

# Workspace Environment Management 4.3

May 30, 2017

## Workspace Environment Management

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

### Resource management

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

### Profile Management

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

## What's new

### Site management

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

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

### Agent localization improvements

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

### User interface improvements

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

### Documentation

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

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

## Fixed issues

The following issues have been fixed since Version 4.3:

- When the Workspace Environment Management session agent is running in command line mode, User Statistics data is not reported to the WEM infrastructure services.  
[WEM-41]
- The Workspace Environment Management session agent interface does not render correctly when a computer display is extended to external displays connected via a dock. This problem, which occurs when extending to multiple displays with different screen resolution settings, results in a portion of the right-hand side of the display not rendering completely. This prevents users seeing the home button or being able to change other native Workspace Environment Management settings.  
[WEM-90]
- The Workspace Environment Management session agent causes the mouse to stop working on virtual machines which have the System Center Configuration Manager (SCCM) client installed with Power Management enabled.  
[WEM-115]
- When you are using the Transformer feature, the session agent generates an unhandled exception if Wi-Fi is turned off using "ms-settings:network-wifi."  
[WEM-133]
- The Workspace Environment Management session agent causes the mouse to stop working on virtual machines after an interruption to network access is restored.  
[WEM-159]

## Known issues

This release contains the following issues:

- On Windows Server 2012 R2, if Adobe Acrobat Reader is installed it prevents Workspace Environment Management associating files of type .PDF with other PDF reader applications. Users are forced to manually select the PDF reader application to use each time they open a PDF.  
[#WEM-33]

## Deprecated

The announcements in this section are intended to give you advanced notice of platforms and Workspace Environment

Management features which are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. This list is subject to change in subsequent releases and may not include every deprecated feature or functionality.

The following platforms and Workspace Environment Management features are *deprecated*. This does not mean that they are removed immediately. Citrix will continue to support them up to and including the next XenApp and XenDesktop Long Term Service Release (LTSR) release.. Deprecated items will be removed in a Current Release following the next LTSR. Alternatives for deprecated items are suggested where possible.

For complete details about product lifecycle support, see [Product Lifecycle Support Policy](#).

Item	Announced 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.
The Administration Console will not be supported on the following platforms after the next LTSR: Windows XP SP3 32-bit and 64-bit Windows Vista SP1 32-bit and 64-bit Windows 8.x 32-bit and 64-bit Windows Server 2003 32-bit and 64-bit Windows Server 2003 R2 32-bit and 64-bit Windows Server 2008 Windows Server 2008 R2	4.2	
Workspace Environment Management will not be supported on the following software after the next LTSR: Microsoft .NET Framework 4.0 Microsoft .NET Framework 4.5.0 Microsoft .NET Framework 4.5.1	4.2	

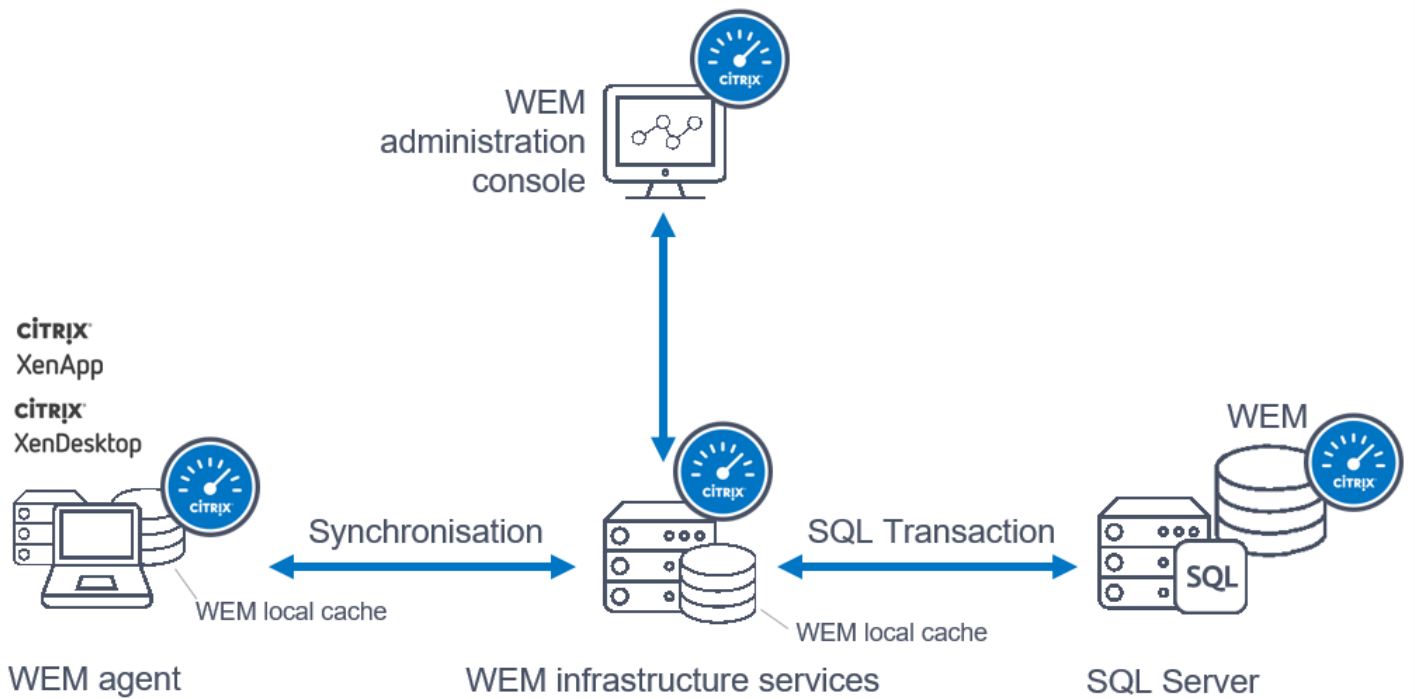
## Removed

The following platforms, Citrix products, and features are either removed in Workspace Environment Management 4.3 or are no longer supported in Workspace Environment Management 4.3.

Item	Replacement
Support for assigning and binding version 4.3 agents to sites via GPO.	Assign and bind version 4.3 agents to sites via administration console.

## Technical overview

Workspace Environment Management (WEM) has the following architecture:



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

## Note

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

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

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

## Note

The agent cannot be installed on the infrastructure server. The agent installer fails in this scenario.

## Note

The Transformer feature is not supported on server operating systems.

**SQL Server Database:** Workspace Environment Management requires an SQL Server database to store its settings. The Workspace Environment Management database requires a minimum of 50 MB of disk space.

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

## Port information

Source	Destination	Type	Port	Details
Infrastructure service	Agent host	TCP	49752	"Agent port". Listening port on the agent host which receives instructions from the infrastructure service.
Administration console	Infrastructure service	TCP	8284	"Administration port". Port on which the administration console connects to the infrastructure service.
Agent	Infrastructure service	TCP	8286	"Agent service port". Port on which the agent connects to the infrastructure server.
Agent cache synchronization process	Infrastructure service	TCP	8285	"Cache synchronization port". Port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server.
Infrastructure service	Citrix License Server	TCP	27000	"Citrix License Server port". The port on which the Citrix License Server is listening and to which the infrastructure service then connects to validate licensing.
Monitoring service	Infrastructure service	TCP	8287	"WEM monitoring port". Listening port on the infrastructure server used by the monitoring service. (Not yet implemented.)

# System requirements

Jun 19, 2017

## Software prerequisites

**.NET Framework.** This is necessary for all Workspace Environment Management components. If the correct version is not available, installation fails. Version 4.5.2 or 4.6.2 are recommended (depending on OS), but the following versions are the minimum requirements:

**.NET 4.0 (full package or Client Profile).** This is the minimum necessary for the agent and administration console.

**.NET 4.5.2.** This is minimum necessary for the infrastructure services.

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

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

**Microsoft SQL Server 2008 R2 or later:** Workspace Environment Management requires **sysadmin access** to a SQL Server instance to create its database, and read/write access to this database to use it.

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

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

**Citrix XenApp and XenDesktop.** Any [currently supported version](#) of XenApp or XenDesktop is required for this release of Workspace Environment Management.

## Tip

### SQL AlwaysOn

Workspace Environment Management does not use any features or settings that would prevent you using SQL AlwaysOn. However, SQL AlwaysOn is currently not one of our test scenarios and cannot therefore be certified. We will continue to monitor demand for SQL AlwaysOn for certification consideration in a future release.

In the meantime if you are using SQL AlwaysOn and run into issues, to get support you may need to break the clustering and demonstrate that the issue is still present without SQL AlwaysOn.

## Operating system prerequisites

### Infrastructure services

Windows Server 2008 R2

Windows Server 2012  
Windows Server 2012 R2  
Windows Server 2016

#### **Administration console**

Windows XP SP3 32-bit and 64-bit  
Windows Vista SP1 32-bit and 64-bit  
Windows 7 32-bit and 64-bit  
Windows 8.x 32-bit and 64-bit  
Windows 10 32-bit and 64-bit  
Windows Server 2003 32-bit and 64-bit  
Windows Server 2003 R2 32-bit and 64-bit  
Windows Server 2008  
Windows Server 2008 R2  
Windows Server 2012  
Windows Server 2012 R2  
Windows Server 2016

#### **Agent**

Windows XP SP3 32-bit and 64-bit  
Windows Vista SP1 32-bit and 64-bit  
Windows 7 32-bit and 64-bit  
Windows 8.x 32-bit and 64-bit  
Windows 10 32-bit and 64-bit  
Windows Server 2003 32-bit and 64-bit\*  
Windows Server 2003 R2 32-bit and 64-bit\*  
Windows Server 2008\*  
Windows Server 2008 R2\*  
Windows Server 2012\*  
Windows Server 2012 R2\*  
Windows Server 2016\*

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

#### Hardware prerequisites

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

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

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

**Database:** 50 MB of available disk space.

#### Service dependencies

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

## Anti-virus exclusions

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

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

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

C:\Program Files (x86)\Norskale\Norskale Infrastructure Services

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

### **In the infrastructure services installation directory:**

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

### **In the agent installation directory:**

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



# Install and configure

May 22, 2017

Install and configure the following components:

- [Infrastructure services](#)
- [Administration console](#)
- [Agent](#)

# Infrastructure services

Jun 28, 2017

There is currently one infrastructure service:

Norskale Infrastructure Service (NT SERVICE\Norskale Infrastructure Service) : Manages WEM Infrastructure services.  
Account: LocalSystem or specified user account.

## Install the infrastructure services

### Important

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

To Install the infrastructure services, run **Citrix Workspace Environment Management Infrastructure Services v4.03.00.00 Setup.exe** on your infrastructure server. The infrastructure services install into the following default directory: C:\Program Files (x86)\Norskale\Norskale Infrastructure Services.

You can customize your installation using the following arguments:

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

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

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

The syntax for these install arguments is:

```
"path:\to\Citrix Workspace Environment Management Infrastructure Services v4.03.00.00 Setup" /v"argument1=\"value1\" argument2=\"value2\""
```

Create SPNs

### Note

When you are using load balancing, all instances of the infrastructure services must be installed and configured using the same service account name.

After the installer is finished, create a Service Principal Name (SPN) for the infrastructure service. Use the command that is applicable to your environment:

- You do not use Windows authentication or load balancing:

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

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

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

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

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

SPNs are case-sensitive.

## Configure load balancing

To configure Workspace Environment Management with a load balancing service:

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

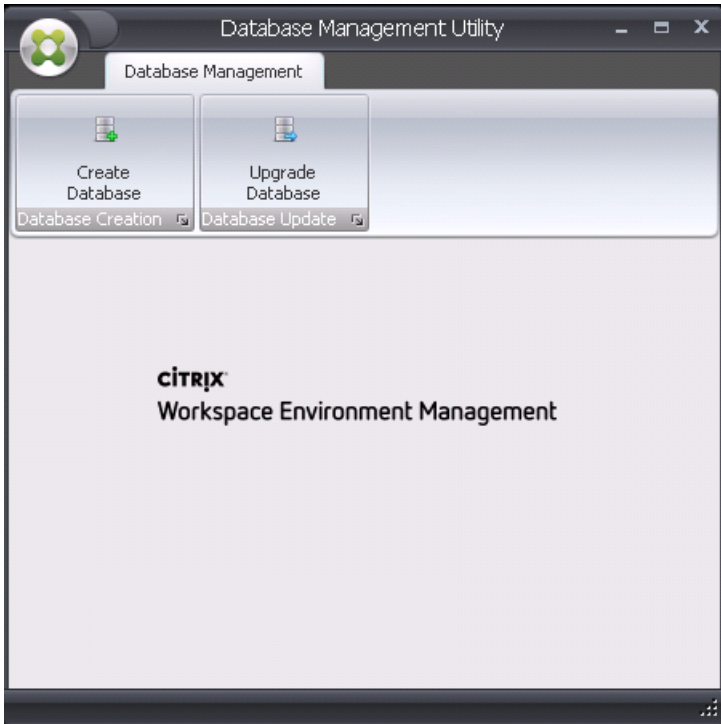
# Create a Workspace Environment Management database

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

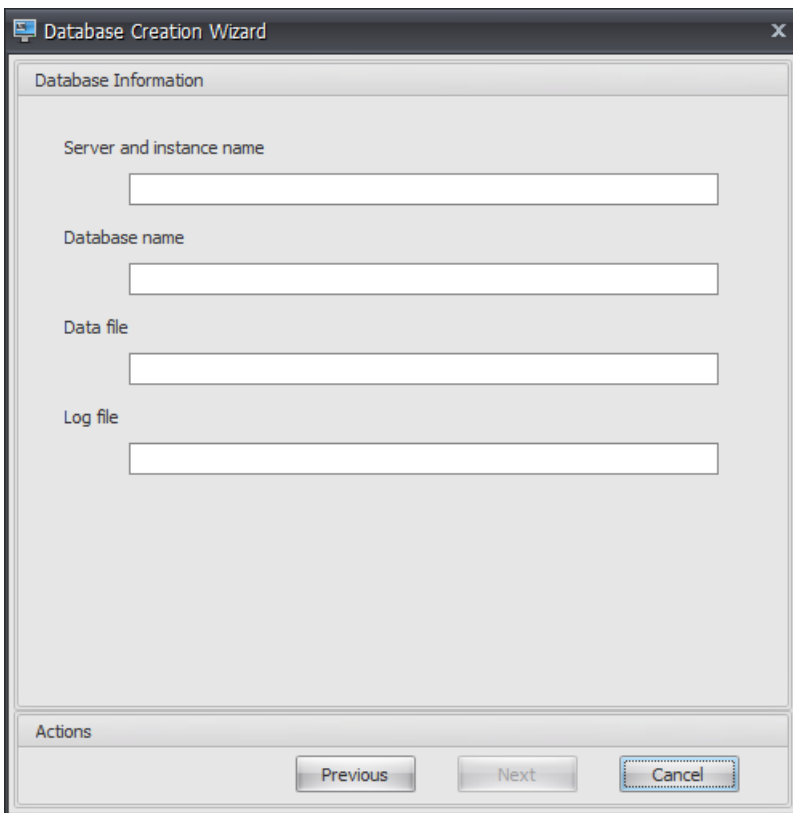
**Note:** If you are using Windows authentication for your SQL Server, run the database creation utility under an identity that has sysadmin permissions.

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

Management>Database Management>Database Management Utility.



2. Click **Create Database**.



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

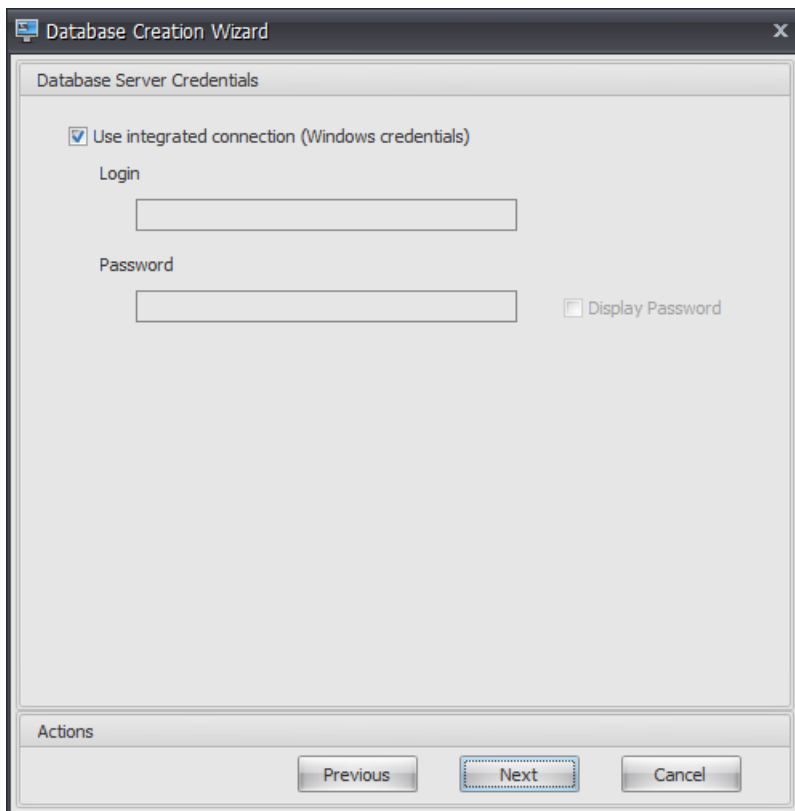
**Server and instance name.** Address of the SQL Server on which the database will be hosted. This address must be reachable exactly as typed from the infrastructure server. Type server and instance name as the machine name, fully qualified domain name, or IP address. Specify a full instance address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

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

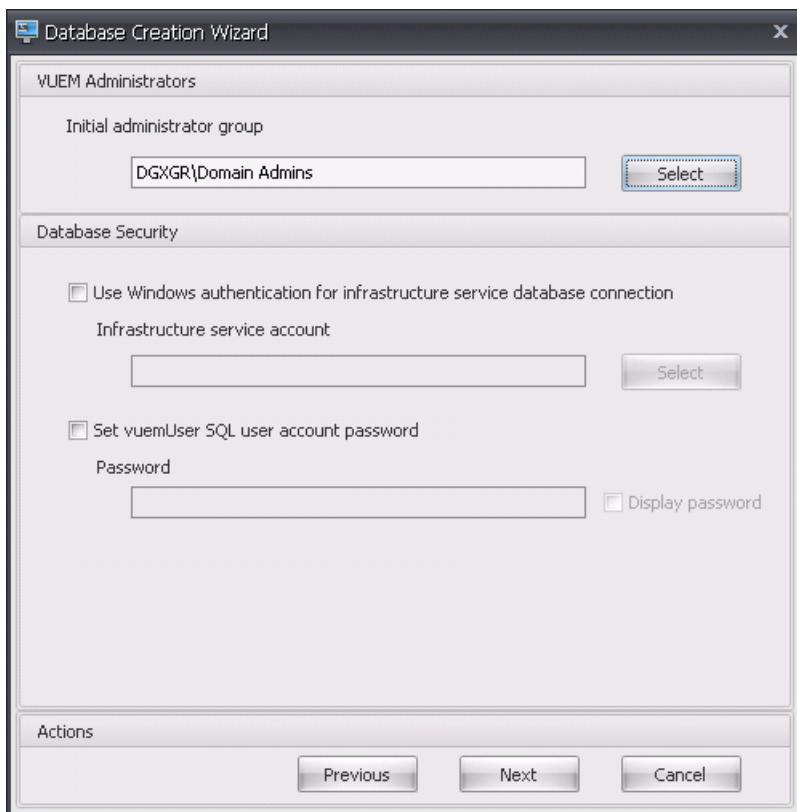
**Log file:** path to the **.ldf** file location on the SQL Server.

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



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

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



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

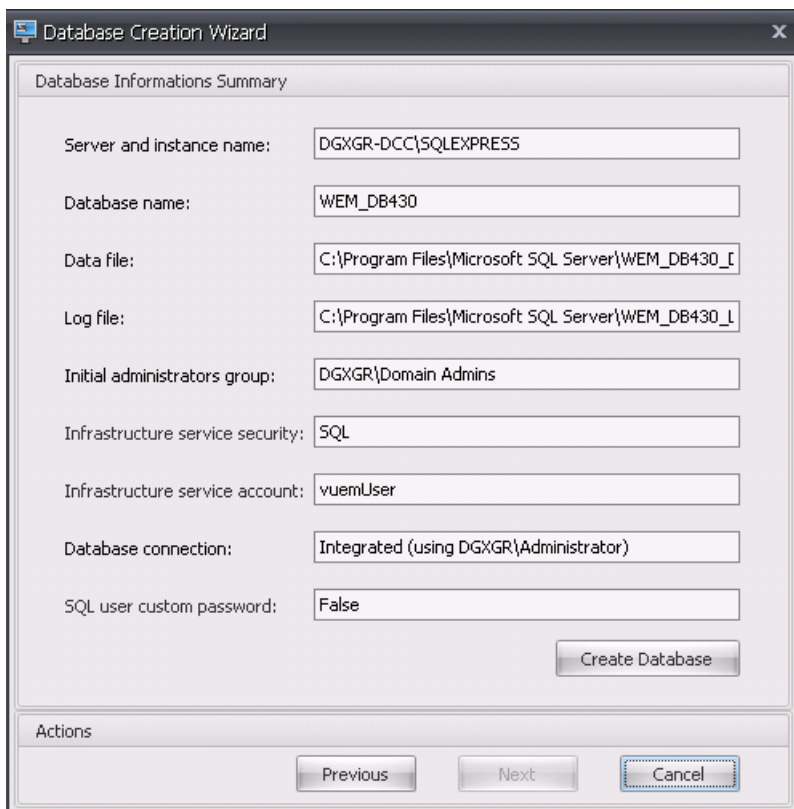
**Initial administrator group.** This user group is pre-configured as Full Access administrators for the Administration Console. Only users configured as Workspace Environment Management administrators are allowed to use the administration console. Specify a valid user group or you will not be able to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

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

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

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

**Important:** If you set your own password here, remember to specify the same password when you [configure the infrastructure service](#).



6. Review the settings you have selected, and when you are satisfied click **Create Database**.

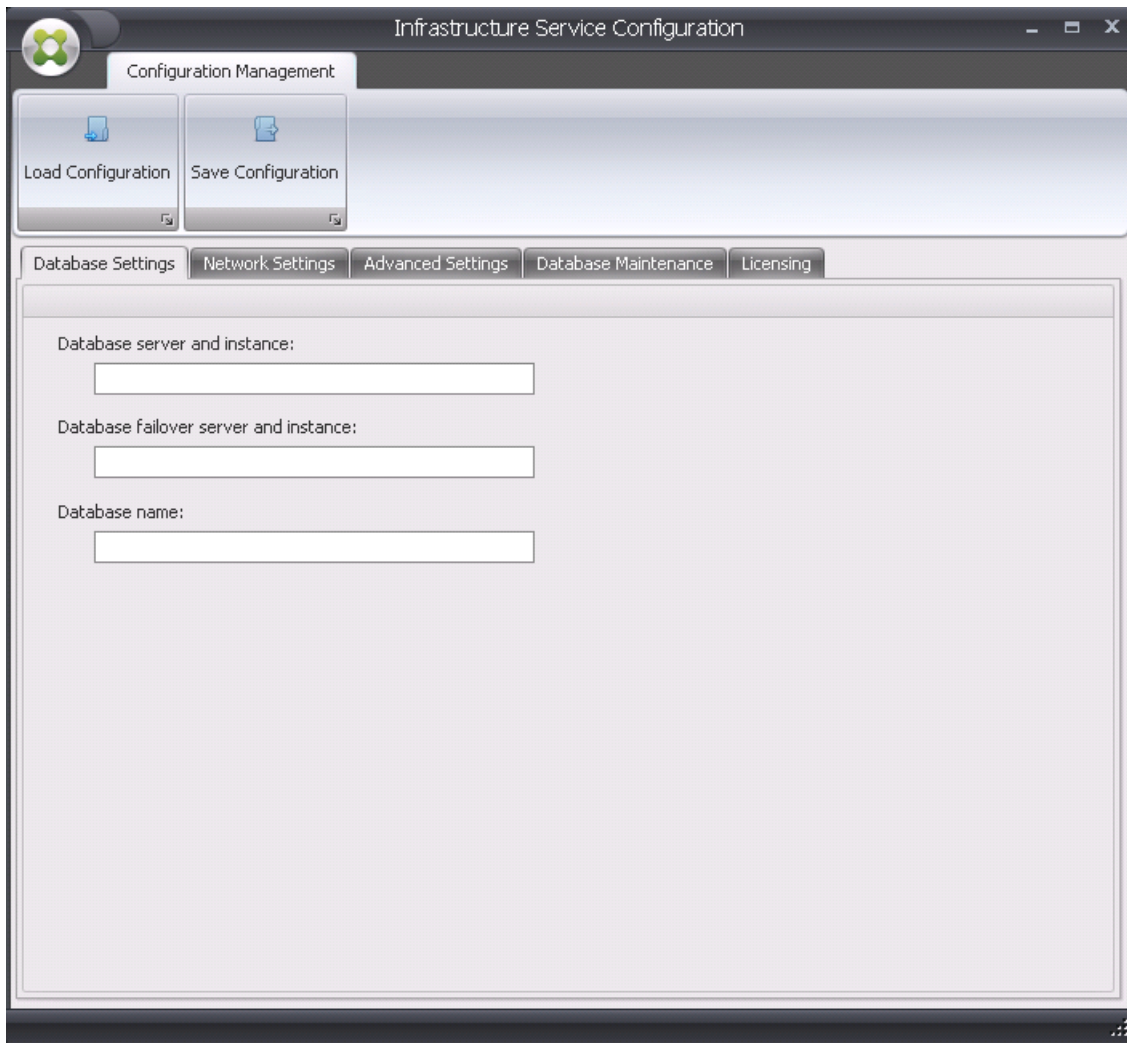
7. When you are notified that the database creation has completed successfully, click **Finish** to exit the wizard.

If there is an error 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

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

1. From the **Start** menu select **Citrix>Workspace Environment Management>Broker Service Configuration**.



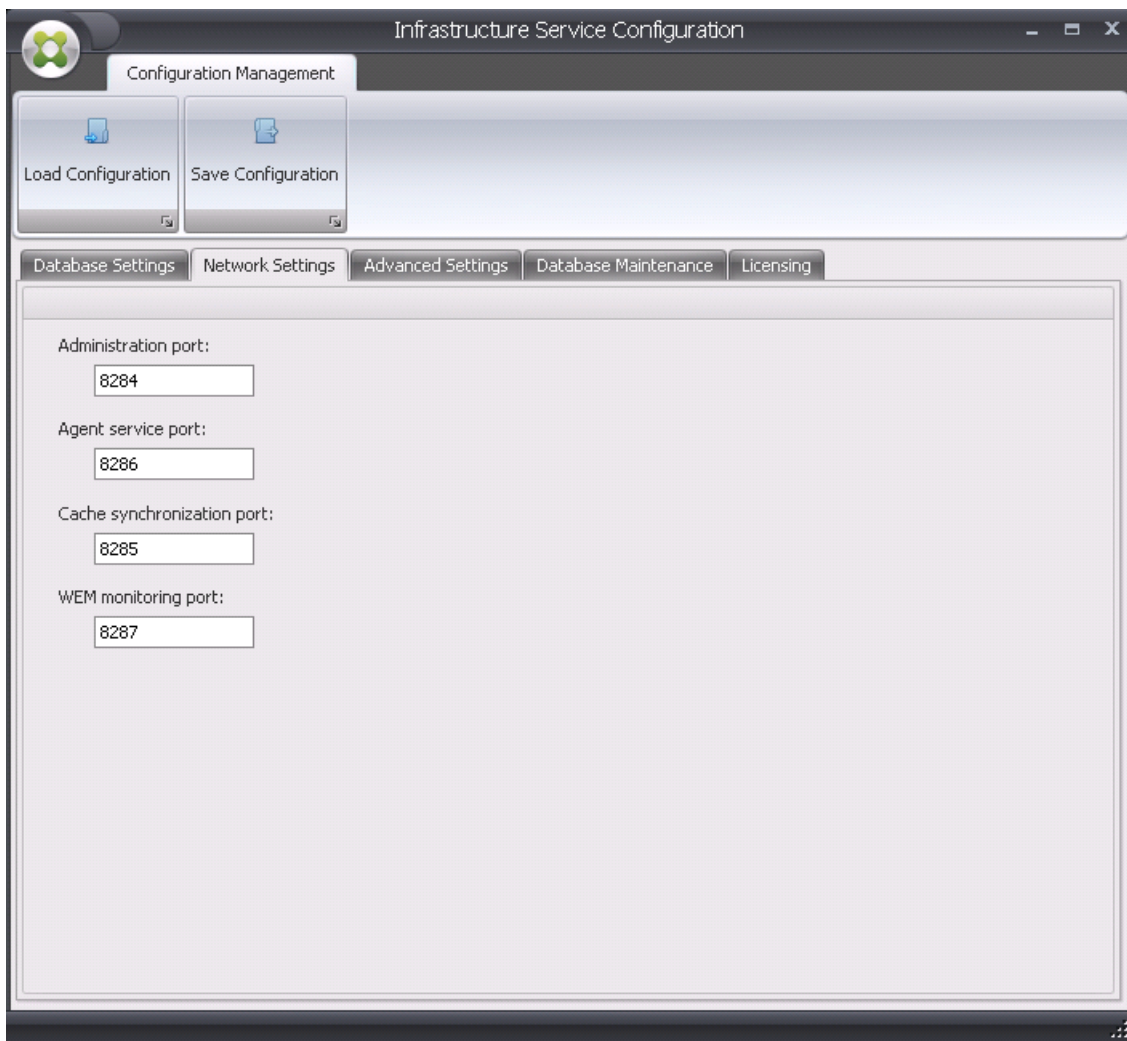
2. In the **Database Settings** tab enter the following details:

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

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

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





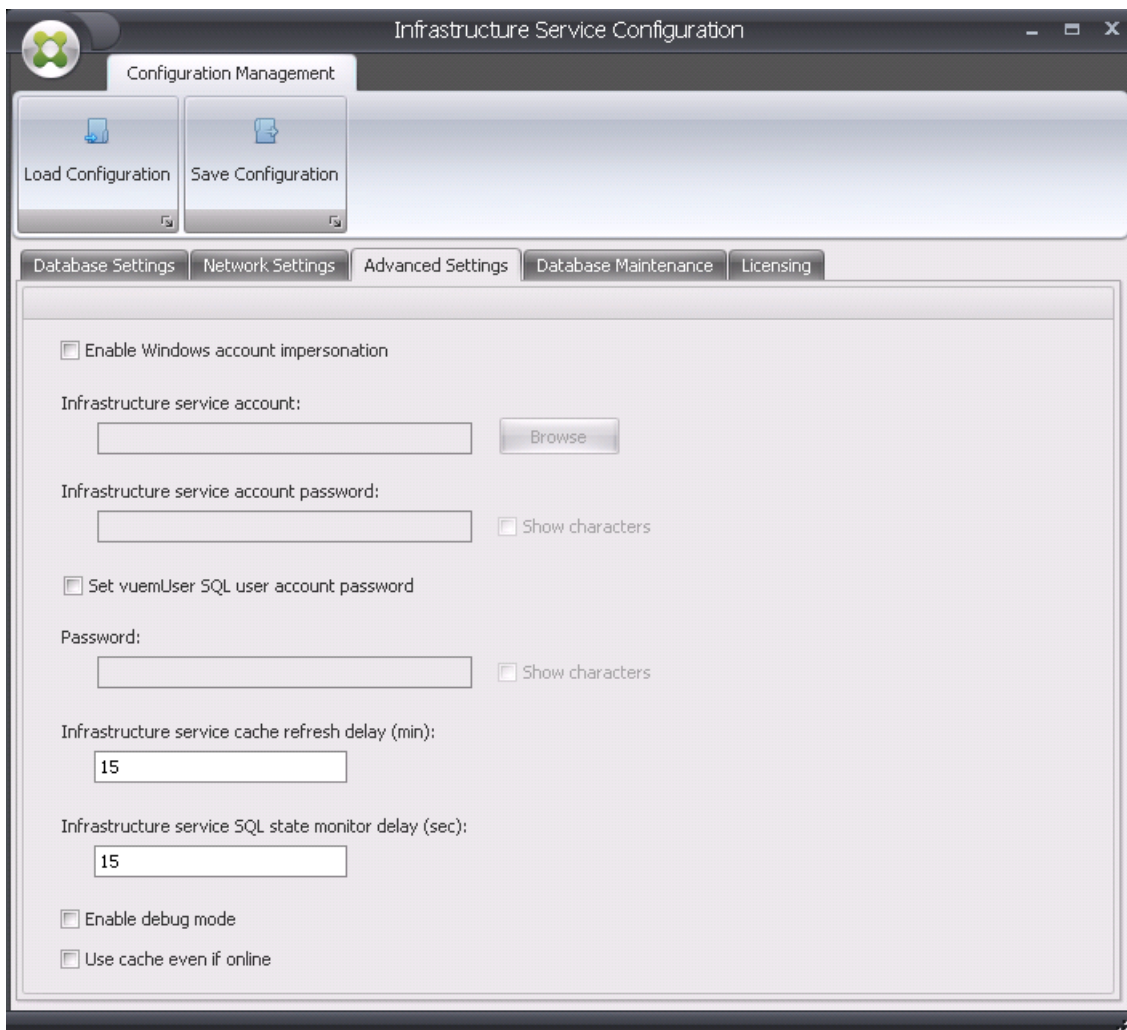
3. In the **Network Settings** tab type the ports the infrastructure service uses:

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

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

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

**WEM monitoring port.** [Not currently used.]



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

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

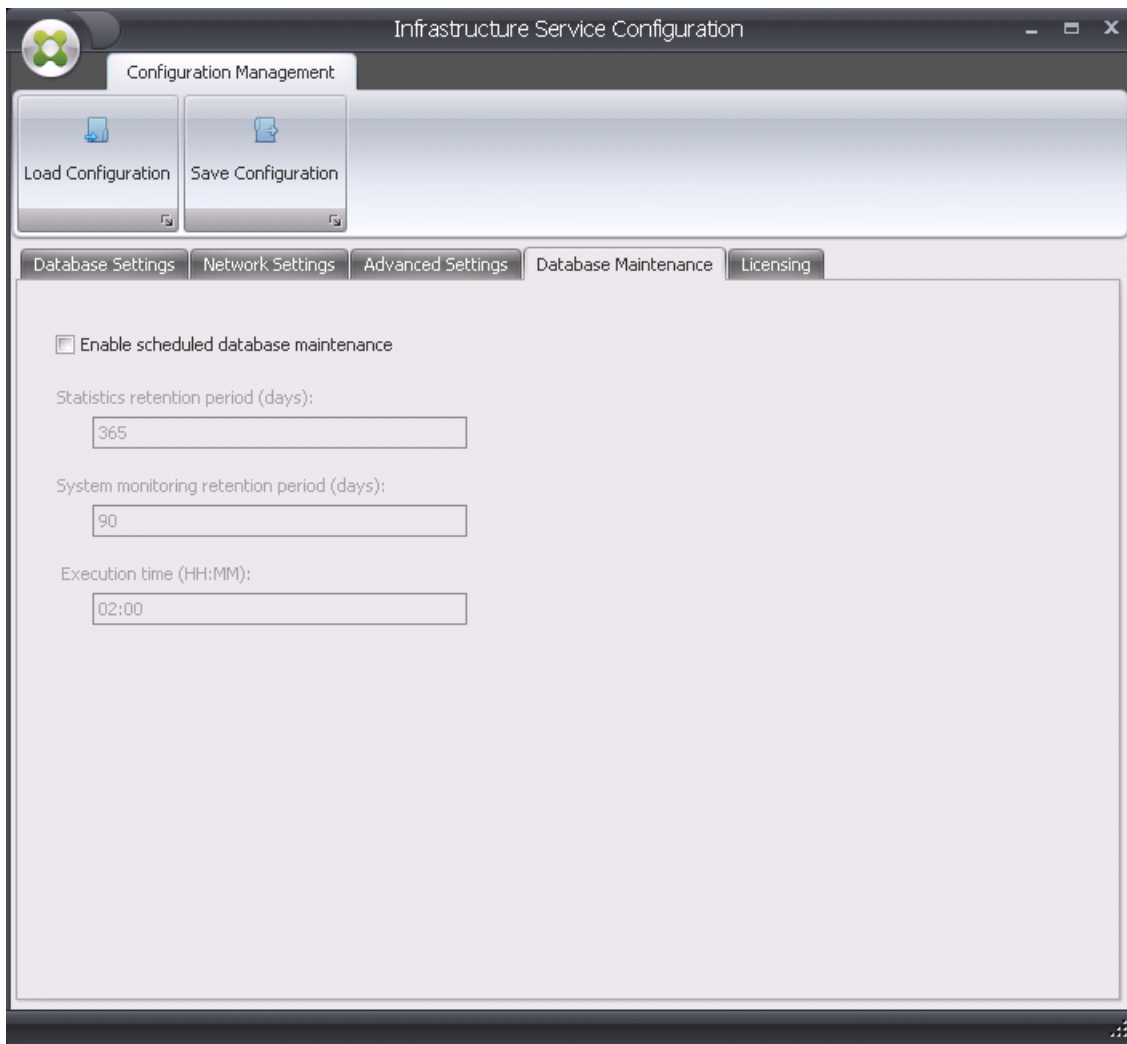
**Set vuemUser SQL user account password.** Allows you to inform the infrastructure service of a custom password configured for the *vuemUser* SQL user during database creation. Only enable this option if you provided your own password during database creation.

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

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

**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.



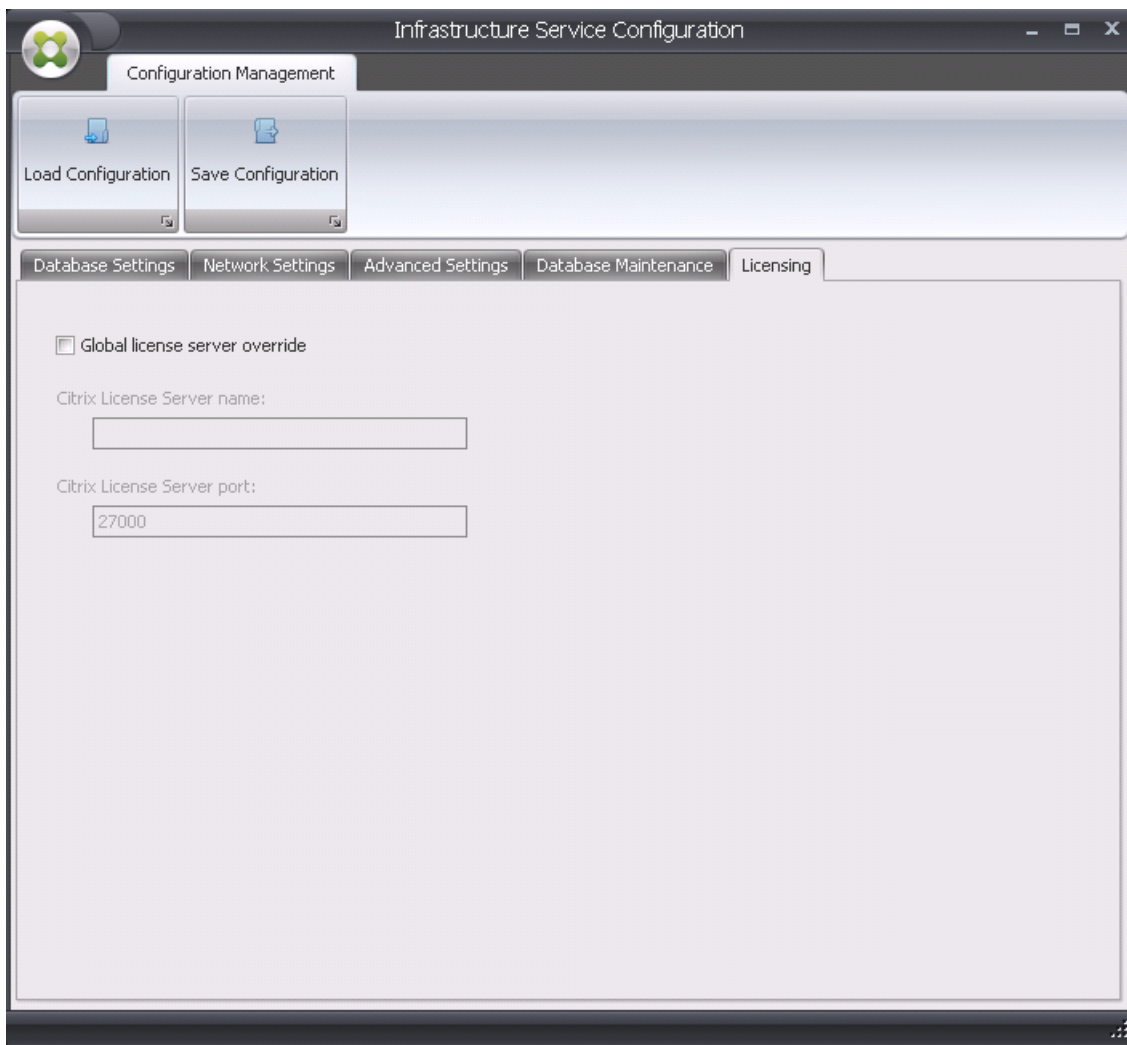
5. You can use the **Database Maintenance** tab to configure database maintenance.

**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.

**System monitoring retention period.** Determines how long system optimization statistics are retained.

**Execution time.** Determines the time at which the database maintenance action is performed.



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

**Global license server override.** Enable this option to enter the credentials of the Citrix License Server used by Workspace Environment Management. Information you enter here will override any Citrix License Server information already in the Workspace Environment Management database.

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

# Administration console

May 22, 2017

## Install the administration console

Run **Citrix Workspace Environment Management Console v4.03.00.00 Setup.exe** on your administrator console environment.

You can customize your installation using these arguments:

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

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

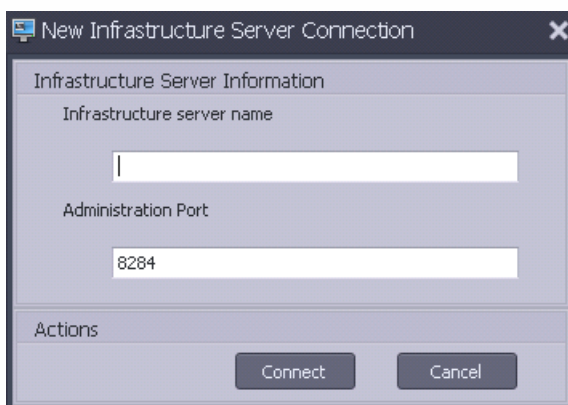
The syntax for these install arguments is as follows:

```
"path:\to\Citrix Workspace Environment Management Console v4.03.00.00 Setup " /v"argument=\"value\""
```

## Configure the administration console

Create an infrastructure server connection

1. In the **Start** menu select **Citrix>Workspace Environment Management>Administration Console**. By default, the administration console launches in a disconnected state.
2. In the ribbon, click **Connect** to open the New Infrastructure Server Connection window.

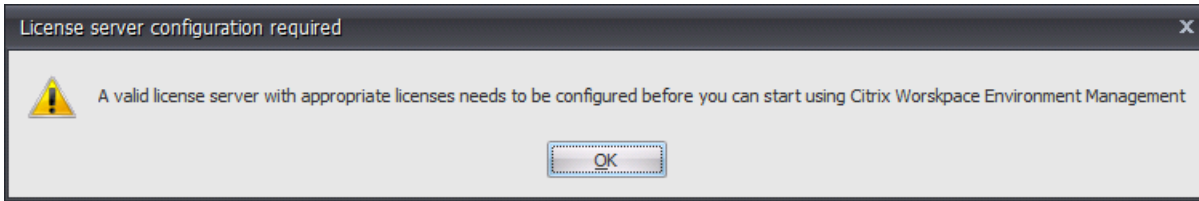


3. Enter the following values then click **Connect**:

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

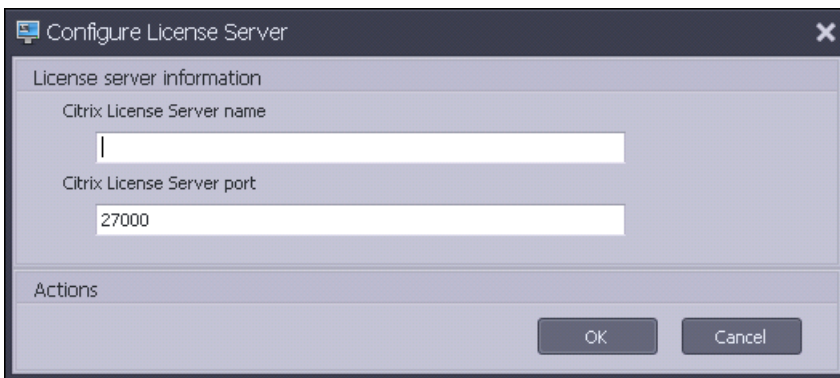
**Administration port.** The port on which the administration console connects to the infrastructure service.

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



Configure the database with a license server

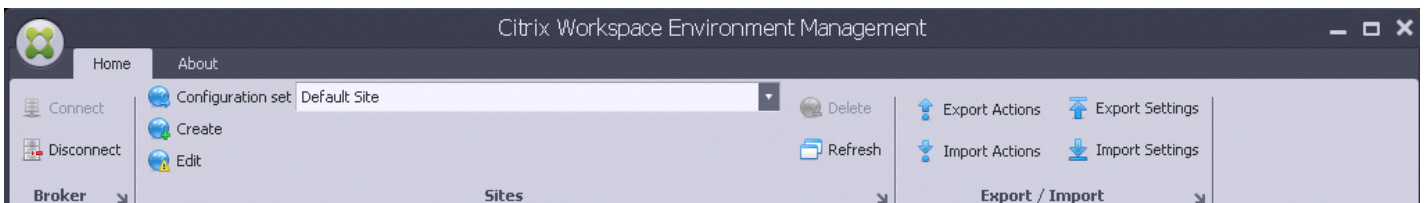
To configure the database with a license server, in the administration console ribbon click **About** then click **Configure License Server** and enter your Citrix License Server details. The Citrix License Server address must resolve from the administration console environment exactly as entered.



## Import quickstart settings

Workspace Environment Management includes XML files which pre-configure your Workspace Environment Management database so that it is proof-of-concept-ready out of the box. The Environmental Settings included in the quickstart setting files are a sample lockdown configuration. All other setting groups are based on best practices.

1. To import the quickstart setting files, in the **Home** ribbon click **Import Settings**:



2. In the **Setting Import Wizard**, select the folder "Configuration Templates" containing the quickstart setting files, then select every Setting Type.

# Agent

May 22, 2017

## Configure the agent

### Note

The Workspace Environment Management agent cannot be installed on the infrastructure server.

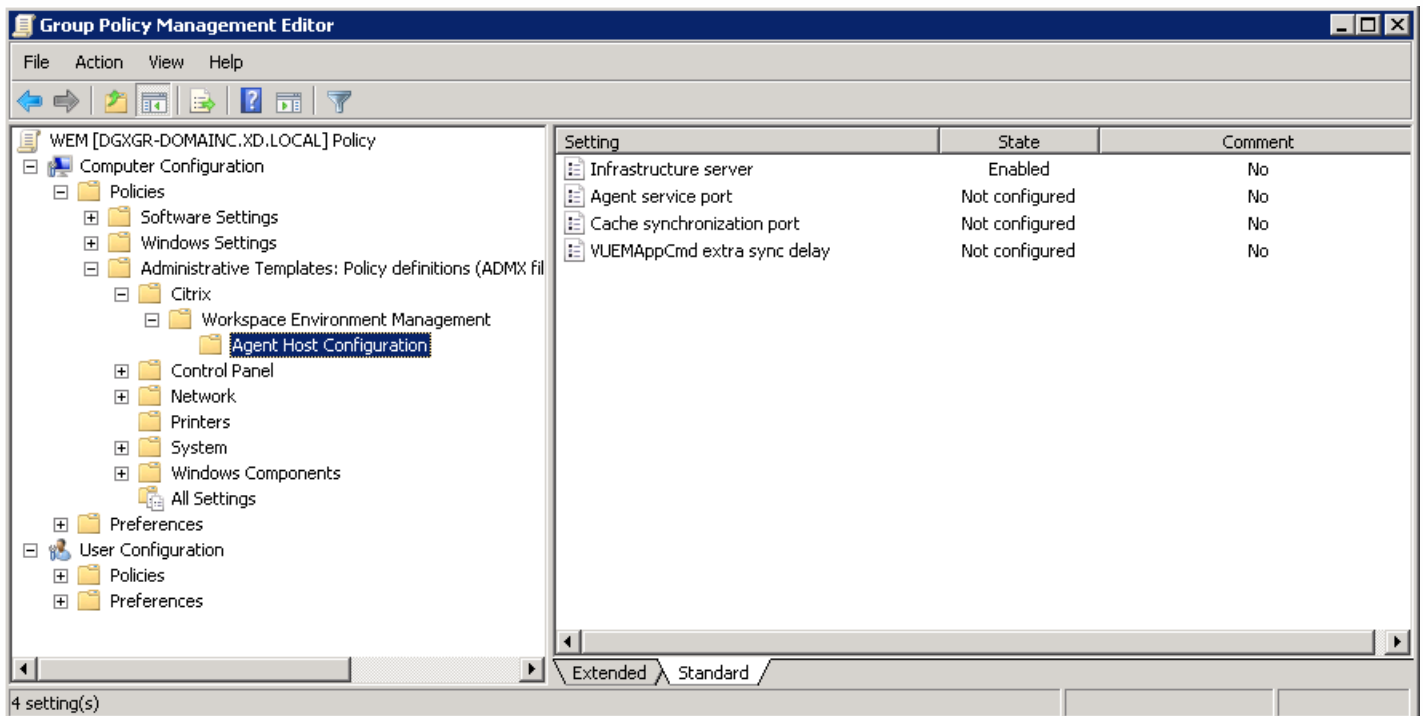
Agent configuration requires administrative access to your Active Directory.

### Prerequisites

To configure the agent, use the **Workspace Environment Management Agent Host Configuration v4.03.00.00.adm** or the **Workspace Environment Management Agent Host Configuration v4.03.00.00.admx** administrative template (provided with Workspace Environment Management).

## Configure group policies

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



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

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

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

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

## Deploy the agent

There is one agent service:

Norskale Agent Host Service (NT SERVICE\Norskale Agent Host Service): Manages WEM Agent. Account: LocalSystem

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

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

The **Citrix Workspace Environment Management Agent Setup** executable acknowledges the following custom arguments:

**WaitForNetwork.** This argument allows you to configure whether the **WaitForNetwork** registry key created during installation is active or not. Accepted values are **0** and **1**. If not specified, the key will not be created during installation.

**SyncForegroundPolicy.** This argument allows you to configure whether the **SyncForegroundPolicy** registry key created during installation is active or not. Accepted values are **0** and **1**. If not specified, the key will not be created during installation.

**GpNetworkStartTimeoutPolicyValue.** This argument allows you to configure the value of the GpNetworkStartTimeoutPolicyValue registry key created during installation, in seconds. By default, this value is 30, but the argument will accept any whole number.

All three keys are created under **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon** during the installation process, and are there to ensure that the user environment receives the infrastructure server address GPOs before logon. In network environments where the Active Directory or Domain Controller servers are slow to respond, this may lead to additional processing time prior to the login screen being displayed. Microsoft recommend setting the value of the **GpNetworkStartTimeoutPolicyValue** key to a minimum of 30 in order for it to have an impact.

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

**AgentSyncPort:** The agent installer runs a script to open 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 8285 is used. Accepted values are any valid port.

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

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

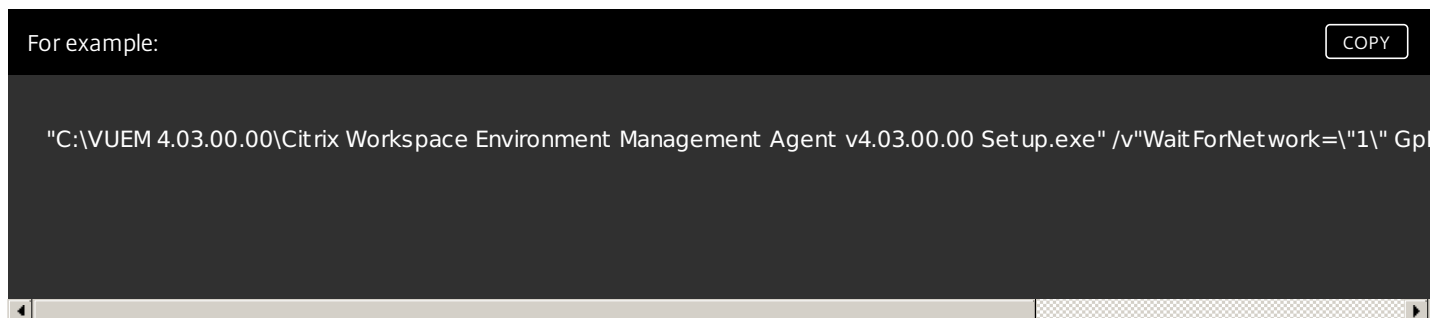
**ARPSYSTEMCOMPONENT.** This argument allows you to designate the agent as a system component, which prevents it from appearing in Add/Remove Programs. Accepted values are 0 or 1.

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

**AgentServiceUseNonPersistentCompliantHistory.** This argument allows you to specify the value of the associated registry setting. If configured, the agent service process optimisation history is saved externally to an XML file in the same location as the agent local cache (by default, the agent installation directory, or the location configured via **AgentCacheAlternateLocation**) rather than in the machine registry. Accepted value is 1.

The syntax for these install arguments is as follows:

```
"path:\to\Citrix Workspace Environment Management Agent v4.03.00.00 Setup.exe"  
/v"argument=\"value\""
```



## Build the agent service cache

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

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

**-help:** display a list of allowed arguments.

**-refreshcache** or **-r**: trigger a cache build or refresh.

# Upgrade a deployment

May 22, 2017

## Introduction

You can upgrade certain deployments to newer versions without having to first set up new machines or Sites; this is called an in-place upgrade. You can upgrade:

- From Workspace Experience Manager version 4.2 to the latest released (current) version
- From Workspace Experience Manager version 4.1 to the latest released (current) version
- From Workspace Experience Manager version 4.0 to the latest released (current) version

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

1. [Infrastructure services](#)
2. [Database](#)
3. [Administration console](#)
4. [Agent](#)

## Step 1: Upgrade the infrastructure services

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

**Note:** Remember to reconfigure the Workspace Environment Management infrastructure services after the database upgrade completes.

## 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.

To upgrade the database, use the Norskale Database Management Utility. This utility 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>Database Management>Database**

## Management Utility.

### 2. Click **Upgrade Database**.

The screenshot shows a 'New Database Upgrade' dialog box with the following fields and options:

- Database Information:**
  - Server and Instance Name: SQL
  - Database Name: Workspace Environment Management
  - Broker uses Windows Authentication
  - Account Name: [Empty] [Select]
- Database Credentials:**
  - Use Integrated Connection (Windows Credentials)
  - Login: [Empty]
  - Password: [Empty]  Display Password
- Actions:**
  - [Upgrade] [Cancel]

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

**Database name.** Name of the database to be upgraded.

#### **Infrastructure service uses Windows authentication.**

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

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

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

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

If there are errors during the database upgrade, please check the **VUEM Database Management Utility Log** file in your

## Step 3: Upgrade the administration console

### Note

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

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

## Step 4: Upgrade the agent

### Note

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

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

After upgrading the agent (via installer or private patch) run the following two commands to ensure that the Agent **.dll** files are correctly precompiled:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe update
```

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe eqi 3
```

(Please note that for 32-bit operating systems, the path is instead

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe).
```

By design, agents are backward-compatible within the same major release version.

# Use the administration console

May 22, 2017

## Start the administration console

1. From the **Start** menu use the **Administration Console** shortcut. By default, the administration console launches in a disconnected state.
2. In the administration console ribbon click **Connect**.
3. In the New Infrastructure Server Connection window, enter the address of your infrastructure server and click **Connect**.

## Configure your installation

1. Click on menu items in the lower-left-hand pane to display their sub-sections in the pane above them.
2. Click on sub-section items to populate the main window area with appropriate content.
3. Change configuration as required. See the [user interface reference](#) for information on settings you can use.

# User interface reference

May 22, 2017

This section describes the Workspace Environment Management administration console user interface. Use the contents list to navigate between the following sections of the user interface:

- [Ribbon](#)
- [Actions](#)
- [Filters](#)
- [Assignments](#)
- [System optimization](#)
- [Policies and profiles](#)
- [Active Directory Objects](#)
- [Transformer settings](#)
- [Advanced settings](#)
- [Administration](#)
- [Monitoring](#)

# Ribbon

May 22, 2017

The ribbon in the administration console contains the following tabs:

- [Home tab](#)
- [About tab](#)



# Home tab

May 22, 2017

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

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

**Infrastructure server name.** Name of the infrastructure server you wish to connect to.

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

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

**Configuration set.** Allows you to switch from one Workspace Environment Management site (configuration set) to another.

**Create.** Opens up the Create configuration set window.

**Name.** Site (configuration set) name as it will appear in the configuration set list in the Ribbon.

**Description.** Site (configuration set) description as it appears in the site edition window.

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

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

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

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

**Export Actions.** Opens up the **Actions Export Wizard**:

Export Actions	<p><b>Action Types to Export.</b> These checkboxes allow you to select the Action categories you wish to export.</p> <p><b>Export Destination.</b> Allows you to specify the location at which the Action Export files are created.</p>
Action Export Processing	<p><b>Export Actions.</b> Creates the Action Export files in the previously-specified location. Each type of Action is exported as a separate XML file.</p>

**Import Actions.** Opens the **Actions Import Wizard**:

Export File Load	<p><b>Export Folder.</b> Allows you to specify which folder to import exported Actions from.</p> <p><b>Action Type to Import.</b> Allows you to select which type of Actions to import.</p>
Actions Selection	<p>You to search for actions by entering a search string and clicking <b>Find</b>.</p> <p><b>Update Existing Action.</b> Allows you to specify whether or not the Action Import will overwrite existing site Actions with identical names. If unselected, duplicate Actions are not imported.</p>
Actions Import Processing	<p><b>Import Actions.</b> Starts the import.</p>

**Export Settings.** Opens up the Settings Export wizard.

Export Settings	<p><b>Setting Types to Export.</b> These checkboxes allow you to select the setting categories you wish to export.</p> <p><b>Export Destination.</b> Allows you to specify the location at which the Setting Export files are created.</p>
Settings Export Processing	<p><b>Export Settings.</b> Creates the Settings Export files in the previously-specified location. Each category of settings is exported as a separate XML file. This pane displays the Settings Export log during the export</p>

**Import Settings.** Opens the Setting Import wizard.

Export File Load	<p><b>Export Folder.</b> Allows you to specify which folder to import exported settings from.</p> <p><b>Setting Types to Import.</b> Allows you to select which category of settings to import.</p>
Settings Import Processing	<p><b>Import Settings.</b> Imports the selected setting categories, overwriting current settings.</p>

# About tab

May 22, 2017

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

**Get Help.** Allows you to open the Citrix Product Documentation website in a web browser window.

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

**Auto Admin Logon.** If enabled, the administration console automatically connects to the last infrastructure service it connected to at startup.

**Enable Debug Mode.** Enables verbose logging for the administration console. Logs are created in the root of the current user "Users" folder.

**Console Skin.** Allows you to select from a variety of skins for the administration console only.

**Port Number.** Allows you to customize the port on which the administration console connects to the infrastructure service. This port must match the port configured in the infrastructure services configuration.

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

# Actions

May 22, 2017

These settings create user resources such as network drives or application short cuts.

# Applications

May 22, 2017

Controls the creation of application shortcuts.

## Tip

To use the Workspace Environment Management agent with XenApp XenApp and XenDesktop applications, edit your XenApp application to point to **VUEMAppCmd.exe** (located in the agent installation directory) with the application path as an argument. Then create your shortcuts as normal, either via XenApp or via Workspace Environment Management, by copying the XenApp shortcut details to a new application action in the admin console.

## 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**.

General tab	<p><b>Name.</b> The display name of the application shortcut, as it appears in the application list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Command Line.</b> The path to the application executable as the client machine will see it. The <b>Browse</b> button allows you to browse to the executable if it is installed locally.</p> <p><b>Working Directory.</b> The shortcut working directory. Automatically filled out if you browse to the executable.</p> <p><b>Parameters.</b> Allows you to specify any launch parameters for the application.</p> <p><b>Start Menu Integration.</b> Allows you to select a specific path in the Start Menu. By default, a new shortcut is created in Programs.</p>
	<p><b>Select Icon.</b> Allows you to browse to an icon file and select an icon for your application. By default, this uses the application executable's icon but you can select any valid icon. Icons are stored in the database as text.</p> <p><b>High Resolution Icons Only.</b> Only displays HD icons in the selection box.</p> <p><b>Application State.</b> Controls whether the application shortcut is enabled or not. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>Maintenance Mode.</b> When active, this will prevent the user from running the application shortcut. The shortcut icon is modified to include a warning sign to denote that the icon is not available, and the user will</p>

Options tab	<p>receive a short message informing them the application is unavailable if they try to launch it. This allows you to proactively manage scenarios where published applications are in maintenance without having to disable or delete application shortcut resources.</p> <p><b>Display Name.</b> The name of the shortcut as it will appear in the user's environment.</p> <p><b>Window Style.</b> This controls what state the application starts in (minimized, maximized, or normal).</p> <p><b>Self-Service Display.</b> If selected, the resource will not be shown in the Workspace Environment Management agent self-service window.</p> <p><b>Hotkey.</b> Allows you to specify a hotkey for the user to launch the application with. Hotkeys are case sensitive and are entered in the following format (e.g.): <b>Ctrl + Alt + S</b>.</p> <p><b>Action Type.</b> Describes what type of action this resource is.</p>
Advanced Settings tab	<p><b>Enable Automatic Self-Healing.</b> When selected, application shortcuts will automatically be recreated by the agent at refresh if they have been moved or deleted by the user.</p> <p><b>Enforce Icon Location.</b> Allows you to specify the exact location of the application shortcut on the user's desktop. Values are in pixels.</p> <p><b>Application Type.</b> Controls the type of application that this shortcut points to. This modifies the settings available on the General tab.</p>

## Start Menu View

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

**Refresh.** Refreshes the application list.

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

**Edit.** Opens up the application edition wizard.

**Delete.** Deletes the selected application shortcut resource.

# Printers

May 22, 2017

This tab controls the mapping of printers.

## Network Printer List

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

### To add a printer

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

General tab	<p><b>Name.</b> The display name of the printer, as it appears in the printer list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Target Path.</b> The path to the printer as it resolves in the user's environment.</p> <p><b>Printer State.</b> Toggles whether the printer is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>External Credentials.</b> Allows you to state specific credentials with which to connect to the printer.</p>
Options tab	<p><b>Self-Healing.</b> Toggles whether the printer is automatically recreated for users when the agent refreshes.</p> <p><b>Action Type.</b> Describes what type of action this resource is. For <b>Use Device Mapping Printers File</b>, specify Target Path as the absolute path to an XML printer list file (see <a href="#">XML printer list configuration</a>). When the agent refreshes it parses this XML file for printers to add to the action queue.</p>

### 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**:

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

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

# Network Drives

May 22, 2017

Controls the mapping of network drives.

## 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**.

Tab	Controls
General	<p><b>Name.</b> The display name of the drive, as it appears in the network drive list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Target Path.</b> The path to the network drive as it resolves in the user's environment. The Browse button allows you to browse to the executable if it is installed locally.</p> <p><b>Network Drive State.</b> Toggles whether the network drive is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>Parameters.</b> Allows you to specify any launch parameters for the application.</p> <p><b>External Credentials.</b> Allows you to state specific credentials with which to connect to the network drive.</p>
Options	<p><b>Enable Automatic Self-Healing.</b> Toggles whether the printer is automatically recreated for your users when the agent refreshes.</p> <p><b>Set as Home Drive.</b></p> <p><b>Action Type.</b> Describes what type of action this resource is. Defaults to Map Network Drive.</p>



# Virtual Drives

May 22, 2017

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

## Virtual Drive List

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

### To add a virtual drive:

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

Tab	Controls
General	<p><b>Name.</b> The display name of the drive, as it appears in the virtual drive list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Target Path.</b> The path to the virtual drive as it resolves in the user's environment.</p> <p><b>Virtual Drive State.</b> Toggles whether the virtual drive is enabled or disabled. When disabled, it will not be processed by the agent even if assigned to a user.</p> <p><b>Parameters.</b> Allows you to specify any launch parameters for the application.</p> <p><b>External Credentials.</b> Allows you to state specific credentials with which to connect to the printer.</p>
Options	<p><b>Action Type.</b> Describes what type of action this resource is.</p>

# Registry Entries

May 22, 2017

Controls the creation of registry entries.

## Registry Value List

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

### To add a registry entry:

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

Tab	Controls
General	<p><b>Name.</b> The display name of the registry entry, as it appears in the registry entry list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Registry Value State.</b> 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.</p> <p><b>Target Path.</b> 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 <b>%ComputerName%\HKEY_CURRENT_USER</b> – this is done automatically.</p> <p><b>Target Name.</b> The name of your registry value as it will appear in the registry (e.g. <b>NoNtSecurity</b>).</p> <p><b>Target Type.</b> The type of registry entry that will be created.</p> <p><b>Target Value.</b> The value of the registry entry once created (e.g. <b>0</b> or <b>C:\Program Files</b>)</p> <p><b>Run Once.</b> By default, Workspace Environment Management creates registry entries every time the agent refreshes. Tick this box to make Workspace Environment Management only create the registry entry once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many registry entries assigned to your users.</p>
Options	<p><b>Action Type.</b> Describes what type of action this resource is.</p>

### To import registry files:

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

**Registry File Name.** This field allows you to browse to a **.reg** file containing the registry settings you want

to import into Workspace Environment Management. For best results, the .reg file should be generated from a clean environment that has only the registry settings you wish to import applied to it.

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

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

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

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

## Note

The wizard cannot import registry entries with duplicate names. If your .reg file contains more than one registry entry with the same name (as displayed in the Registry Values List), select one of these entries for import and rename it if you want to import the others.

# Environment Variables

May 22, 2017

Controls the creation of environment variables.

## 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**.

Tab	Controls
General	<p><b>Name.</b> The display name of the variable, as it appears in the environment variable list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Environment Variable State.</b> Toggles whether the environment variable is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>Variable Name.</b> The functional name of the environment variable.</p> <p><b>Variable Value.</b> The environment variable value.</p>
Options	<p><b>Action Type.</b> Describes what type of action this resource is.</p> <p><b>Execution order.</b></p>

# Ports

May 22, 2017

Controls the mapping of ports.

## Ports list

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

### To add a port:

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

Tab	Controls
General	<p><b>Name.</b> The display name of the port, as it appears in the port list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Port State.</b> Toggles whether the port is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>Port Name.</b> The functional name of the port.</p> <p><b>Port Target.</b> The target port.</p>
Options	<p><b>Action Type.</b> Describes what type of action this resource is.</p>

# Ini Files

May 22, 2017

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

## Ini files operation list

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

### To add 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**.

Tab	Controls
General	<p><b>Name.</b> The display name of the <b>.ini</b> file operation, as it appears in the <b>Ini File Operations</b> list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>.ini File Operation State.</b> Toggles whether the <b>.ini</b> file operation is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>Target Path.</b> This specifies the location of the <b>.ini</b> file that will be modified as it resolves in the user's environment.</p> <p><b>Target Section.</b> This specifies which section of the <b>.ini</b> file is targeted by this operation. If you specify a non-existent section, it will be created.</p> <p><b>Target Value Name.</b> This specifies the name of the value that will be added.</p> <p><b>Target Value.</b> This specifies the value itself.</p> <p><b>Run Once.</b> By default, Workspace Environment Management performs a <b>.ini</b> 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 <b>.ini</b> file operations assigned to your users.</p>
Options	<p><b>Action Type.</b> Describes what type of action this resource is.</p>

# External Tasks

May 22, 2017

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

## External task list

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

### To add an external task:

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

Tab	Controls
General	<p><b>Name.</b> The display name of the external task, as it appears in the external task list.</p> <p><b>Name.</b> The display name of the external task, as it appears in the external task list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Target Path.</b> The path to the external task script as it resolves in the user's environment.</p> <p><b>Target Arguments.</b> Allows you to specify any launch parameters or arguments.</p> <p><b>External Task State.</b> Toggles whether the external task is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>Run Hidden.</b> If selected, the external task runs in the background and is not shown to the user.</p> <p><b>Run Once.</b> By default, Workspace Environment Management runs an external task every time the agent refreshes. Tick this box to make Workspace Environment Management only run the external task once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many external tasks assigned to your users.</p> <p><b>Wait for Task Completion.</b> This toggles whether or not the agent waits for the external task to complete. The Timeout value controls the maximum wait time.</p> <p><b>Execute Only at Logon.</b> If selected, the external task will only be run at logon rather than during every single refresh.</p> <p><b>External Task Execution Order.</b> This allows you to specify a priority for each individual external task, in case multiple tasks are assigned to one user and some tasks rely on results from others to run successfully.</p>
Options	<p><b>Action Type.</b> Describes what type of action this resource is.</p>

# File System Operations

May 22, 2017

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

## File system operations list

A list of your existing file/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**.

Tab	Controls
General	<p><b>Name.</b> The display name of the file/folder operation, as it appears in the list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>Filesystem Operation State.</b> Toggles whether the file system operation is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>Source Path.</b> The path to the source file or folder that is copied.</p> <p><b>Target Path.</b> The destination path for the source file or folder that is copied.</p> <p><b>Overwrite Target if Existing.</b> Toggles whether the file/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.</p> <p><b>Run Once.</b> By default, Workspace Environment Management runs a file system operation every time the agent refreshes. Tick this box to make Workspace Environment Management only run the operation once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many file system operations assigned to your users.</p>
Options	<p><b>Action Type.</b> Describes what type of action this file/folder action is: <b>Copy, Delete, Move, Rename</b> or <b>Symbolic Link</b> operation. Please note that for symbolic link creation, you will need to give users the <b>SeCreateSymbolicLinkPrivilege</b> privilege for Windows to allow symbolic link creation.</p>



# User DSN

May 22, 2017

Controls the creation of user DSNs.

## User DSN list

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

### 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**.

Tab	Controls
General	<p><b>Name.</b> The display name of the user DSN, as it appears in the user DSN list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>User DSN State.</b> 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.</p> <p><b>DSN Name.</b> The functional name of the user DSN.</p> <p><b>Driver.</b> The DSN driver. At present, only SQL server DSNs are supported.</p> <p><b>Server Name.</b> The name of the SQL server to which the user DSN is connecting.</p> <p><b>Database Name.</b> The name of the SQL database to which the user DSN is connecting.</p>
Options	<p><b>Connect Using Specific Credentials.</b> Allows you to specify credentials with which to connect to the server/database.</p> <p><b>Run Once.</b> 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.</p> <p><b>Action Type.</b> Describes what type of action this resource is.</p>

# File Associations

May 22, 2017

Controls the creation of file associations in the user environment.

## File association list

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

### To add a file association:

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

Tab	Controls
General	<p><b>Name.</b> The display name of the file association, as it appears in the file association list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the resource.</p> <p><b>File Association State.</b> Toggles whether the file association is enabled or disabled. When disabled, it is not processed by the agent even if assigned to a user.</p> <p><b>File Extension.</b> Allows you to specify the extension used for this file association.</p> <p><b>ProgID.</b> Allows you to specify the extension <b>ProgID</b>.</p> <p><b>Action.</b> Allows you to select the action type: open, edit or print.</p> <p><b>Target.</b> Allows you to specify the executable used with this file extension.</p> <p><b>Command.</b> Allows you to state any specific commands the executable should follow.</p> <p><b>Set as Default Action.</b> Toggles whether the association is set as a default for that file extension or not.</p> <p><b>Overwrite.</b> Toggles whether or not this file association will overwrite any existing associations for the specified extension.</p> <p><b>Run Once.</b> By default, Workspace Environment Management creates a file association every time the agent refreshes. Tick this box to make Workspace Environment Management only create the file association once, rather than at every refresh. This speeds up the agent refresh process, especially if you have many file associations assigned to your users.</p>
Options	<p><b>Action Type.</b> Describes what type of action this resource is.</p>

# Filters

May 22, 2017

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

- [Rules](#)
- [Conditions](#)

# Rules

May 22, 2017

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

## Filter rule list

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

### To add a filter rule:

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

Tab	Controls
General	<p><b>Name.</b> The display name of the rule, as it appears in the rule list.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the rule.</p> <p><b>Filter Rule State.</b> Toggles whether the rule is enabled or disabled. When disabled, the agent does not process actions using this rule even if they are assigned.</p> <p><b>Available Conditions.</b> These are the <a href="#">filter conditions</a> available to be added to the rule. Note. The <b>DateTime</b> filter expects results in the format: YYYY/MM/DD HH:mm</p> <p>Multiple values can be separated with semicolons (;) and ranges can be separated with hyphens. When specifying a range between two times on the same date, the date should be included in both ends of the range, e.g.: 1969/12/31 09:00-1969/12/31 17:00</p> <p><b>Configured Conditions.</b> These are the conditions already added to the rule.</p> <p>Note: these conditions are <b>AND</b> statements, not <b>OR</b> statements. Adding multiple conditions requires them all to trigger for the filter to be considered triggered.</p>

# Conditions

May 22, 2017

Conditions are specific triggers which allow you to configure the circumstances under which the agent acts to assign a resource to a user.

## Filter condition list

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

### To add a filter condition:

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

Tab	Controls
General	<p><b>Name.</b> The display name of the condition, as it appears in the condition list and in the rule creation/edition wizard.</p> <p><b>Description.</b> This field is only shown in the edition/creation wizard and allows you to specify additional information about the condition.</p> <p><b>Filter Condition State.</b> Toggles whether the filter is enabled or disabled. When disabled, it will not appear in the rule creation/edition wizard.</p> <p><b>Filter Condition Type.</b> The type of filter condition type to use. See <a href="#">Filter conditions</a>. Note: rules using the <b>Always True</b> condition will always trigger.</p> <p><b>Settings.</b> These are the specific settings for individual conditions. See <a href="#">Filter conditions</a>.</p>

## Note

When entering an IP address, you can either specify individual addresses or ranges.

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

# Assignments

May 22, 2017

## Tip

Before assigning actions to users you need to perform the following steps in the order given:

- Configure users, see [Users](#) in Active Directory Objects.
- Define conditions, see [Conditions](#).
- Define filter rules, see [Rules](#).
- Configure actions, see [Actions Assignment](#).

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

### To assign actions to users/groups:

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

# Action Assignment

May 22, 2017

## Configured Users

This is your list of configured users and groups (see [Configured Users](#)). Double-click a user or group to show the assignments menu. You can use **Find** to filter the list by name or ID against a text string.

## Assignments

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

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

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

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

# Modelling Wizard

May 22, 2017

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

Pane	Controls
1	<b>Actions Modelling Target User:</b> You can <b>Select</b> the account name for the user you wish to model.
2	<b>Resultant Actions.</b> The actions assigned to the user (whether individually or to groups the user belongs to). <b>User Groups.</b> The groups the user belongs to.



# System optimization

May 22, 2017

These settings allow you to optimize applications and desktops.

- [Fast Logoff](#)
- [CPU Management](#)
- [Memory Management](#)
- [I/O Management](#)
- [Process Management](#)

# Fast Logoff

May 22, 2017

## Settings

**Enable Fast Logoff.** Enables fast logoff for all users on this site. Fast logoff logs users out instantly while continuing to perform logoff tasks in the background. **Note** Fast Logoff works with XenApp/RDS resources only.

**Exclude Specific Groups.** Allows you to exclude specific groups of users from fast logoff.

# CPU Management

May 22, 2017

These settings allow you to optimize CPU usage.

## CPU Management Settings

These settings control global CPU optimization.

**Enable CPU Spikes Protection.** This setting will prevent all processes from taking more than a percentage of the server's processing power by lowering their priority.

**CPU Usage Limit.** This is the percentage of CPU utilization that will trigger CPU spike protection. Please note that this is a total percentage across all cores.

**Limit Sample Time.** This is the duration over which a process must exceed the CPU Usage Limit for its priority to be lowered.

**Idle Priority Time.** This is the length of time for which the process' priority is lowered.

**Limit CPU/Core Usage.** If enabled, processes that trigger CPU Spike Protection are also confined to the selected number of cores (**CPU/Core Usage Limit**) while Spike Protection is triggered.

**Enable Intelligent CPU Optimization.** If enabled, the agent keeps a list of processes that have triggered spike protection and intelligently optimizes process CPU priority based on that process history. Processes that repeatedly trigger spike protection are assigned lower CPU priority at launch than processes that behave correctly.

**Enable Intelligent I/O Optimization.** If enabled, the agent keeps a list of processes that have triggered spike protection and intelligently optimizes process I/O priority based on that process history. Processes that repeatedly trigger spike protection are assigned lower I/O priority at launch than processes that behave correctly.

**Exclude Specified Processes.** Excludes processes from CPU spike protection by executable name (e.g. notepad.exe).

## CPU Priority

**Enable Process Priority.** If enabled, this allows you to manually set process priority for specified processes.

## CPU Affinity

**Enable Process Affinity.** If enabled, this allows you to manually set process affinity for specified processes.

## CPU Clamping

These settings allow you to forcefully prevent named processes from using more than X% of the CPU. **Note** The clamping percentage is global, not per core (that is, 10% on a quad-core CPU is 10%, not 10% of one core).

**Enable Process Clamping.** Toggles whether process clamping is enabled or not.

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

**Remove.** Deletes the highlighted process from the clamping list.

**Edit.** Allows you to edit the values entered for a given process.



# Memory Management

May 22, 2017

These settings allow you to optimize application memory usage.

**Enable Working Set Optimization.** Toggles whether WSO is enabled or not. When enabled, applications that are idle (have not been interacted with by a user) for a certain time are forced to release excess memory until they are no longer idle.

**Idle Sample Time.** Time in minutes for which an application must be idle before it is forced to release excess memory.

**Idle State Limit.** The CPU usage threshold under which a process is considered idle.

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

# I/O Management

May 22, 2017

These settings allow you to optimize I/O usage.

## I/O Priority

**Enable Process I/O Priority.** If enabled, this allows you to manually set I/O priority for specified processes.

# Process Management

May 22, 2017

These settings allow you to whitelist or blacklist specific processes.

## Process Management

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

### Note

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

## Process BlackList

These settings allow you to blacklist specific processes.

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

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

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

## Process WhiteList

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

**Enable Process Whitelist.** This enables process whitelisting. Processes must be added by executable name (for example, cmd.exe). **Note** If enabled, **Enable Process Whitelist** automatically blacklists all processes not in the whitelist.

**Exclude Local Administrators.** Excludes local administrator accounts from the process whitelisting (they are able to run all processes).

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

# Policies and profiles

May 22, 2017

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

- [Environmental Settings](#)
- [Microsoft USV Settings](#)
- [Citrix Profile Management Settings](#)
- [VMware Persona settings](#)



# Environmental Settings

May 22, 2017

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

## Start Menu

These options modify the user's Start Menu.

**Process Environmental Settings.** This checkbox toggles whether or not the agent processes environmental settings. If it is cleared, no environmental settings are processed.

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

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

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

## Desktop

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

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

## Windows Explorer

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

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

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

**Restrict Specified Drives.** If enabled, the listed drives are blocked. Neither the user nor their applications can access them.

## Control Panel

**Hide Control Panel.** This option is enabled by default to secure the user environment. If disabled, the user has access to his Windows control panel.

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

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

See [Common Control Panel applets](#) along with their canonical names.

## Known Folders Management

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

SBC/HVD Tuning

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

# Microsoft USV Settings

May 22, 2017

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

## Roaming Profiles Configuration

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

**Process USV Configuration.** Controls whether or not the agent processes USV settings. If it is cleared, no USV settings are processed.

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

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

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

## Roaming Profiles Advanced Configuration

These are the advanced roaming profile optimization options.

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

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

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

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

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

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

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

**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 wish.

**Search Recursion.** Controls how many levels of recursion the user profile search will go through.

## Folders Redirection

**Process Folder Redirection Configuration.** This checkbox toggles whether or not the Agent will process folder redirections. If it is cleared, no folder redirections are processed. Select the options here to controls whether and where the user's folders are redirected.

**Delete Local Redirected Folders.** If enabled, the Agent will delete the local copies of the folders selected for redirection.

# Citrix Profile Management Settings

Jun 20, 2017

These settings control Workspace Environment Management's integration with Citrix User Profile Management (UPM) technology. Workspace Environment Management supports Citrix User Profile Management (UPM) up to and including version 5.7.

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

These settings control the main Citrix Profile Management parameters.

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

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

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

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

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

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

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

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

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

These settings control Profile Management profile handling.

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

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

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

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

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

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

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

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

These options control advanced UPM settings.

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

**Set Directory of MFT cache file.** Allows you to specify the MFT cache file directory.

**Process Internet cookie files on logoff.** If enabled, stale cookies are deleted at logoff.

**Delete redirected folders.** If enabled, will delete local copies of redirected folders.

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

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

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

These options control Profile Management logging.

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

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

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

**Set Path to Log File.** Allows you to specify the location at which the log file will be created.

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.

These options control file system exclusions for Profile Management.

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

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

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

**Profile Cleansing.** Opens the **Profile Cleansing** wizard, which allows you to clean up existing profiles.

**Profiles Root Folder.** This field allows you to specify the root folder of your user profiles. You can also Browse to this folder if you wish.

**Search Recursion.** This setting controls how many levels of recursion the user profile search will go through.

**Scan Profiles Folder.** Will scan the specified folder with the specified recursion settings to find user profiles, then will display all profiles found.

**Cleanse Profiles.** This button will cleanse the selected profiles per the Folder Exclusion settings.

These options control Profile Management synchronization settings.

**Enable Directory Synchronization.** If enabled, the listed folders are synchronized with the profile store at refresh.

**Enable File Mirroring.** If enabled, the listed files are mirrored to the profile store, ensuring users always get the most up-to-date versions of these files.

**Enable Folder Mirroring.** If enabled, the listed folders are mirrored to the profile store, ensuring users always get the most up-to-date versions of these folders.

These options control streamed user profile settings.

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

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

**Set timeout for pending area lock files:** frees up files so they are written back to the user store from the pending area after the specified time, in the event that the user store remains locked when a server becomes unresponsive.

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

These options control cross-platform settings.

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

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

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

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

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



# VMware Persona settings

May 22, 2017

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

These settings control the main Persona parameters.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Active Directory Objects

May 30, 2017

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

## Note

Users, computers, groups and OUs must be added to Workspace Environment Management before the agent manages them.

# Users

May 22, 2017

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

**Name.** The name of the user or group.

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

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

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

# Machines

May 31, 2017

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

## Tip

To check whether agents on these machines are correctly registered with the infrastructure server, see Agents in the [Administration](#) section.

### To add a computer or computer group to the current site (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 site (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, edit any of the following details, then click **OK**.

**Description.** Additional information about the computer or OU.

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

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

# Transformer settings

May 22, 2017

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

- [General](#)
- [Advanced](#)

# General

May 22, 2017

These settings control the appearance and basic settings for Transformer.

**Enable Transformer.** If you enable this option, Agent Hosts connected to this site will automatically go into *kiosk mode*. While in kiosk mode, the Agent Host becomes a web/application launcher which will redirect the user to the configured remote desktop interface. The user environment can be completely locked down and the user only allowed to interact with the Agent. If you disable this option, none of the settings in either the **General** or **Advanced** pages are processed.

**Web Interface URL.** This URL is used as the web frontend for the user's virtual desktop. This should be the access URL for your XenDesktop or XenApp environment,

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

**Enable Window Mode.** If enabled, the Citrix Workspace Environment Management Agent kiosk will start in windowed mode. The user will still be locked out of their Windows environment.

**Allow Language Selection.** If enabled, users are allowed to pick what language the Transformer interface is in.

**Show Navigation Buttons.** If enabled, the "Forward", "Back" and "Home" web navigation buttons display on the Agent kiosk window. "Home" sends users back to the web interface URL defined above.

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

**Show 12 Hour Clock.** By default, the Transformer clock is a 24-hour clock. If enabled, this will instead display a 12-hour clock (AM/PM).

**Enable Application Panel.** If enabled, this will display a panel with the user's applications as assigned in Citrix Workspace Environment Management.

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

**Change Unlock Password.** This option 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 support agents to troubleshoot the user environment without restrictions.

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

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

# Advanced

May 22, 2017

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

**Enable Process Launcher.** If enabled, this option will put the Citrix Workspace Environment Management Agent into process launcher mode. While in process launcher mode, the Citrix Workspace Environment Management Agent will launch the process specified in Process Command Line. If terminated, the process will simply be re-launched.

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

**Process Arguments.** This field 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).

**Fix Browser Rendering.** If enabled, this will force IE to run in IE7 compatibility mode.

**Log Off Screen Redirection.** If enabled, this will automatically redirect the user to the logon page whenever they land on the logoff page.

**Suppress Script Errors.** If enabled, the Agent will suppress any script errors it encounters.

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

**Hide Kiosk While in Citrix Session.** If enabled, the Citrix Workspace Environment Management Agent kiosk is hidden while the user is connected to their Citrix session.

**Always Show Admin Menu.** If enabled, will display the kiosk admin menu at all times – this gives all users access to the kiosk admin menu.

**Hide Taskbar & Start Button.** If enabled, this will hide the user's taskbar and start menu; otherwise, the user will still be able to access their desktop.

**Lock Alt-Tab.** If enabled, this will ignore 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.

**Administration Settings.** By default, the Citrix Workspace Environment Management Agent kiosk mode allows the user to control some aspects of the underlying OS. These options allow you to disable these features.

**Pre-Launch Receiver.** If enabled, the Agent will launch Receiver and wait for it to load before bringing up the kiosk mode window.

**Disable Unlock.** If enabled, the Agent cannot be unlocked via the **Ctrl+Alt+U** unlock shortcut.



**Enable Auto-Logon Mode.** If enabled, users are automatically logged on into the desktop environment by the Agent, bypassing the Windows login screen.

**Log Off Web Portal When Session is Launched.** If enabled, the web frontend specified in the General Settings page is logged off when the user's desktop session is launched.

**End of Session Options.** This allows you to specify which action the Agent should take with the environment it is running in when the user ends their session.

**Shut Down at Specified Time.** If enabled, the Agent will automatically shut off the environment it is running in at the specified local time.

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

# Advanced settings

May 22, 2017

These settings modify how and when the agent processes actions.

# Configuration

May 22, 2017

These options control basic Agent behaviour.

**Agent Actions.** These settings determine whether or not the agent processes actions configured in the [Actions](#) tab. These settings apply at login, automatic refresh, or manual (user or administrator triggered) refresh.

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

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

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

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

**Process Registry Values.** When selected, the agent processes registry entry actions.

**Process Environment Variables.** When selected, the agent processes environment variable actions.

**Process Ports.** When selected, the agent processes port actions.

**Process Ini Files Operations.** When selected, the agent processes .ini file actions.

**Process External Tasks.** When selected, the agent processes external task actions.

**Process File System Operations.** When selected, the file system operation actions.

**Process File Associations.** When selected, the agent processes file association actions.

**Process User DSNs.** When selected, the agent processes user DSN actions.

**Agent Service Actions.** These settings determine when the agent service processes its instructions.

**Launch Agent at Logon.** Determines whether or not the agent runs at logon.

**Launch Agent at Reconnect.** Determines whether or not the agent runs when reconnecting to a published desktop.

**Launch Agent for Admins.** Determines whether agent runs when a user is an administrator.

**Agent Type.** Determines whether the user is presented with a user interface (UI) or not (CMD) when interacting with the Agent.

**Enable (Virtual) Desktop Compatibility.** This setting is necessary for the agent to be launched when the user is logged in to session 1. If you have any users on physical desktops or VDI, select this option.

**Execute only CMD Agent in Published Applications.** If enabled, the agent will launch in command line mode (CMD) when launching a published application, rather than in UI mode. CMD mode displays a command prompt instead of an agent splash screen.

These settings determine whether or not the agent performs an environment cleanup on refresh.

**Shortcut Deletion at Startup.** The agent deletes all shortcuts of the selected type whenever 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.

These options control the agent settings.

**Enable Agent Logging.** Enables the agent log file.

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

**Debug Mode.** This enables verbose logging for the agent.

**Enable Offline Mode.** If this is disabled, the agent does not fall back on its cache if it cannot connect to the infrastructure service. **Note** In order for Offline Mode to work, SQL Server Compact Edition 3.5 SP2 must be installed in the user environment and on the Workspace Environment Management infrastructure server.

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

**Refresh Settings.** If enabled, the agent triggers a Windows refresh when an agent refresh occurs.

**Refresh on Environmental Setting Change.** If enabled, the agent triggers a Windows refresh when an environmental setting is modified.

**Asynchronous Printer Processing.** If enabled, the agent processes printers asynchronously from other actions.

**Asynchronous Network Drive Processing.** If enabled, the agent processes network drives asynchronously from other actions.

**Initial Environment/Desktop Cleanup.** If enabled, the agent cleans up the environment/desktop at first login only.

**Check Application Existence.** If enabled, the agent checks that an application is available to the user/group before creating a shortcut to that application.

**Expand App Variables.** If enabled, variables are expanded by default (see [Environment variables](#) for normal behavior when the agent encounters a variable).

**Enable Cross-Domain User Group Search.** If enabled, the agent queries user groups in all Active Directory domains.

**Note:** This is an extremely time-intensive process which should only be selected if necessary.

**Broker Service Timeout.** The timeout value after which the agent switches to its own cache, when it fails to connect to the infrastructure service. The default value is 2000 milliseconds.

**Directory Services Timeout.** The timeout value for directory services on the Agent Host machine, after which the agent uses its own internal cache of user group associations. The default value is 2000 milliseconds.

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

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

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

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

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

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

**Filter Processing Enforcement.** If enabled, these options will force the Agent Host to re-process filters at every refresh.

These settings configure the Agent Host service.

**Agent Cache Refresh Delay.** This setting controls how long the Agent Host service will wait to refresh its cache.

**SQL Settings Refresh Delay.** This setting controls how long the Agent Host service will wait to refresh its SQL connection settings.

**Agent Extra Launch Delay.** This setting controls how long the Agent Host service will wait to launch the Agent Host executable.

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

**Bypass ie4unit Check.** By default, the Agent Host service will wait for ie4unit to run before launching the Agent Host executable. This setting forces the Agent Host service to not wait for ie4unit.

**Agent Launch Exclusions.** If enabled, the Citrix Workspace Environment Management Agent Host will not be launched for any user belonging to the specified user groups.

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

# UI Agent Personalization

May 22, 2017

These options allow you to personalize the look and feel of the Citrix Workspace Environment Management Agent Host as well as help desk and self-service facilities.

These settings let you customize how the Agent Host looks in the user's environment.

**Custom Background Image Path.** If entered, will display a custom image when the Agent Host launches/refreshes, rather than the Citrix Workspace Environment Management logo. The image used must be accessible from the user environment. It is recommended you use a 400\*200px .bmp file.

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

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

**UI Agent Skin.** Allows you to select from a variety of skins for the UI Agent only.

**Hide Agent Splashscreen.** If enabled, will not show the splash screen when the Agent Host is loading/refreshing. This will only take effect after the Agent Host has refreshed while the setting is enabled.

**Hide Agent Icon in Published Applications.** If enabled, published applications will not show the Citrix Workspace Environment Management Agent icon.

**Hide Agent Splashscreen in Published Applications.** If enabled, the Agent splash screen will not be shown for published apps running through it.

**Only Admins Can Close Agent.** If enabled, non-administrators cannot shut down the Citrix Workspace Environment Management Agent Host.

**Allow Users to Manage Printers.** If enabled, users can access the Citrix Workspace Environment Management Agent Host **Manage Printers** menu to assign a default printer and modify print preferences.

**Allow Users to Manage Applications.** If enabled, users can access the Citrix Workspace Environment Management Agent Host **Manage Applications** menu, which allows them to manage where their application shortcuts are created. Shortcuts created in self-healing mode cannot be deleted using this menu.

**Prevent Admins to Close Agent.** If enabled, administrators cannot shut down the Citrix Workspace Environment Management Agent Host.

**Enable Applications Shortcuts.** If enabled, users can run applications from the Manage Applications menu.

**Disable Administrative Refresh Feedback.** When Administrators force an Agent Host to refresh from the Administration Console, select this option to prevent a notification tooltip appearing in the user environment.

These options control the Agent Host's help desk functionalities.

**Help Link Action.** This field controls what happens when the user clicks on the **Help** command in the Citrix Workspace

Environment Management Agent Host.

**Custom Link Action.** This field controls what happens when the user clicks on the **Support** command in the Citrix Workspace Environment Management Agent Host.

**Enable Screen Capture.** If enabled, users are given the option to open a screen capture utility. This allows the user to screenshot any errors in their environment, which they can then send to your support staff.

**Enable Send to Support Option.** If enabled, the user is able to send screenshots and log files directly to the nominated support email address, with the specified template. This requires a working, configured email client.

**Custom Subject.** If enabled, the support email generated by the Citrix Workspace Environment Management Agent Host screen capture utility is sent with the specified subject.

**Email Template.** This field allows you to specify a template for the support email generated by the Citrix Workspace Environment Management Agent Host screen capture utility. Note You must configure the email template to include useful information.

See [Dynamic tokens](#) for a list of hash-tags which can be used in the email template. **Note** Users are only presented with the option to enter a comment if the **##UserScreenCaptureComment##** hash-tag is included in the email template.

**Use SMTP to Send Email.** If enabled, this will send the support email using SMTP instead of MAPI.

**Test SMTP.** Tests your SMTP settings as entered above to verify that they are correct.

**Shut Down At Specified Time.** If enabled, the Agent Host will automatically shut off the environment it is running in at the specified local time.

**Shut Down When Idle.** If enabled, the Agent Host will automatically shut off the environment it is running in after running idle (no user input) for the specified length of time.

# Administration

May 22, 2017

These settings control administrative functions such as delegation, user statistics, and change logging.



# Administrators

Jun 14, 2017

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

## Configured Administrators List

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

To add an administrator:

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

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

**Description.** Additional information about the user or group.

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

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

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

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

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

**Action Creators** can create and manage actions.

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

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

**Assignment Managers** can assign resources to users or groups.

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

**Policies and Profiles Managers** can manage Policies and Profiles settings.

**Configured Users Managers** can add, edit, and remove users or groups from the configured users list.

Users or groups with assigned actions cannot be edited or deleted by Configured Users Managers.

**Transformer Managers** can manage Transformer settings.

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

**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

May 22, 2017

This page displays statistics about your Workspace Environment Management installation.

## Statistics

This page displays a summary of users whose agent hosts have connected to the database.

**Users Summary.** Displays a count of total users who have reserved a Workspace Environment Management license, for both the current site (configuration set) and all sites (configuration sets). Also displays a count of new users in the last 24 hours and in the last month.

**Users History.** This displays connection information for all the users associated with the current site (configuration set), including the last connection time, the name of the machine from which they last connected and the session agent type (UI or CMD) and version. You can use **Find** to filter the list by name or ID against a text string.

# Agents

May 22, 2017

This page displays statistics about the agents in your Workspace Environment Management installation.

## Statistics

This page displays a summary of the Workspace Environment Management agents recorded in the Workspace Environment Management database.

**Agents Summary.** Displays a count of total agents who have reserved a Workspace Environment Management license, for both the current site (configuration set) and all sites (configuration sets). It also reports agents added in the last 24 hours and in the last month.

**Agents History.** This displays connection information for all agents registered with this site (configuration set), including the last connection time, the name of the device from which they last connected and the agent version. You can use Find to filter the list by name or ID against a text string.

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)**.

## Registrations

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

### Important

Agents must only be registered with one configuration set.

The following information is reported:

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

**State.** Registration status of agent on the agent host computer, indicated by icons and the following description giving more information about registration success or failure:

**Agent is not bound to any site.** The infrastructure server cannot resolve any site (configuration set) for this agent because the agent is not bound to any site (configuration set).

**Agent is bound to one site.** The infrastructure server is sending the necessary machine-dependent settings to the agent for that site (configuration set).

**Agent is bound to multiple sites.** The infrastructure server cannot resolve a site (configuration set) for this agent

because the agent is bound to more than one site (configuration set).

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

May 22, 2017

This tab displays a list of all changes made to the Workspace Environment Management settings in the database. By default, the log is unpopulated until the log is refreshed manually.

**Filtering Options.** These options allow you to filter the log by site (configuration set), and date range.

**Export Log.** Exports the log in XLS format.

**Refresh Log.** Refreshes the log.

**Clear Log.** Clears the log for all configuration sets. *This cannot be undone.* Clearing the log adds one event in the new log indicating this has been done. This option is only available to Global Full Access administrators.

This tab lists all changes made to your Workspace Environment Management agents. The log is unpopulated until you click **Refresh**.

**Filtering Options.** These options allow you to filter the log by site (configuration set), and date range.

**Export Log.** Exports the log in XLS format.

**Refresh Log.** Refreshes the log.

**Clear Log.** Clears the log for all configuration sets. *This cannot be undone.* Clearing the log adds one event in the new log indicating this has been done. This option is only available to Global Full Access administrators.

# Monitoring

May 22, 2017

These pages contain detailed user login and machine boot reports. You can **Export** all reports in various formats.

# Daily Reports

May 22, 2017

**Daily Login Report.** A daily summary of login times across all users connected to this site. You can double-click a category for a detailed view showing individual logon times for each user on each device.

**Daily Boot Report.** A daily summary of boot times across all devices connected to this site. You can double-click a category for a detailed view showing individual boot times for each device.



# User Trends

May 22, 2017

**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

May 22, 2017

**User Report.** This report allows you to view login trends for a single user over the selected period. You can double-click each data point for a detailed view.

**Device Report.** This report allows you to view boot trends for a single device over the selected period. You can double-click each data point for a detailed view.

# Configuration

May 22, 2017

## 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.

# Dynamic tokens

May 22, 2017

## 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:

### String operations

COPY

```
#Left(string,length)#
```

```
#Right(string,length)#
```

```
#Truncate(string,length)#
```

```
&Trim(string)&
```

```
&RemoveSpaces(string)&
```

```
&Expand(string)&
```

```
$Split(string,[splitter],index)$
```

```
#Mid(string,start index)#
```

```
!Mid(string,start index,length)!
```

## Note

All Operators are case sensitive. String operations are also supported with hashtags and Active Directory attributes. In cases where your string operations are nested, **Mid** operations are always performed last.

## Hashtags

Hash-tags are a replacement feature widely in Workspace Environment Management item processing. The following example illustrates how you use hash-tags:

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

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

The following hash-tags have been implemented for general use:

```
Hash tags COPY  
  
##UserName##  
  
##UserProfile##  
  
##FullUserName##  
  
##UserInitials##  
  
##UserAppData##  
  
##UserPersonal##  
  
##UserDocuments##  
  
##UserDesktop##  
  
##UserFavorites##  
  
##UserTemplates##  
  
##UserStartMenu##  
  
##UserStartMenuPrograms##  
  
##ComputerName##  
  
##ClientName##
```

##ClientIPAddress##

##ADSite##

##DefaultRegValue##

##UserLDAPPath##

##VUEMAgentFolder##

##RDSSessionID##

##RDSSessionName##

##ClientRemoteOS##

##ClientOSInfos##

Hash-tag **##UserScreenCaptureComment##** is implemented for use in specific parts of the product. This tag can be included in the Email Template under **Advanced Settings > UI Agent Personalisation > Helpdesk Options**. When included, users are presented with a comment field located below the screen capture in the agent screen capture utility. The comment is included in the support email at the location at which you placed the tag in the email template.

## Note

All Hashtags are case sensitive.

## Active Directory Attributes

To work with Active Directory Attributes, Workspace Environment Management replaces the **[ADAttribute:attrName]** value with the related Active Directory attribute.

For user OU structures, Citrix Workspace Environment Management replaces the **[UserParentOU:level]** value with the related Active Directory OU name.

## Note

All **AD** attributes are case sensitive.



# Common Control Panel applets

May 22, 2017

The following Control Panel applets are common in Windows:

Applet name	Canonical name
Action Center	Microsoft.ActionCenter
Administrative Tools	Microsoft.AdministrativeTools
AutoPlay	Microsoft.AutoPlay
Biometric Devices	Microsoft.BiometricDevices
BitLocker Drive Encryption	Microsoft.BitLockerDriveEncryption
Color Management	Microsoft.ColorManagement
Credential Manager	Microsoft.CredentialManager
Date and Time	Microsoft.DateAndTime
Default Programs	Microsoft.DefaultPrograms
Device Manager	Microsoft.DeviceManager
Devices and Printers	Microsoft.DevicesAndPrinters
Display	Microsoft.Display
Ease of Access Center	Microsoft.EaseOfAccessCenter
Family Safety	Microsoft.ParentalControls
File History	Microsoft.FileHistory
Folder Options	Microsoft.FolderOptions



Fonts	Microsoft.Fonts
HomeGroup	Microsoft.HomeGroup
Indexing Options	Microsoft.IndexingOptions
Infrared	Microsoft.Infrared
Internet Options	Microsoft.InternetOptions
iSCSI Initiator	Microsoft.iSCSIInitiator
iSNS Server	Microsoft.iSNSServer
Keyboard	Microsoft.Keyboard
Language	Microsoft.Language
Location Settings	Microsoft.LocationSettings
Mouse	Microsoft.Mouse
MPIOConfiguration	Microsoft.MPIOConfiguration
Network and Sharing Center	Microsoft.NetworkAndSharingCenter
Notification Area Icons	Microsoft.NotificationAreaIcons
Pen and Touch	Microsoft.PenAndTouch
Personalization	Microsoft.Personalization
Phone and Modem	Microsoft.PhoneAndModem
Power Options	Microsoft.PowerOptions
Programs and Features	Microsoft.ProgramsAndFeatures

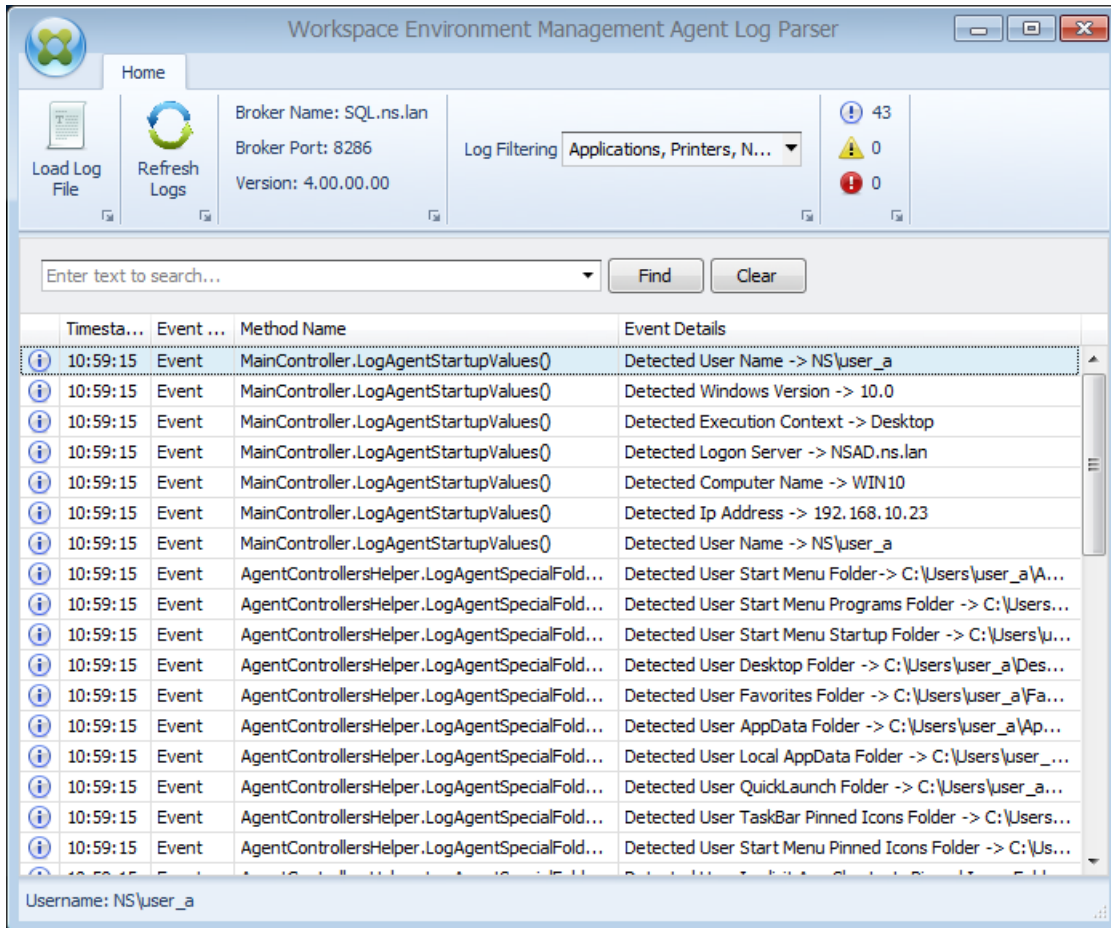
Recovery	Microsoft.Recovery
Region	Microsoft.RegionAndLanguage
RemoteApp and Desktop Connections	Microsoft.RemoteAppAndDesktopConnections
Sound	Microsoft.Sound
Speech Recognition	Microsoft.SpeechRecognition
Storage Spaces	Microsoft.StorageSpaces
Sync Center	Microsoft.SyncCenter
System	Microsoft.System
Tablet PC Settings	Microsoft.TabletPCSettings
Taskbar and Navigation	Microsoft.Taskbar
Troubleshooting	Microsoft.Troubleshooting
TSAppInstall	Microsoft.TSAppInstall
User Accounts	Microsoft.UserAccounts
Windows Anytime Upgrade	Microsoft.WindowsAnytimeUpgrade
Windows Defender	Microsoft.WindowsDefender
Windows Firewall	Microsoft.WindowsFirewall
Windows Mobility Center	Microsoft.MobilityCenter
Windows To Go	Microsoft.PortableWorkspaceCreator
Windows Update	Microsoft.WindowsUpdate



# Log parser

May 22, 2017

Workspace Environment Management includes a log parser application which is located in the agent installation directory:



The **Log Parser** allows you to open any Workspace Environment Management agent log file, making them searchable and filterable. The parser also summarizes the total number of events, warnings and exceptions (in the top right of the ribbon), as well as details about the log file (the name and port of the infrastructure service it first connected to, as well as the agent version and username).

# XML printer list configuration

May 22, 2017

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 COPY
<?xml version="1.0" encoding="UTF-8"?>
  <ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  ...
  </ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

Every client and associated device is represented by an object of the following type:

```
XML COPY
SerializableKeyValuePair<string, List<VUEMUserAssignedPrinter>>>
```

Each device is represented like this:

```
xml COPY
```

```
<SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>  
  
  <Key>DEVICE1</Key>  
  
  <Value>  
  
    <VUEMUserAssignedPrinter>  
  
      ...  
  
    </VUEMUserAssignedPrinter>  
  
  </Value>  
  
</SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

Each block of devices must be matched to a specific client or computer name. The **<Key>** tag contains the relevant name. The **<Value>** tag contains a list of **VUEMUserAssignedPrinter** objects matching the printers assigned to the specified client.

xml

COPY

```

<?xml version="1.0" encoding="utf-8"?>

<ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter xmlns:xsi="http://www.w3.org/2001/XMLSchema-i

  <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

    <Key>DEVICE1</Key>

    <Value>

      <VUEMUserAssignedPrinter>

        ...

      </VUEMUserAssignedPrinter>

    </Value>

  </SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

</ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>

```

## VUEMUserAssignedPrinter tag syntax

Each configured printer must be defined in a **<VUEMUserAssignedPrinter>** tag, using the following attributes:

**<IdPrinter>**. This is the Workspace Environment Management printer ID for the configured printer. Each printer must have a different ID. **Note** The XML Printer List action configured in the Workspace Environment Management Administration Console is also a printer action with its own ID which must be different from the ID of printers individually configured in the XML list.

**<IdSite>**. Contains the site ID for the relevant Workspace Environment Management site, which must match the ID of an existing site.

**<State>**. Specifies the state of the printer where 1 is active and 0 is disabled.

**<ActionType>**. Must always be 0.

**<UseExt Credentials>**. Must be 0. The use of specific Windows credentials is not currently supported.

**<isDefault>**. If 1, printer is the default Windows printer. If 0, it is not configured as default.

**<IdFilterRule>**. Must always be 1.

**<RevisionId>**. Must always be 1. If printer properties are subsequently modified, increment this value by 1 to notify the Agent Host and ensure the printer action is re-processed.

**<Name>**. This is the printer name as perceived by the Workspace Environment Management Agent Host. This field **cannot**

be left blank.

**<Description>**. This is the printer description as perceived by the Workspace Environment Management Agent Host. This field can be blank.

**<DisplayName>**. This is unused and should be left blank.

**<TargetPath>**. This is the UNC path to the printer.

**<ExtLogin>**. Contains the name of the Windows account used when specifying Windows credentials for connection. [Currently unsupported. Leave this field blank].

**<ExtPassword>**. Contains the password for the Windows account used when specifying Windows credentials for connection. [Currently unsupported. Leave this field blank].

**<Reserved01>**. This contains advanced settings. **Do not** alter it in any way.

```
<Reserved01>
<Name>SelfHealingEnabled</Name>
<Value>0</Value>
<Name>SelfHealingEnabled</Name>
<Value>0</Value>
```

To activate self-healing for a given printer object, simply copy and paste the above contents, changing the highlight **0** value to **1**.

## Example printer object

The following example assigns two active printers on the client or computer **DEVICE1**:

- **HP LaserJet 2200 Series** on UNC path `\\server.example.net\HP LaserJet 2200 Series` (default printer)
- **Canon C5531i Series** printer on UNC path `\\server.example.net\Canon C5531i Series`

It also assigns one active printer on the client or computer **DEVICE2**:

- **HP LaserJet 2200 Series** on UNC path `\\server.example.net\HP LaserJet 2200 Series`

```
xml
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter xmlns:xsi="http://www.w3.org/2001/XMLSchema-i
  <SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
    <Key>DEVICE1</Key>
    <Value>
      <VUEMUserAssignedPrinter>
```



```

</VUEMUserAssignedPrinter>
  <IdPrinter>1</IdPrinter>
  <IdSite>1</IdSite>
  <State>1</State>
  <ActionType>0</ActionType>
  <UseExtCredentials>0</UseExtCredentials>
  <isDefault>1</isDefault>
  <IdFilterRule>1</IdFilterRule>
  <RevisionId>1</RevisionId>
  <Name>HP LaserJet 2200 Series</Name>
  <Description />
  <DisplayName />
  <TargetPath>\\server.example.net\HP LaserJet 2200 Series</TargetPath>
  <ExtLogin />
  <ExtPassword />
  <Reserved01>&lt;?xml version="1.0" encoding="utf-8"?&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:xsi="f
</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="f

</VUEMUserAssignedPrinter>

</Value>

<Key>DEVICE2</Key>

<Value>

  <VUEMUserAssignedPrinter>

    <IdPrinter>1</IdPrinter>

    <IdSite>1</IdSite>

    <State>1</State>

    <ActionType>0</ActionType>

    <UseExtCredentials>0</UseExtCredentials>

    <isDefault>0</isDefault>

    <IdFilterRule>1</IdFilterRule>

    <RevisionId>1</RevisionId>

    <Name>HP LaserJet 2200 Series</Name>

    <Description />

    <DisplayName />

    <TargetPath>\\server.example.net\HP LaserJet 2200 Series</TargetPath>

    <ExtLogin />

```

```
<Ext Password />
```

```
<Reserved01>&lt;?xml version="1.0" encoding="utf-8"?&gt;&lt;ArrayOfVUEMActionAdvancedOption xmlns:xsi="f
```

```
</VUEMUserAssignedPrinter>
```

```
</Value></SerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

```
</ArrayOfSerializableKeyValuePairOfStringListOfVUEMUserAssignedPrinter>
```

# Filter conditions

May 22, 2017

Workspace Environment Management includes the following filter conditions which you use to configure the circumstances under which the agent assigns resources to users. (For details of using these conditions in the administration console, see [filter conditions](#).)

Condition Name	<b>Always True</b>
Expected value type	N/A
Expected result type	N/A
Expected syntax	N/A
Returns	true

Condition Name	<b>ComputerName Match</b>
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	<b>ClientName Match</b>
Expected value type	N/A
Expected value type	String

Expected syntax	<p>Single name test : Clientname</p> <p>Multiple tests (OR) : Clientname1;Clientname2</p> <p>Wildcard (also works with multiples) : ClientName*</p>
Returns	True if the current client name matches the tested value false otherwise

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

Condition Name	<b>Client IP Address Match</b>
Expected value type	N/A
Expected result type	IP address
Expected syntax	<p>Single name test : ClientIpAddress</p> <p>Multiple tests (OR) : ClientIpAddress1;ClientIpAddress2</p> <p>Wildcard (also works with multiples) : ClientIpAddress*</p> <p>Range (also works with multiples) : IpAddress1-IpAddress2</p>

Returns	True if the current client ip address matches the tested value false otherwise
---------	--

Condition Name	<b>Active Directory Site Match</b>
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	<b>Scheduling</b>
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	<b>Environment Variable Match</b>
Expected value type	String. Name of the tested variable
Expected result type	String. Expected value of the tested variable
Expected syntax	Single name test : value Not null test: ?

Returns	True if environment variable exists and value matches false otherwise.
---------	--

Condition Name	<b>Registry Value Match</b>
Expected value type	String. Full path and name of the registry value to test. Example : Registry Key <b>HKCU\Software\Citrix\TestValueName</b>
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	<b>WMI Query result Match</b>
Expected value type	N/A
Expected result type	String.
Expected syntax	Valid WMI query. <a href="https://msdn.microsoft.com/en-us/library/aa392902(v=vs.85).aspx">https://msdn.microsoft.com/en-us/library/aa392902(v=vs.85).aspx</a>
Returns	True if query is successful and has result false otherwise.

Condition Name	<b>User Country Match</b>
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	<b>User UI Language Match</b>
Expected value type	N/A
Expected result type	String. Two letter ISO language name. Example FR
Expected syntax	Two letter ISO language name. Example FR
Returns	True if user UI ISO language name matches the specified value false otherwise.

Condition Name	<b>User SBC Resource Type</b>
Expected value type	N/A
Expected result type	Select from dropbox
Expected syntax	N/A
Returns	True if user context (published desktop or application) matches selected value false otherwise.

Condition Name	<b>OS Platform Type</b>
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 selected value false otherwise.



Condition Name	<b>Connection State</b>
Expected value type	N/A
Expected result type	Select from dropbox
Expected syntax	N/A
Returns	True if connection state (online or offline) matches selected value false otherwise.

Condition Name	<b>XenApp Version Match</b>
Expected value type	N/A
Expected result type	String. XenApp Version. Example: 6.5
Expected syntax	N/A
Returns	True if version matches selected value false otherwise.

Condition Name	<b>XenApp Farm Name Match</b>
Expected value type	N/A
Expected result type	String. XenApp Farm Name (up to version 6.5). Example: Farm
Expected syntax	N/A
Returns	True if name matches selected value false otherwise.

Condition Name	<b>XenApp Zone Name Match</b>
Expected value type	N/A
Expected result type	String. XenApp Zone Name (up to version 6.5). Example: Zone
Expected syntax	N/A
Returns	True if name matches selected value false otherwise.

Condition Name	<b>XenDesktop Farm Name Match</b>
Expected value type	N/A
Expected result type	String. XenDesktop Farm Name (up to version 5). Example: Farm
Expected syntax	N/A
Returns	True if name matches selected value false otherwise.

Condition Name	<b>XenDesktop Desktop Group Name Match</b>
Expected value type	N/A
Expected result type	String. XenDesktop Desktop Group Example: Group
Expected syntax	N/A
Returns	True if name matches selected value false otherwise.

Condition Name	<b>Provisioning Services Image Mode</b>

Expected value type	N/A
Expected result type	Select from dropbox
Expected syntax	N/A
Returns	True if current provisioning services image mode matches selected value false otherwise.

Condition Name	<b>Client OS</b>
Expected value type	N/A
Expected result type	Select from dropbox
Expected syntax	N/A
Returns	True if current client operating system matches selected value false otherwise.

Condition Name	<b>Active Directory Path Match</b>
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 Wilcard test: OU=Users* Multiple entries: separate entries with semicolon (;)
Returns	True if attribute exists and value matches false otherwise.

Condition Name	<b>Active Directory Attribute Match</b>
----------------	---

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 value matches false otherwise.

Condition Name	<b>Name or Value is in List</b>
Expected value type	String. Full file path of the xml list generated by the Integrity List manager utility
Expected result type	String. Expected value of the name/value to look for in the list
Expected syntax	String
Returns	True if the value is found in the name/value pairs in the specified list false otherwise.

Condition Name	<b>No ComputerName Match</b>
Negative condition behavior	Will execute <b>ComputerName Match</b> and return the opposite result (true if false, false if true).  See condition <b>ComputerName Match</b> for more information.

Condition Name	<b>No ClientName Match</b>
Negative condition behavior	Will execute ClientName Match and return the opposite result (true if false, false if true).

See condition **ClientName Match** for more information.

Condition Name	<b>No IP Address Match</b>
Negative condition behavior	Will execute IP Address Match and return the opposite result (true if false, false if true).  See condition <b>IP Address Match</b> for more information.

Condition Name	<b>No Client IP Address Match</b>
Negative condition behavior	Will execute Client IP Address Match and return the opposite result (true if false, false if true).  See condition <b>Client IP Address Match</b> for more information.

Condition Name	<b>No Active Directory Site Match</b>
Negative condition behavior	Will execute Active Directory Site Match and return the opposite result (true if false, false if true).  See condition <b>Active Directory Site Match</b> for more information.

Condition Name	<b>No Environment Variable Match</b>
Negative condition behavior	Will execute Environment Variable Match and return the opposite result (true if false, false if true).

See condition **Environment Variable Match** for more information.

Condition Name	<b>No Registry Value Match</b>
Negative condition behavior	Will execute Registry Value Match and return the opposite result (true if false, false if true).  See condition <b>Registry Value Match</b> for more information.

Condition Name	<b>No WMI Query result Match</b>
Negative condition behavior	Will execute WMI Query result Match and return the opposite result (true if false, false if true).  See condition <b>WMI Query result Match</b> for more information.

Condition Name	<b>No User Country Match</b>
Negative condition behavior	Will execute User Country Match and return the opposite result (true if false, false if true).  See condition <b>User Country Match</b> for more information.

Condition Name	<b>No User UI Language Match</b>
Negative condition behavior	Will execute User UI Language Match and return the opposite result (true if false, false if true).

See condition **User UI Language Match** for more information.

Condition Name	<b>No XenApp Version Match</b>
Negative condition behavior	Will execute XenApp Version Match and return the opposite result (true if false, false if true).  See condition <b>XenApp Version Match</b> for more information.

Condition Name	<b>No XenApp Farm Name Match</b>
Negative condition behavior	Will execute XenApp Farm Name Match and return the opposite result (true if false, false if true).  See condition <b>XenApp Farm Name Match</b> for more information.

Condition Name	<b>No XenApp Zone Name Match</b>
Negative condition behavior	Will execute XenApp Zone Name Match and return the opposite result (true if false, false if true).  See condition <b>XenApp Zone Name Match</b> for more information.

Condition Name	<b>No XenDesktop Farm Name Match</b>
Negative condition behavior	Will execute XenDesktop Farm Name Match and return the opposite result (true if false, false if true).

See condition **XenDesktop Farm Name Match** for more information.

Condition Name	<b>No XenDesktop Desktop Group Name Match</b>
Negative condition behavior	Will execute XenDesktop Desktop Group Name Match and return the opposite result (true if false, false if true).  See condition <b>XenDesktop Desktop Group Name Match</b> for more information.

Condition Name	<b>No Active Directory Path Match</b>
Negative condition behavior	Will execute Active Directory Path Match and return the opposite result (true if false, false if true).  See condition <b>Active Directory Path Match</b> for more information.

Condition Name	<b>No Active Directory Attribute Match</b>
Negative condition behavior	Will execute Active Attribute Path Match and return the opposite result (true if false, false if true).  See condition <b>Active Attribute Path Match</b> for more information.

Condition Name	<b>Name or Value is not in List</b>
Negative condition behavior	Will execute Name or Value is in List and return the opposite result (true if false, false if true).



See condition **Name or Value is in List** for more information.

Condition Name	<b>Client Remote OS Match</b>
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	<b>No Client Remote OS Match</b>
Negative condition behavior	Will execute Client Remote OS Match and return the opposite result (true if false, false if true).  See condition <b>Client Remote OS Match</b> for more information.

Condition Name	<b>Dynamic Value Match</b>
Expected value type	String. Any dynamic expression using environment variables or Dynamic Tokens
Expected result type	String. Expected value of the tested expression
Expected syntax	Single name test : value  Not null test: ?
Returns	True if dynamic expression result value exists and value matches false otherwise.

Condition Name	<b>No Dynamic Value Match</b>
Negative condition behavior	Will execute Dynamic Value Match and return the opposite result (true if false, false if true).  See condition <b>Dynamic Value Match</b> for more information.

Condition Name	<b>Transformer Mode State</b>
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	<b>No Client OS Match</b>
Negative condition behavior	Will execute Client OS Match and return the opposite result (true if false, false if true).  See condition <b>Client OS Match</b> for more information.

Condition Name	<b>Active Directory Group Match</b>
Expected value type	N/A
Expected result type	String
Expected syntax	Single name test : group netbios name (DOMAIN\Groupname)

	Multiple tests (OR) : Groupname1;Groupname2
Returns	True if any of the current user groups matches the tested value false otherwise

Condition Name	<b>No Active Directory Group Match</b>
Negative condition behavior	Will execute Active Directory Group Match and return the opposite result (true if false, false if true).  See condition <b>Active Directory Group Match</b> for more information.

Condition Name	<b>File Version Match</b>
Expected value type	String. Full path and name of the file to test. Example : <b>C:\Test\TestFile.dll</b>
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	<b>No File Version Match</b>
Negative condition behavior	Will execute File Version Match and return the opposite result (true if false, false if true).  See condition <b>File Version Match</b> for more information.

Condition Name	<b>Network Connection State</b>
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.

Condition Name	<b>Published Resource Name</b>
Expected value type	N/A
Expected result type	String. Name of the published resource (XenApp/XenDesktop/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	<b>Name is in List</b>
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	<b>Name is not in List</b>
Negative condition behavior	Will execute Name is in List and return the opposite result (true if false, false if true).  See condition <b>Name is in List</b> for more information.

Condition Name	<b>File/Folder exists</b>
Expected value type	N/A
Expected result type	String.
Expected syntax	Full path of the file system entry (file or folder) to test
Returns	True if the specified file system entry exists false otherwise

Condition Name	<b>File/Folder does not exist</b>
Negative condition behavior	Will execute File/Folder exists and return the opposite result (true if false, false if true).  See condition <b>File/Folder exists</b> for more information.

Condition Name	<b>DateTime Match</b>
Expected value type	N/A
Expected result type	DateTime as String. Date/time to test
Expected syntax	Single Date: 06/01/2016

	<p>Date Range: 06/01/2016-08/01/2016</p> <p>Multiple entries: entry1;entry2 Ranges and single dates can be mixed</p>
Returns	True if execution datetime matches any of the specified entry false otherwise.

Condition Name	<b>No DateTime Match</b>
Negative condition behavior	<p>Will execute DateTime Match and return the opposite result (true if false, false if true).</p> <p>See condition <b>DateTime Match</b> for more information.</p>

# Glossary

May 30, 2017

This topic contains terms and definitions used in the Workspace Environment Management (WEM) software and documentation.

\* *Replaced at WEM 4.3.*

## **Admin Broker Port\***

Changed to "administration port" at WEM 4.3.

## **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.

## **administration port**

Port on which the administration console connects to the infrastructure service. The port defaults to 8284 and corresponds to the AdminPort command-line argument.

## **agent**

The Workspace Environment Management agent consists of two components: the agent service and the session agent. These components are installed on the agent host.

## **Agent Host executable\***

Changed to "session agent" at WEM 4.3.

## **Agent Host machine\***

Changed to "agent host" at WEM 4.3.

## **Agent Host service\***

Changed to "agent service" at WEM 4.3.

## **Agent Broker Port\***

Changed to "agent service port" at WEM 4.3.

## **Agent Cache Synchronization Port\***

Changed to "cache synchronization port" at WEM 4.3.

## **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**

Listening port on the agent host which receives instructions from the infrastructure service. Used, for example, to force agents to refresh from the administration console. The port default is 49752.

## **agent service**

The service deployed on VDAs or on physical Windows devices in transformer use cases. It is responsible for enforcing the settings you configure using the administration console.

#### **agent service port**

A port on which the agent connects to the infrastructure server. The port defaults to 8286 and corresponds to the AgentPort command-line argument.

#### **Agent Sync Broker Port\***

Changed to "cache synchronization port" at WEM 4.3.

#### **broker\***

Changed to "infrastructure service" at WEM 4.3.

#### **Broker account\***

Changed to "infrastructure service account" at WEM 4.3.

#### **Broker server\***

Changed to "infrastructure server" at WEM 4.3.

#### **Broker Service Account\***

Changed to "infrastructure service account" at WEM 4.3.

#### **cache synchronization port**

A port on which the agent cache synchronization process connects to the infrastructure service to synchronize the agent cache with the infrastructure server. The port defaults to 8285 and corresponds to the AgentSyncPort command-line argument.

#### **Citrix License Server port**

The port on which the Citrix License Server is listening and to which the infrastructure service then connects to validate licensing. The port default is 27000.

#### **configuration set**

A set of Workspace Environment Management configuration settings.

#### **Connection Broker\***

Changed to "infrastructure server" at WEM 4.3.

#### **database**

A database created in an SQL Server instance and containing the Workspace Environment Management configuration settings.

#### **database server account**

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**



The computer on which the Workspace Environment Management infrastructure services are installed.

**Infrastructure Server Administration Port\***

Changed to "administration port" at WEM 4.3.

**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."

**infrastructure service account**

The account which the infrastructure service uses to connect to the database. By default this account is the vuemUser SQL account, but during database creation you can optionally specify other Windows credentials for the infrastructure service to use.

**Infrastructure service server\***

Changed to "infrastructure server" at WEM 4.3.

**infrastructure services**

Services installed on the infrastructure server by the infrastructure services installation process.

**initial administrators group**

A user group which is selected during database creation. Only members of this group have Full Access to all Workspace Environment Management sites in the administration console. By default this group is the only group with this access.

**integrated connection**

Connection of the database creation wizard to the SQL instance using the current Windows account instead of an SQL account.

**kiosk mode**

A mode in which the agent becomes a web or application launcher redirecting users to a single app or desktop experience. This allows administrators to lock down the user environment to a single app or desktop.

**Monitoring Broker Port\***

Changed to "WEM monitoring port" at WEM 4.3.

**mixed-mode authentication**

In SQL Server, an authentication mode that enables both Windows Authentication and SQL Server Authentication. This is the default mechanism by which the infrastructure service connects to the database.

**License server port\***

Changed to "Citrix License Server port" at WEM 4.3.

**network drive**

A physical storage device on a LAN, a server, or a NAS device.

**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\***

Changed to "Configuration set" at WEM 4.3.

### **SQL user account**

An SQL user account with name of "vuemUser" created during installation. This is the default account that the infrastructure service uses to connect to the database.

### **transformer**

A feature in which Workspace Environment Management agents connect in a restricted kiosk mode.

### **virtual drive**

A Windows virtual drive (also called an MS-DOS device name) created using the subst command or the DefineDosDevice function. A virtual drive maps a local file path to a drive letter.

### **virtual IP address (VIP)**

An IP address that does not correspond to an actual physical network interface (port).

### **VUEM**

Virtual User Environment Management. This is a legacy Norskale term that appears in some places in the product.

### **vuemUser**

An SQL account created during Workspace Environment Management database creation. This is the default account that the Workspace Environment Management infrastructure service uses to connect to the database.

### **WEM Broker\***

Changed to "infrastructure service" at WEM 4.3.

### **WEM monitoring port**

A listening port on the infrastructure server used by the monitoring service. The port defaults to 8287. (Not yet implemented.)

### **WEM UI Agent executable\***

Changed to "session agent" at WEM 4.3.

### **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\***

Changed to "Windows authentication" at WEM 4.3.