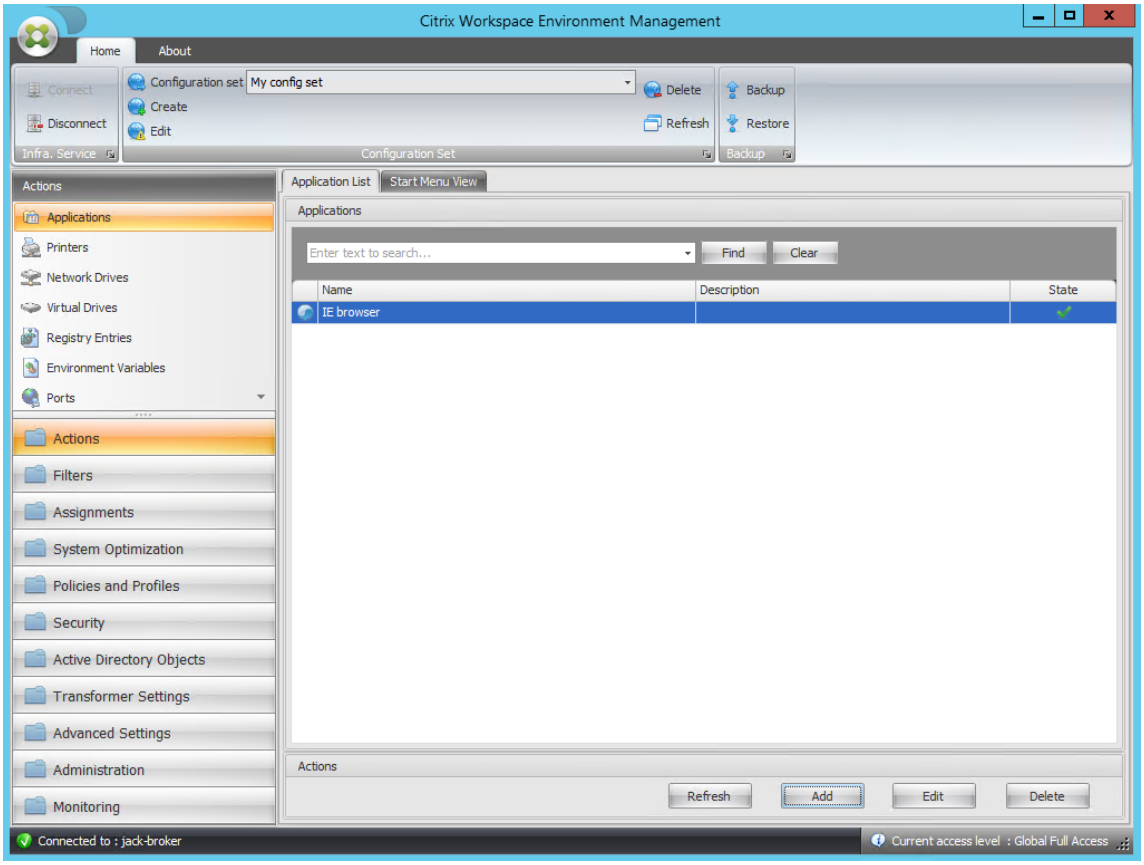
11. Move the configured condition from the **Available** pane to the **Configured** pane and then click **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



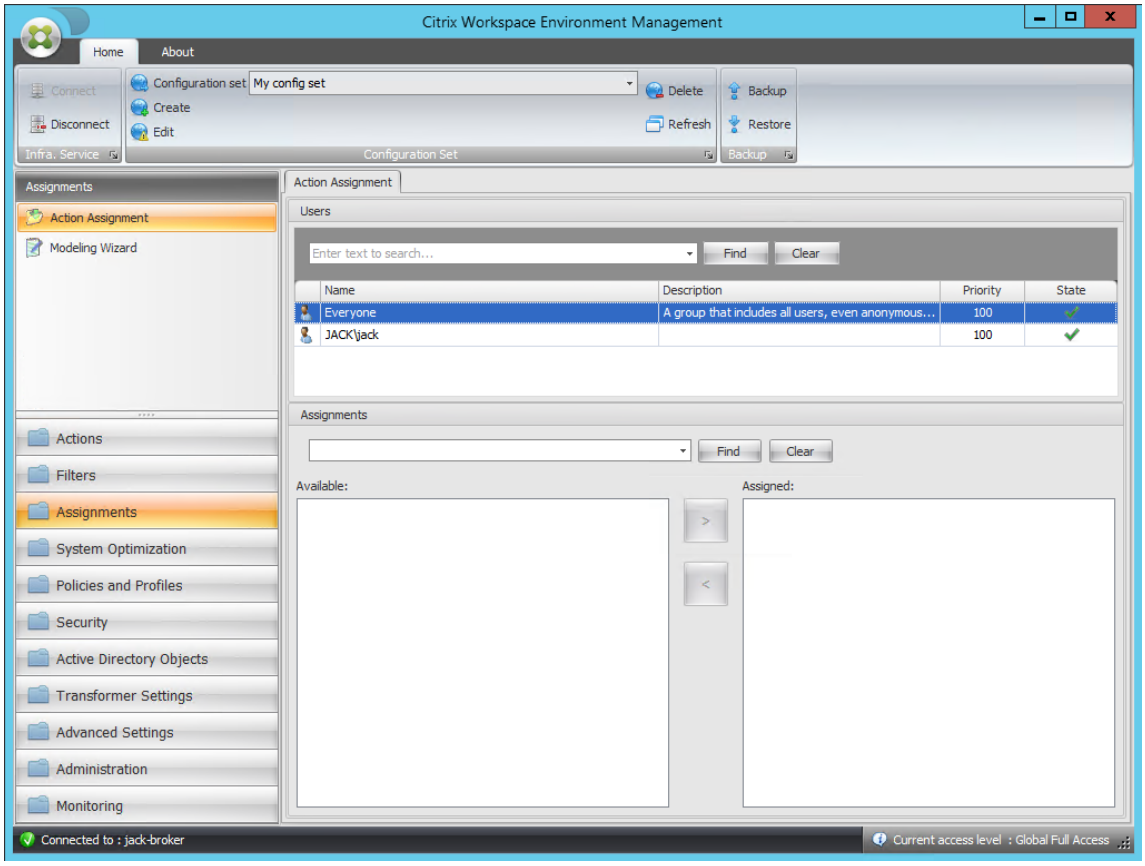
12. Go to the **Administration Console > Actions > Applications > Application List** tab and then add an application.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



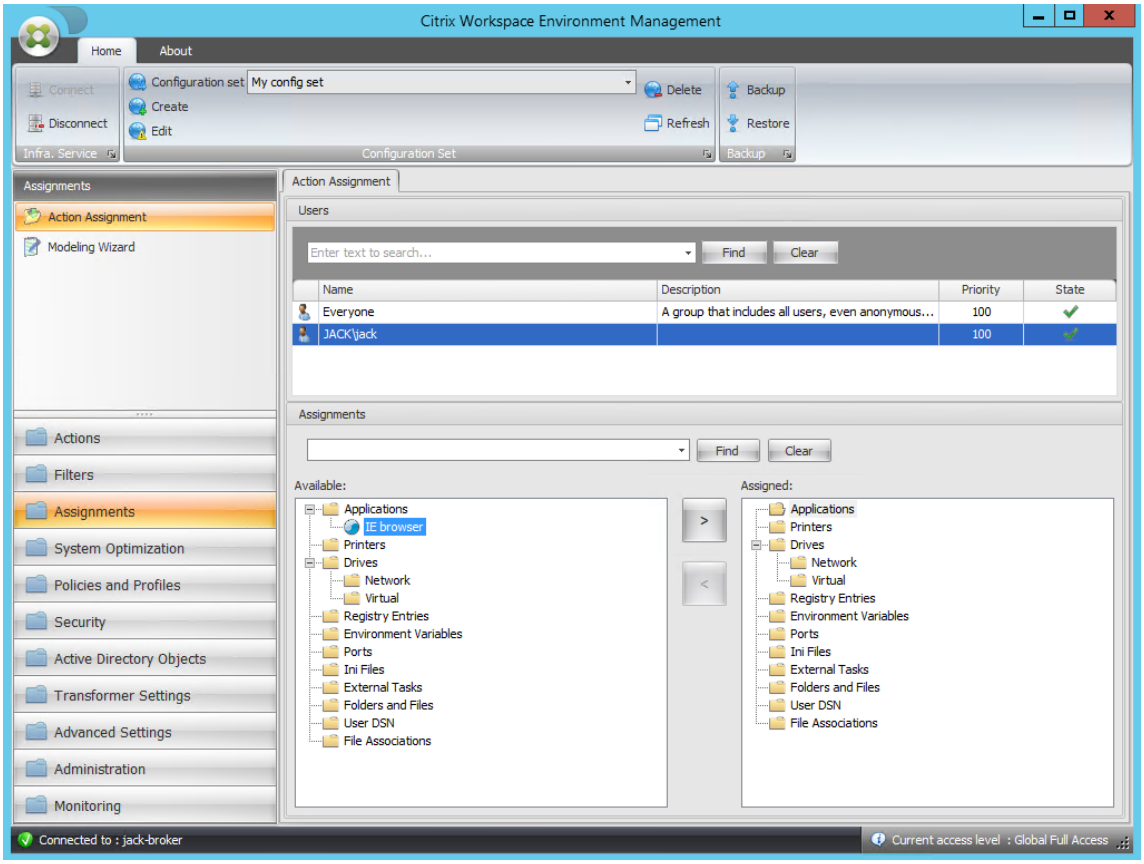
13. Go to the **Administration Console > Assignments > Action Assignment** tab.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

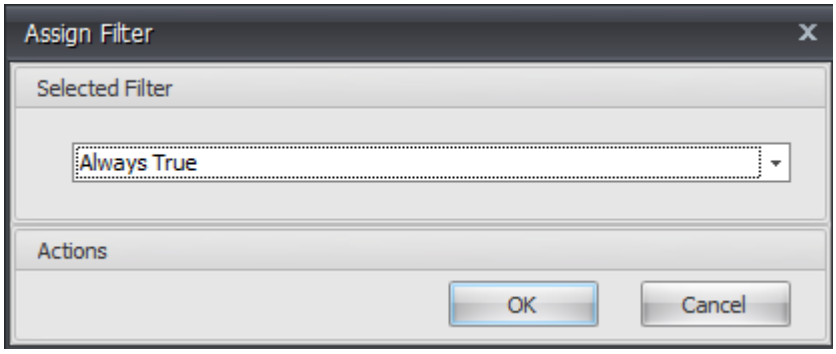


14. Double-click the desired user or user group (in this example, select the agent host).

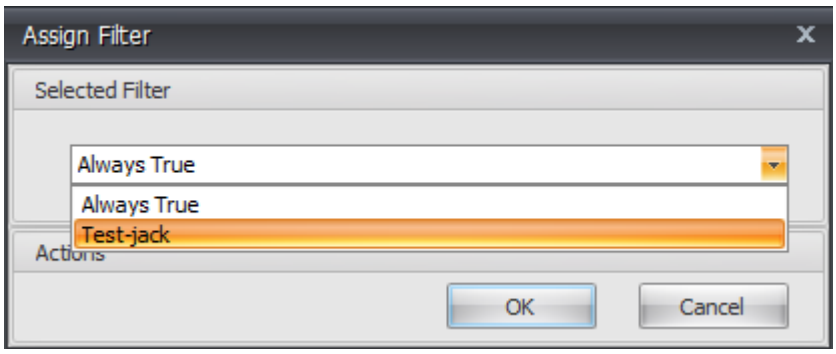
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



15. Move the application from the **Available** pane to the **Assigned** pane.

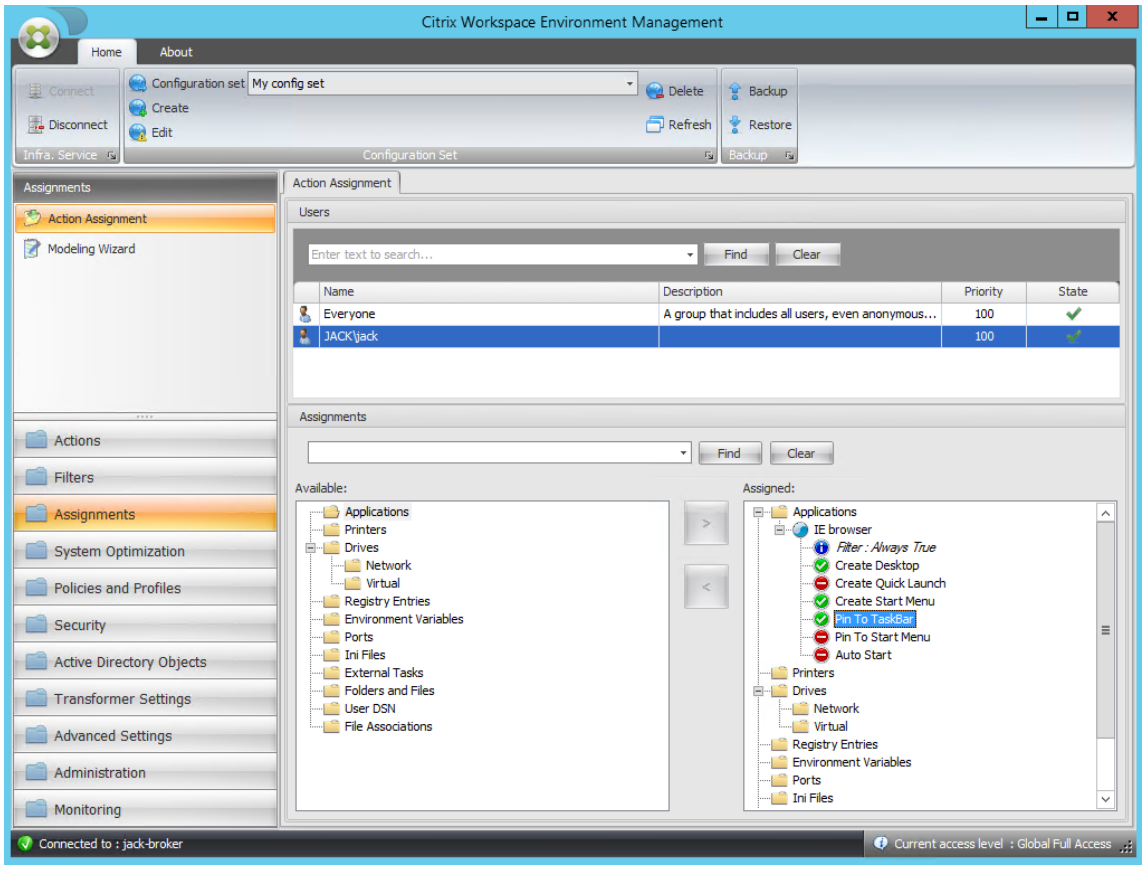


16. Select the filter and then click **OK**.



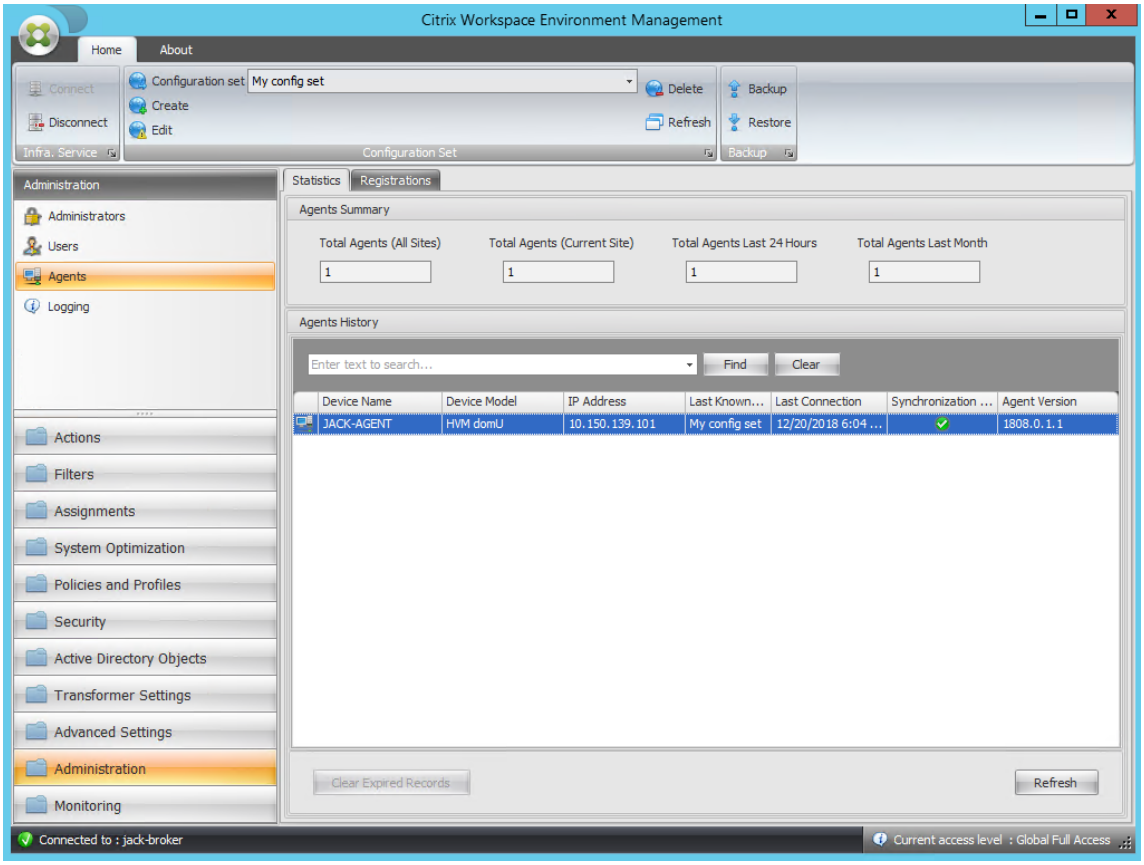
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

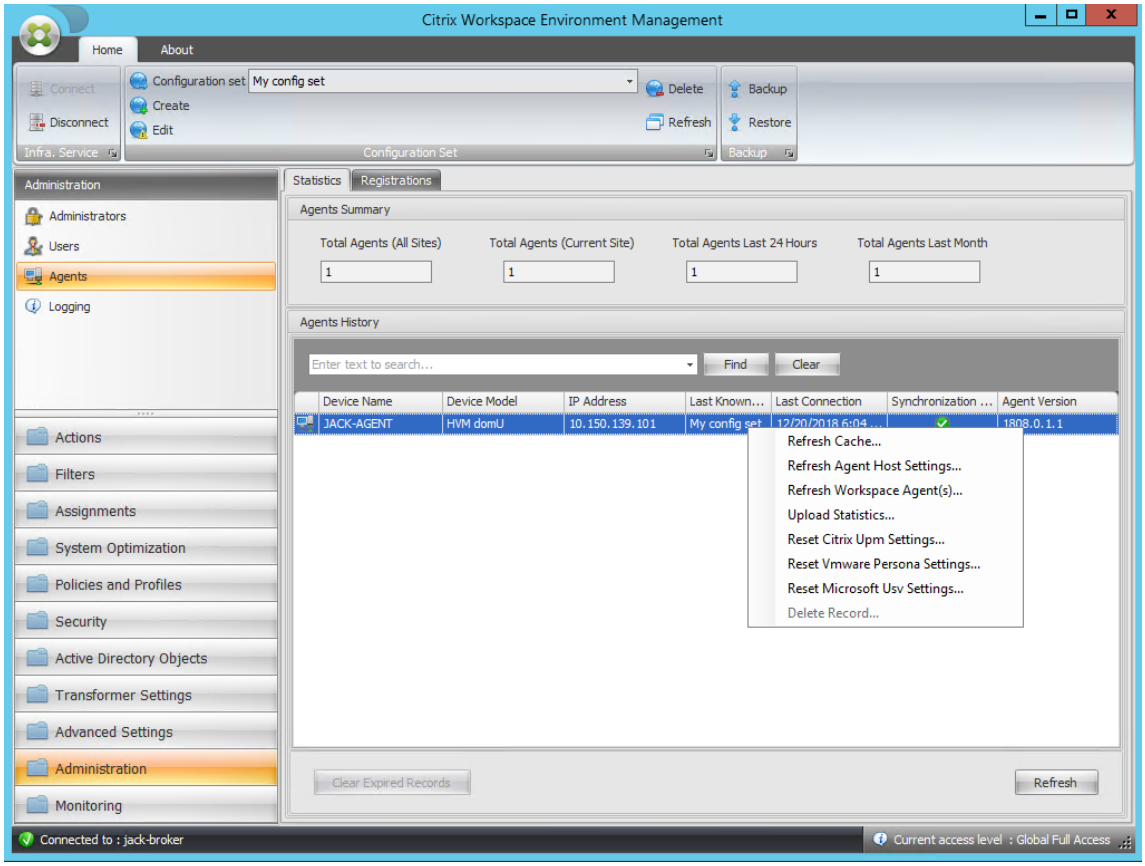
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



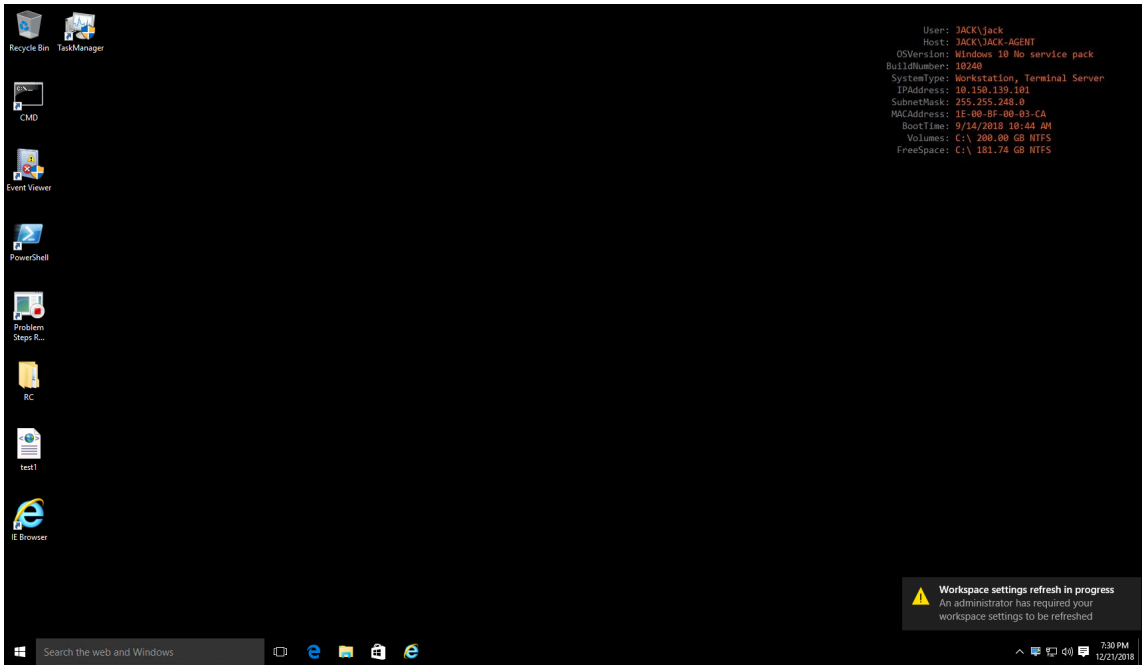
19. Right-click the agent and then select **Refresh Workspace Agent(s)** in the context menu.

> **Note:**
>
> For the settings to take effect, you can also go to the machine on which the agent is running and then refresh Citrix WEM Agent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



20. Go to the machine on which the agent is running (agent host) to verify that the configured condition works.



In this example, the application was assigned to the agent machine successfully. It was created on the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

desktop and pinned to the taskbar.

XML printer list configuration

December 6, 2022

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
        >
<!--NeedCopy-->
```

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>

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```

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
      >
<!--NeedCopy-->
```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

<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
2 <!--NeedCopy-->
```

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**

```
1     <?xml version="1.0" encoding="utf-8"?>
2       <
          ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:
          xsd="http://www.w3.org/2001/XMLSchema">
3         <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
4             <Key>DEVICE1</Key>
5             <Value>
6                 <VUEMUserAssignedPrinter>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                    <IdPrinter>1</IdPrinter>
                    <IdSite>1</IdSite>
                    <State>1</State>
                    <ActionType>0</ActionType>
                    <UseExtCredentials>0</UseExtCredentials>
                    <isDefault>1</isDefault>
                    <IdFilterRule>1</IdFilterRule>
                    <RevisionId>1</RevisionId>
                    <Name>HP LaserJet 2200 Series</Name>
                    <Description />
                    <DisplayName />
                    <TargetPath>\\server.example.net\HP LaserJet 2200
                       Series</TargetPath>
                    <ExtLogin />
                    <ExtPassword />
                    <Reserved01>&lt;?xml version="1.0" encoding="utf-8"
                       ?&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:
                       xsi="http://www.w3.org/2001/XMLSchema-instance"
                       xmlns:xsd="http://www.w3.org/2001/XMLSchema"&gt
                       ;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;
                       SelfHealingEnabled&lt;/Name&gt;&lt;Value&gt;0&lt
                       ;/Value&gt;&lt;/VUEMActionAdvancedOption&gt;&lt
                       ;/ArrayOfVUEMActionAdvancedOption&gt;</
                       Reserved01>
                </VUEMUserAssignedPrinter>
            </Value>
            <Value>
                <VUEMUserAssignedPrinter>
                    <IdPrinter>2</IdPrinter>
                    <IdSite>1</IdSite>
                    <State>1</State>
                    <ActionType>0</ActionType>
                    <UseExtCredentials>0</UseExtCredentials>
                    <isDefault>0</isDefault>
                    <IdFilterRule>1</IdFilterRule>
                    <RevisionId>1</RevisionId>
                    <Name>Canon C5531i Series</Name>
                    <Description />
                    <DisplayName />
                    <TargetPath>\\server.example.net\Canon C5531i
                       Series</TargetPath>
                    <ExtLogin />
                    <ExtPassword />
                    <Reserved01>&lt;?xml version="1.0" encoding="utf-8"
                       ?&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:
                       xsi="http://www.w3.org/2001/XMLSchema-instance"
                       xmlns:xsd="http://www.w3.org/2001/XMLSchema"&gt
                       ;&lt;VUEMActionAdvancedOption&gt;&lt;Name&gt;
                       SelfHealingEnabled&lt;/Name&gt;&lt;Value&gt;0&lt
                       ;/Value&gt;&lt;/VUEMActionAdvancedOption&gt;&lt
                       ;/ArrayOfVUEMActionAdvancedOption&gt;</
                       Reserved01>
                </VUEMUserAssignedPrinter>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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
               >
65  <!--NeedCopy-->
```

Glossary

March 30, 2022

This article contains terms and definitions used in the Workspace Environment Management (WEM) software and documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

[1] on-premises term only

[2] Citrix Cloud service term only

Admin Broker Port. Legacy term for "administration port".

administration console. An interface that connects to the infrastructure services. You use the administration console to create and assign resources, manage policies, authorize users, and so on.

In Citrix Cloud, the Workspace Environment Management service administration console is hosted on a Citrix Cloud-based Citrix virtual apps server. You use the administration console to manage your WEM installation from the service's **Manage** tab using your web browser.

administration port [1]. Port on which the administration console connects to the infrastructure service. The port defaults to 8284 and corresponds to the AdminPort command-line argument.

agent. The Workspace Environment Management agent consists of two components: the agent service and the session agent. These components are installed on the agent host.

Agent Host executable. Legacy term for "session agent".

Agent Host machine. Legacy term for "agent host".

Agent Host service. Legacy term for "agent service".

Agent Broker Port. Legacy term for "agent service port".

Agent Cache Synchronization Port. Legacy term for"cache synchronization port".

agent host. The machine on which the agent is installed.

agent host configuration GPO. The Group Policy Object (GPO) administrative template provided with the agent installation as ADM or ADMX files. Administrators import these files into Active Directory and then apply the settings to a suitable organizational unit.

agent port [1]. Listening port on the agent host which receives instructions from the infrastructure service. Used, for example, to force agents to refresh from the administration console. The port default is 49752.

agent service. The service deployed on VDAs or on physical Windows devices in Transformer use cases. It is responsible for enforcing the settings you configure using the administration console.

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".

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).