Personalization Product Guide

Version 2018.1

Contents

Personalization Product Guide **1**
About Environment Manager **5**
Licensing 5
Architecture 7
Console 9
Environment Manager Administrative Tools 17
Service Packs 17
Best Practices for Configuration 19
Wildcards and Regular Expressions 23
Performance Monitor Counters 24
About User Personalization **28**
Designing and Implementing Environment Manager Personalization 29
User Personalization Architecture 30
Configure Personalization Servers 36
Personalization Servers Policy **44**
Configure a Personalization Servers List 44
Personalization Groups **46**
Add a Personalization Group 46
Create Group Personalization Membership Rules 46
User Data Partitioning 48
Personalization Group Arrangement 48
Personalization Group Settings 49
Personalization Group Membership Rules 53
Application Personalization for Personalization Groups 57
Windows Personalization and Personalization Groups 64
Profile Migration 64
Excluded Users 72
Endpoint Self-Service Tool 72
Application Personalization **77**
Application Processing Rules 77
Application Groups 77
Applications 86
Inclusions and Exclusions 91
Application Data Collection **101**
Add New Applications 101
Add Inclusions 101
Windows Personalization **102**
Windows Settings Groups 102
Custom Windows Settings 106
Default Windows Settings Groups 108
Sites **112**
Add a Personalization Site 112

Environment Manager Sites Hierarchy 112
Environment Manager Site Membership Rules 113
Environment Manager Site Conditions 115
Servers and Virtual Hosts 115
Personalization Tools 118
Import and Export Personalization Configurations 118
Global Options 123
Access Rights 123
Advanced Personalization Settings 125
Application Exclusions 132
Data Collection Settings 133
GeoSync 134
Personalization Analysis 154
Generate a Personalization Analysis Report 154
Personalization Analysis and Windows Settings 155
Size and Usage Reports 155
Archive Reports 159
Environment Manager Support Console 162
Support Console Functionality 162
Streamed Applications 163
Citrix XenApp 163
Symantec Virtualization 165
Support for Citrix Offline Plug-in 6.0 166

About Environment Manager

Environment Manager provides on-demand personalization of user desktops on-demand and helps protect endpoints with fine-grained contextual policy control.

Environment Manager Personalization provides:

- Fast logon times
- A fully personalized desktop experience, regardless of location or device
- A secure desktop environment that adapts based on user context

Use Environment Manager Policy to:

- Enforce policy real-time throughout the user session, not just at login
- Help meet corporate and industry-based compliance mandates such as HIPAA, FINRA, and PCI
- Run multiple policies in parallel for the best possible user experience.

Licensing

The Licensing console allows you to manage User Workspace Manager product licenses.

The Licensing console allows you to:

- Manage licenses for single products, the User Workspace Manager Suite and Evaluation licenses.
- Export license packages to MSI or LIC file format for saving to the Management Center or other computers which can be remotely accessed.
- Import and manage licenses from LIC file format.

For information about license deployment to endpoints, see Management Center Help.

Managing Licenses

License details are included in the License Agreement which is issued when an order for ther software has been completed.

The License Agreement includes the following information:

- Product, Feature, and Version Details
- Issue Date
- Expiry Date
- Customer Name
- Serial ID

Together with the license agreement you will receive either a TXT file or a LIC file. Use these in the Licensing Console to add or import the license.

Add a License

1. Open the Licensing console.
2. Click **Add**.

   The Add License Key dialog displays.
3. Enter the License Key and click **Add**.

   If you received a TXT file license, open the file and copy the license key, paste it in to the Add License Key dialog.

   If you received a LIC file license, refer to "Import License Files" on the next page.

Details of the license are displayed in the console and the license key is added to the following location:

%ALLUSERSPROFILE%\AppSense\Licenses

Activate a License

Once added, some licenses require activating.

1. Select a license or add one to the licensing console.
2. Click **Activate**.
3. Type or copy and paste the activation code.
4. Press **Enter** to accept the code.

The license console saves the license key to the MS Windows registry on the local machine. The License Status field updates to show the status of the license and the license details display in the lower part of the console.

To check that the license is active on your endpoint, search the registry for the license code. If the search finds the code, then the license is active.

Remove a License

1. Highlight the required license and click **Remove**.

   A confirmation dialog displays.
2. Click **Yes** to confirm.

The selected license is deleted and removed from the console and the MS Windows registry or %ALLUSERSPROFILE%\AppSense\Licenses location, whichever is applicable to the license type.

Export License Files

Export licenses to an MSI or LIC file to create a backup and enable distribution to other endpoints using the Licensing console or the Management Center.

1. Highlight the license you want to export.
2. Click **Export** to display Windows Save As dialog.
3. Browse to the required location to save the license file.
4. Enter a name for the file.
5. Select the file type: MSI or LIC.
6. Click **Save**.

A file is created and saved in the selected location. This file can be copied to any network location and loaded via the Licensing console or in the Management Center console.

Import License Files

Import a previously exported license to an endpoint using the Licensing console.

1. Open the Licensing console.
2. Click **Import** to display the Windows Open dialog.
3. Navigate to the required LIC file.
4. Click **Open**.

Details of the license are displayed in the console and the license key is added to the following location:

%ALLUSERSPROFILE%\AppSense\Licenses

Troubleshooting

I received a license, what do I do?

If you have received a product license you can load the license by launching the Licensing Console on your client computer and entering the license code.

I have entered a license, but it says it is not activated, why?

Some licenses require activation before they can be used. Activation codes are provided by Ivanti. Activate a license by entering the License and Activation codes into the console.

Architecture

The Environment Manager system consists of the Environment Manager Console, Environment Manager Agent, Personalization Server and Database.

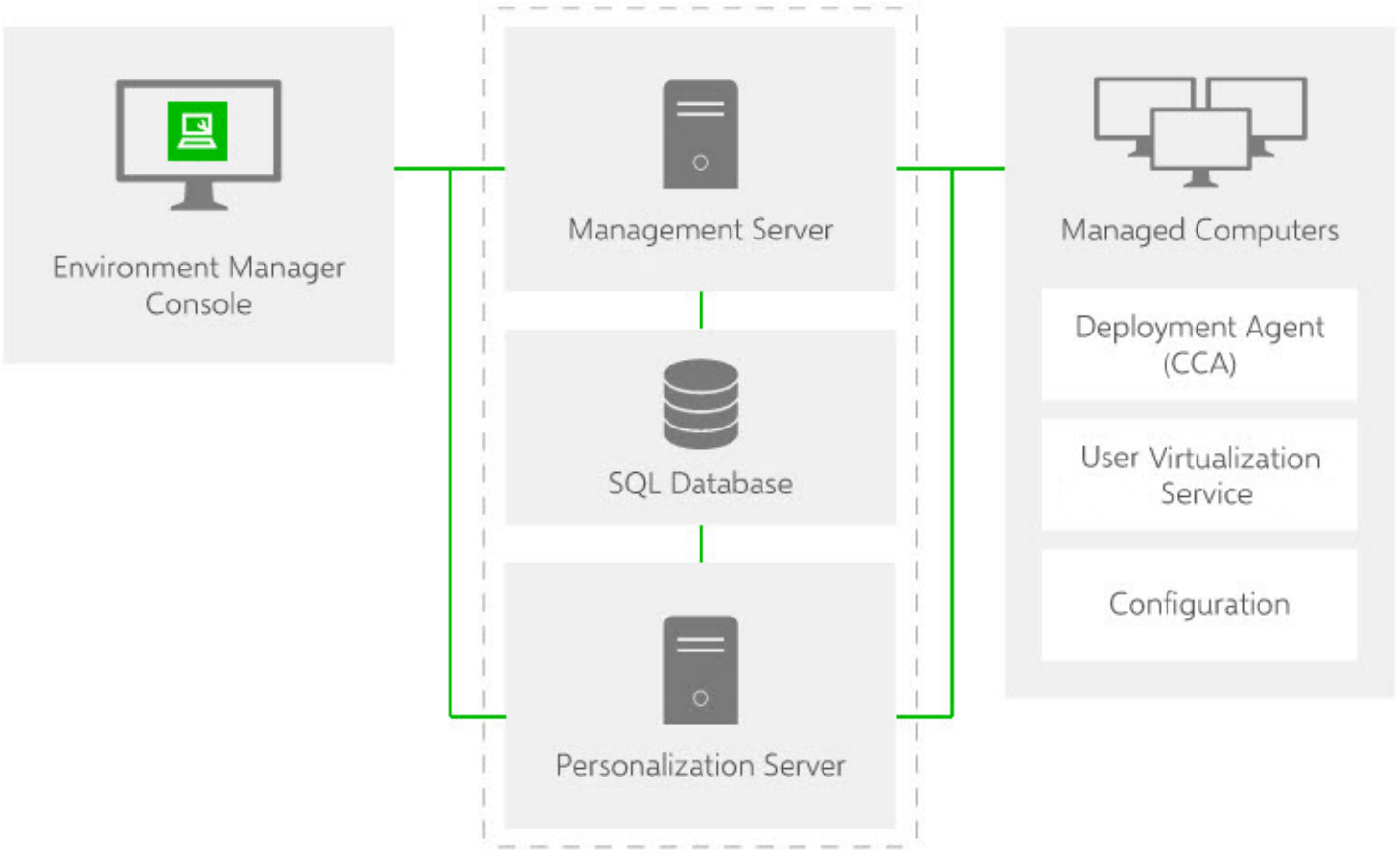
The console is an administrative tool to create and manage configurations. The agent resides on the controlled computers and can receive configurations from the Management Center or third party deployment system to manage the machine and user environment. The console also provides a live connection to the Personalization Database.

The Personalization Server runs as a website, using IIS on either Windows Server 2003 or 2008. Client machines (Tier 1) connect through HTTP(s) handlers, and the Console uses WCF Services.

The Personalization Server acts as a broker between the Client and Database, providing a secure channel to read and write the Personalization data. It is designed to support thousands of users simultaneously and multiple Personalization Servers can be configured in parallel to use a single Database.

Environment Manager can operate either in Standalone or Enterprise mode. In Standalone mode, the console saves its settings directly to the local system. In Enterprise mode, different configurations can be deployed to the controlled computers depending on your system requirements. This help describes the use of Environment Manager in Standalone mode.

For details on centralized management mode please refer to the Management Center Help system.



Policy Configuration and User Personalization work together to provide complementary control of the entire user environment. Inevitably there are some areas of overlap. The profile settings are applied in the following stages:

- Default Settings - Policy Configuration
- Usually occur through the use of mandatory profiles, although Policy Configuration is free to set anything at this stage.
- Virtual Settings - User Personalization
- User specific changes to their own personality settings that are being managed by User Personalization. These are applied on top of the defaults.
- Enforced Settings - Policy Configuration

Any policies that the administrator wants to set regardless of how the user has changed their application previously, so these are applied last. The user may be free to change these whilst the application is running, but they will be reapplied the next time the application runs.

Console

The Environment Manager Console launches from the start menu:

Start > **All Programs** > **AppSense** > **Environment Manager** > **Environment Manager Console**.

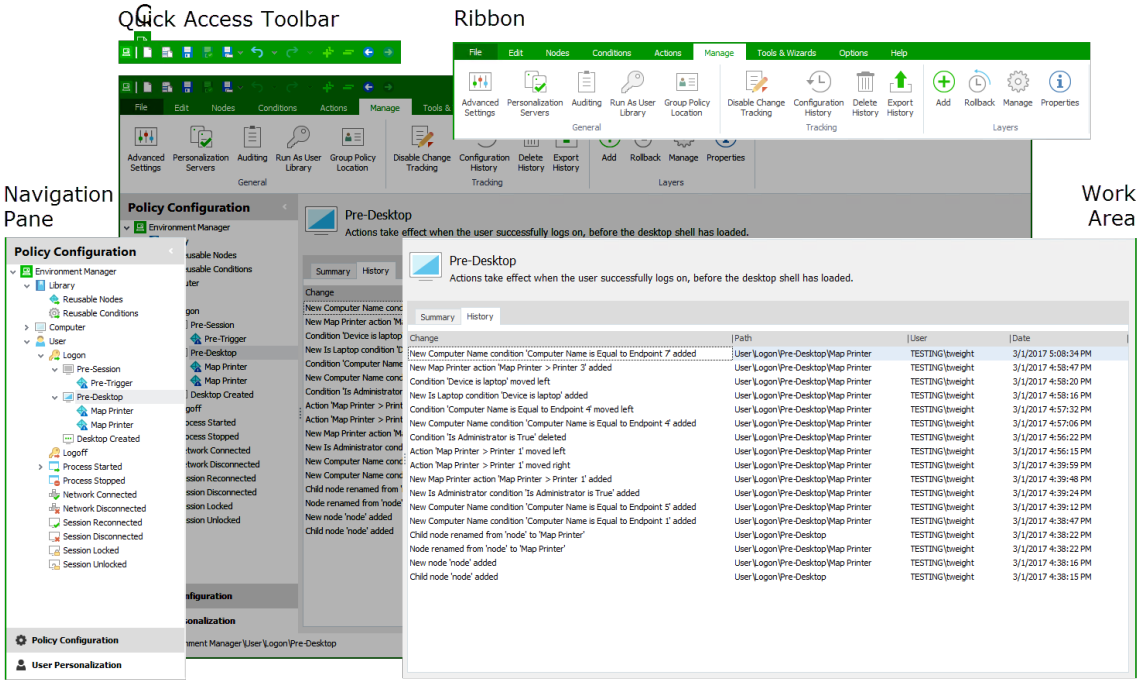
When accessed in this way the console opens with an empty and untitled configuration. The console also starts when a saved configuration is opened.

There are three variants of the Environment Manager console:

- **Personalization** - Installs only the personalization element of Environment Manager
- **Policy** - Installs only the policy element of Environment Manager
- **Both consoles** - Installs the combined console; both personalization and policy are installed.

The choice of which console to install is made during installation.

Elements



Resolution

Recommended screen resolution for the console is 1024 x 768 pixels.

Installing the Consoles

The traditional Environment Manager installation, using Setup.exe, automatically installs the combined console. Some administrators may not require access to both. For example, they may only be responsible for configuring personalization and have no need for the policy side of the console. Installing the Personalization or Policy consoles can only be done using the EnvironmentManagerConsole MSIs.

For more information about installation, see the User Workspace Manager help.

Ribbons

Ribbons include buttons for performing actions, arranged in groups, according to the area of the console to which the actions relate. For example, the **Edit** ribbon page includes all common tasks, such as **Cut**, **Copy** and **Paste**.

Split ribbon buttons contain multiple options and are indicated by an arrow just below the button. Click the arrow to display and select the list of options, or simply click the button for the default action.

Help

The **Help** button on the Help ribbon launches the Help for the product and displays the topic relating to the current area of the console in view. A smaller icon for launching the Help displays at the far right of the console, level with the ribbon page tabs.

Navigation Pane

The Navigationpane consists of the navigation tree and navigation buttons. The navigation tree is the area for managing nodes of the configuration. The navigation buttons allow you to view the different areas of the console, i.e. the Policy Configuration and User Personalization.

Work Area

The **Work Area** provides the main area for managing the settings of the configuration and product. The contents of the work area vary according to the selected nodes in the navigation tree and the selected navigation buttons. Sometimes the work area is split into two panes. For example, one pane can provide a summary of the settings in the other pane.

Additional Console Features

- **Shortcut Menu** — right-click shortcuts are available in the navigation tree and some areas of the console.
- **Drag and Drop** — this feature is available in some nodes of the navigation tree.
- **Cut/Copy/Paste** — these actions can be performed using the buttons in the **Edit** ribbon, shortcut menu options and also using keyboard shortcuts.

File Menu

The **File** menu provides options for managing configurations including create new, open existing, save, import and export configurations and print.

Option	Description
New	Creates a new default configuration which is locked for editing.
Open	Opens an existing configuration from one of the following locations: • **Live configuration on this computer** • **Configuration from the Management Center** • **Configuration file from disk**: AppSense Environment Manager Package Files format (AEMP). • **Configuration from System Center Configuration Manager**

Option	Description
	• **Configuration from Endpoint Manager** - when opening a configuration from an Ivanti Endpoint Manager Core Server, you will need a console connection. For further details refer to the Connect the Endpoint Manager Core Server to the Environment Manager Console step. A live configuration is located on a computer which has Environment Manager Agent installed and running.
Save	Updates the current configuration with any changes made since the last change. Click the arrow by the icon to access the following Management Center Specific options: • **Save and Continue Editing** - Save the configuration and keep it locked and open for editing. The configuration cannot be deployed whilst locked. Use to save your changes whilst continuing to update the configuration. • **Save and Unlock** - Save the configuration and unlock it ready for deployment. • **Unlock without saving** - Unlock the configuration without saving changes. A live configuration is located on a computer which has Environment Manager Agent installed and running.
Save As	Saves the configuration with a new name to one of the following locations: • **Live configuration on this computer** - Save the current configuration on the current computer and apply it as the working configuration. • **Configuration in the Management Center** - Creates the current configuration in the package store on the selected Management Center. • **Configuration in System Center Configuration Manager** - Saves your configuration to the specified System Center Configuration Manager server. • **Configuration file on disk** - Saves the current configuration as a file on a local or network drive in AEMP format. • **Configuration in Endpoint Manager** - Saves the current configuration to a Package store in Ivanti Endpoint Manager. For further details on creating Policy configurations for Endpoint Manager deployment refer to the Create a new Environment Manager Policy and save it to your core server Help section.
Import & Export	• **Import configuration from MSI** - Imports a configuration from an existing MSI package, for example, legacy configurations which have been exported and saved from legacy consoles. • **Export Configuration as MSI** - Exports the current configuration as a MSI package.

Option	Description
Exit	Closes the console. You are prompted to save any changes you have made to the current configuration.

Quick Access Toolbar

The **Quick Access**toolbar provides quick functionality for managing the configuration setup, such as **Save**, **Save and Unlock**, **Undo**, **Redo**, and navigation to previously and next displayed views.

Button	Description
	**New** Opens a new, empty default configuration which is locked for editing. If you already have a configuration open, you will be prompted to save it before you open a new one.
	**Open Configuration from the Management Center** Opens an existing configuration from the Management Center.
	**Save** Saves changes to the configuration. The configuration will remain locked if opened from the Management Center.
	**Save and Unlock** Saves the configuration to the Management Center and unlocks it to allow deployment. The current configuration closes and a new default configuration opens.
	**Save As** Saves the configuration with a new name to one of the following locations: • **Live configuration on this computer** - Save the current configuration on the current computer and apply it as the working configuration. • **Configuration in the Management Center** - Creates the current configuration in the package store on the selected Management Center. • **Configuration in System Center Configuration Manager** - Saves your configuration to the specified System Center Configuration Manager server. • **Configuration file on disk** - Saves the current configuration as a file on a local or network drive in AEMP format.
	**Back and Forward**

Button	Description
	Cycle through the views you have visited in a session. For example, if you select the Computer trigger and then the User trigger, the Back button takes you to the Computer trigger and a subsequent click of the forward button, takes you to the User trigger. These are navigation tools only and do not affect the action you have performed in the console.
	**Undo** Clears the action history. Up to 20 previous actions are listed. Select the point at which you want to clear the actions. The action selected and all preceding actions are undone.
	**Redo** Re-applies the cleared action history. Up to 20 cleared actions are listed. Select the point at which you want to redo the actions. The action selected and all preceding actions are redone.
	**Expand All** Expand all nodes, actions and conditions in a selected area of the console. Context sensitive to the selected item and works in the navigation tree or the work area. For example, if used when the Computer trigger is highlighted, all triggers and nodes within the Computer trigger are fully expanded. To expand all triggers and nodes in a configuration, select the Environment Manager item at the top of the pane and select Expand All. In the work area, if a condition is highlighted, all sub conditions and actions are fully expanded.
	Collapse All Collapses all nodes, actions and conditions - works as Expand All but in reverse.

Managing the Quick Access Toolbar

The Quick Access Toolbar can be configured to add and remove functions and change its position within the console:

- Right-click on a ribbon button or file menu option and select **Add to Quick Access Toolbar** to add it to the Quick Access Toolbar.
- Right-click on a toolbar item and select **Remove From Quick Access Toolbar** to remove it.
- Right click on a ribbon or the toolbar and select **Show Quick Access Toolbar Below the Ribbon** to display the toolbar below the ribbon.

Find and Replace

Environment Manager configurations can be searched using text strings and regular expressions. The whole of the navigation tree can be searched or individual areas, such as a node or a trigger, can be targeted. Searches include all nodes, child nodes, conditions and actions in a configuration or within the selected area.

Find and Replace could be used, for example, to change the name of a server throughout the configuration, to amend the IP address of a particular endpoint or just to find where in a configuration a particular registry key is referenced.

Perform a Find and Replace

1. In the Edit ribbon, select **Find and Replace**.

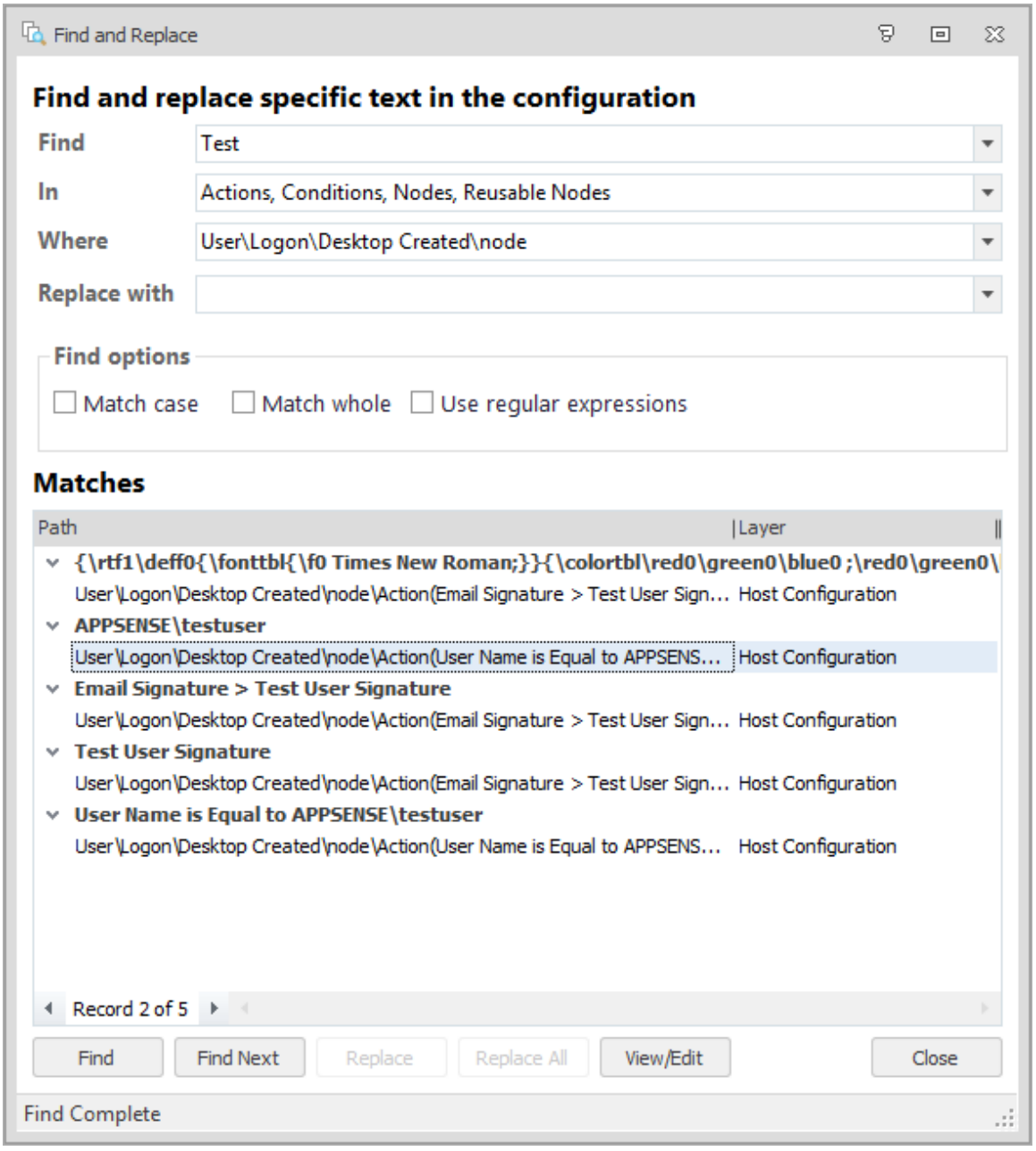
   The Find and Replace dialog displays. If you want to target the search, select the required area of the configuration prior to opening the dialog. In the example below, the Computer\Process Started trigger was selected. This can be changed in the dialog as explained in step 4.

2. In the **Find** field, enter the text to search for or the regular expression you want to use for the search.
3. In the **In** field, define which elements of the configuration you want to search - **Actions**, **Conditions**, **Nodes** and/or Reusable Nodes.
4. Check that the **Where** field shows the path to the area of the configuration you want to search. If the path is incorrect:
   - Amend the path manually
   - Delete the path to search the whole configuration
   - Select a previously searched path from the drop-down
5. In the **Replace with** field, enter the replacement text. If you are performing a search, this field can be left blank.
6. Configure the find options by selecting any combination of the check boxes:
   - **Match Case** - Search for only those items which match the capitalization of the text in the Find text
   - **Match Whole Word** - Search for only those items which match the whole word in the Find field.
   - **Use Regular Expressions** - Return any items which match the regular expression entered in the Find field.
7. Click **Find** to display all items that match your search criteria.

Search Results

The search results list any item which matches the query and show where the item is found in the configuration.

In the example below, the user has searched for "CurrentVersion". The search results include the registry key "Software\Microsoft\Windows\CurrentVersion\Explorer". This registry key is referenced in actions found in two different triggers in the configuration. The path to each of the actions is displayed beneath the match.



Select a path to automatically navigate to that area of the configuration. To move to the next match, click **Find Next**.

If you want to replace text, select the required match and click **Replace** - to replace all matches click **Replace All**.

You can redefine a search at any time by updating the criteria and clicking **Find** to update the results. For example, you restrict your search to Conditions or focus the search on another area of the configuration.

To view or edit an action or condition in the search results, select the item and click **View/Edit**. The item opens in the relevant dialog.

Environment Manager Administrative Tools

Environment Manager is packaged with standalone utilities that help administrators create configurations and manage the Personalization Database. The tools are run independently from Environment Manager and all our other products.

The Administrative Tools installer is included with the Environment Manager installation media in both 32 and 64-bit versions:

- EnvironmentManagerTools32
- EnvironmentManagerTools64

Once installed to the default location, the following tools are available:

- Environment Manager Monitor (EmMon)
- Personalization Server Log Viewer
- Environment Manager File Conversion
- EMP File Utility
- EMP Migrate Utility
- EMP Migrate Command Line Utility
- EMP Registry Utility
- File Based Registry Explorer

Service Packs

Service Packs are self-contained packages or patches that are used to update specific files within a User Workspace Manager application without reinstalling the full application. Service packs can be applied more often and reduce the need for system restarts on your endpoints. Service packs are delivered as a Windows Installer patch (MSP) file and are often referred to as patch files.

Install a Service Pack

Service Packs can be installed or deployed using the same technology and techniques used when installing MSIs. Both Microsoft System Center and the Management Center 8 FR4 can deploy MSPs. If neither of these products are available, service packs can be installed using the command line interface.

For example, the command:

msiexec.exe /p EnvironmentManagerAgent64.msp

installs any files that have been amended as part of the patch for just Environment Manager 64 bit agent.

The following command installs the base version of the Environment Manager Agent (MSI) and the Environment Manager patch file (MSP) simultaneously:

msiexec.exe /i EnvironmentManagerAgent64.msi
PATCH=c:\fullpath\EnvironmentManagerAgent64.msp

A base version must be installed before the patch file can be applied.

If the patch file contains driver or hook files that are currently in use on the machine the patch is being applied to, you are informed that a reboot is required. If you chose to continue, the system is restarted when the patch has been applied.

For information on installing and upgrading service packs using Management Center, see the User Workspace Manager help.

Installation Order and Dependencies

It is recommended that all components of a service pack are installed and that the PersonalizationServerXX.MSP is installed first. All other components have no required install order.

Roll back a Service Pack

You can roll back or install service packs using either the Management Center (8 FR4 onwards) or the Windows Control Panel.

When you uninstall a service pack, the product reverts to the previous latest build - whether a service pack or base version.

With the exception of the Personalization Server component patch file (PersonalizationServerXX.msp) All agent and console service pack components can be uninstalled.

Roll Back a Service Pack Using the Management Center

1. In the Management Center console, select **Overview** > **Deployment Groups tab** > **Deployment Groups**.
2. Highlight the Deployment Group and select **Settings** > **Assigned Packages**.

   The Assigned Packages work area displays a list of all the products and their associated packages.
3. Highlight the required Environment Manager service pack and click **Unassign** from the Actions menu.

4. Click **Review and Submit**.

   The Submit Changes dialog displays.

5. Check the details are correct and click **Submit**.

The patch is unassigned based on the deployment group Installation Schedule.

Roll Back a Service Pack Using the Windows Control Panel

From the Control Panel select Programs and Features and uninstall the required patch.

Best Practices for Configuration

This section outlines the key points for consideration when setting up your Environment Manager configuration.

Mandatory vs Local Profiles

During design and implementation stages, consideration should be given to the type of profile which needs to be used as the base to be loaded for the user before Environment Manager Personalization overlays the user's actual settings.

Typically, Mandatory profiles are used which are very light weight and contribute to faster logon times for users. This profile is ideal for environments where all users are accessing devices which are permanently online.

If users also use laptops to work offline, then you need to look at how their account is managed when the laptop is offline; do they:

- Use an Active Directory account?
- Use a Local Profile and provide Active Directory credentials when accessing company resources?

In these instances, it may be easier to leave the user profile path within Active Directory blank and allow users to load a local profile as a base. The cached copy of the local profile must be deleted using the Microsoft utility, DELPROF.

Another solution is to create the **MAN** file for the Mandatory profile, placed within the location of %SYSTEMDRIVE%\Default User.

This allows two benefits:

- You do not have to specify a path within the User properties of Active Directory
- As it is a Mandatory profile, the Windows operating system will flush this automatically.

This will require some time to copy to each managed device.

Applications that use INI Files

Some applications that are used within an environment require the use of INI files or files of this type to keep certain settings for the user.

If the INI file is kept within the user's profile this is typically not a problem for Environment Manager Personalization.

When the INI file is not kept within the user's profile, but in another location, for example, C:\Windows, then you may not want Environment Manager Personalization to capture information from this location, due to the nature and the amount of files in that location.

At this point, you can use Environment Manager Policy actions to copy down the file or folder to the location during either a Logon or a Process Start trigger for the application and then copy the file or folder back up to the user's home directory during a Logoff or Process Stop trigger.

Personalization Membership Performance

Each condition evaluates matches and queries at different speeds providing different response times. These differences could be due to some conditions evaluating against local data and therefore providing rapid response times. Other conditions may require connection to the network thereby increasing response times and relying on connection speeds.

The conditions in the tables below have been rated by performance speed for carrying out matches and queries. By creating configurations with these response times in mind, performance can be optimized. For example, if a configuration contains OR conditions, place them in order of response time with the quickest evaluating first. If the first condition matches, the configuration is not held up by the slower response time of the second condition.

Directory Services Expressions

Condition	Match	Query
Site Membership	Fast	N/A
Computer OU Membership	Slow	Slow
User OU Membership	Slow	Slow

User Expressions

Condition	Match	Query
Is Administrator	Fast	N/A
User Name	Fast	Fast
User Group Name	Fast	Medium

Computer Expressions

Condition	Match	Query
Computer IP Address	Fast	Fast
Computer Domain Membership	Fast	Fast
Computer NETBios Name	Fast	Fast
Computer Group	Fast	Medium
Computer Name	Slow	Slow

Enabling Reverse DNS Lookup on the server increases the performance of the Computer Name condition.

Printer Settings for Personalization

If printer settings are required to be kept by the user, then the following keys need to be added to Windows Settings within the Personalization Server:

HKEY_CURRENT_USER\Printers

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Devices

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Masquerading Applications

To enable managed applications to share user Personalization settings, it is necessary to create an application group. For example, this could be a Microsoft Office group containing Word, Excel, Outlook and PowerPoint.

It may, however, be useful to use a Masquerading Application to allow an application access to another application's personalization data without having to create an application group. For example, running mlcfg32.cpl against Outlook's personalization data to view its registry settings on the client.

To do this, create an entry in the Advanced Settings dialog:

- Name: **MasqueradingApps**
- Value: **rundll32.exe;office12\mlcfg32.cpl;outlook.exe;12.0.0.0:**

This value equates to:

<RealExe>;<RealExe Commandline>;<TargetExe>;<TargetExeVersion>:

For this example, mlcfg32.cpl is grouped with Outlook to share its personalization data.

<TargetExeVersion> matches the version configured in the database for Outlook. If it is set to a wildcard (.*), any version can be supplied here.
These entries can be chained together to provide multiple settings.

Client Specific Masquerading

The MasqueradingApps setting is global and as such, applies on all managed end-point devices. However, to achieve the same behavior, applications can be launched on individual client machines with a special command-line argument: /APPSENSESPECIAL.

The syntax on the client is:

<RealExe> /appsensespecial:<TargetExe>:<TargetExeVersion>

Some applications such as regedit.exe, do not work correctly with extra command-line arguments. These applications should be launched using a command shell which has been run with the APPSENSESPECIAL switch.

For example, cmd.exe /appsensespecial:notepad.exe:1.0.0.0 would launch with the command shell sharing the personalization settings of Notepad. Regedit.exe can now be launched from within the command shell and will have access to Notepad's settings.

In the above scenario, ensure that regedit.exe is not already defined as a managed application or blacklisted.
There should be no other instances of cmd.exe or regedit.exe running.

Create Personalization Caches Based on Environment Variables

The Advanced setting, *MasqueradeAppByEnvVar* allows the Personalization cache used by Environment Manager to be changed based on the existence of an environment variable on the end point.

This allows greater flexibility where Personalization is required for the same version of an application, across multiple machines where one instance of the application is using different plug-ins.

For example, if Microsoft Excel 2007 is run on three Windows 7 devices, by design it would share Personalization settings between all three. If one of those devices was running different plug-ins to the others, it could be useful for this version of Excel to use separate Personalization settings.

Configure Personalization Caches Based on Environment Variables

The following steps show how to configure the user interface using the Excel scenario.

1. Create the following entry in the **Advanced Settings** dialog:
    - Name: **MasqueradeAppByEnvVar**
    - Value: **TargetExe>%ENV_VAR%**

For the Excel scenario, the value would be Excel.exe>%MASQ%.

MASQ is an environment variable set on the client.

2. Create the following managed applications:

Name	Executable	OS RegEx	Version RegEx
Excel	Excel.exe	.*	.*
Excel MASQ	Excel.exe.masq	.*	.*

The Excel.exe.masq executable entry provides an alternative to excel.exe using a different cache to allow separate Personalization to be used for the same application.

Client Configuration

Add the environment variable called **MASQ** with a value of **masq**.

When Excel is run, its Personalization settings go into a cache called Excel **MASQ**.

If the MASQ variable is removed, Excel settings will go into a cache called Excel.

Wildcards and Regular Expressions

This section contains examples of wildcards and regular expressions and how they can be used in Environment Manager.

Environment Manager uses **CAtlRegExp** Class regular expressions.

For further information on CAtlRegExp Class regular expressions, refer to www.msdn.microsoft.com.

Expression	Matches
^[a-f]+	"**alice**" matches because her name starts with a letter between a and f "**john**" does not match because his name starts with a letter greater than f "**Alice**" does not match because her name does not start with a lowercase letter
^[a-fA-F]+	"**Alice**" matches because with this expression uppercase letters are allowed
[a-zA-Z]+\d\d\d$	"**UserWithThreeNumbers123**" matches because the user name is made up of alpha numerics followed by 3 numbers "**UserWithFourNumbers1234**" does not match because the user name has four numbers in it

The domain name can also be specified in regular expressions. For example, **appsense\\^[a-f]+** matches all user names which have a first letter a to h. Without a domain name in the regular expression, the query matches any user names which have a first letter from a to h in any domain.

Expression	Matches
(notepad)|(winword)|(calc).exe	**notepad.exe** matches because it is in the list **wordpad.exe** does not match because it is not in the list
^!(notepad.exe)	**notepad.exe** does not match because notepad is specifically excluded **wordpad.exe** matches because it is not notepad
^!((notepad.exe)|(calc.exe)|(winword.exe))	**wordpad.exe** matches because it is not in the list **calc.exe** does not match because it is in the list

Performance Monitor Counters

Environment Manager Personalization Server provides performance counters that can be analyzed within Performance Monitor (PerfMon.exe).

The available counters are contained within the *Environment Manager Personalization* group.

Configuration Request Counters

An HTTP configuration request is made by a client following a session request. A user configuration is returned to the client. The configuration contains such things as Personalization Groups with managed applications and global properties.

The following counters are available for the configuration request:

Counter	Description
Configuration invalid requests	The total number of invalid HTTP configuration requests processed.
Configuration max time	The maximum time (ms) taken to process an HTTP configuration request.
Configuration min time	The minimum time (ms) taken to process an HTTP configuration request.
Configuration process request time	The time (ms) taken to process the latest HTTP configuration request.
Configuration total average time	The average time (ms) taken to process an HTTP configuration request.
Configuration total time	The total time (ms) taken to process all HTTP configuration requests.

Counter	Description
Configurations per second	The number of HTTP configuration requests processed per second.
Configurations total failed	The total number of failed HTTP configuration requests processed.
Configuration total succeeded	The total number of successful HTTP configuration requests processed.

Session Request Counters

An HTTP session request is made by a client following user logon. The server determines the user site membership and returns a list of server URLs to use for subsequent configuration and synchronization requests.

The following counters are available for the session request:

Counter	Description
Session invalid requests	The total number of invalid HTTP session requests processed.
Session max time	The maximum time (ms) taken to process an HTTP session request.
Session min time	The minimum time (ms) taken to process an HTTP session request.
Session process request time	The time (ms) taken to process the latest HTTP session request.
Session total average time	The average time (ms) taken to process an HTTP session request.
Session total time	The total time (ms) taken to process all HTTP session requests.
Session per second	The number of HTTP session requests processed per second.
Session total failed	The total number of failed HTTP session requests processed.
Session total succeeded	The total number of successful HTTP session requests processed.

Synchronization Request Counters

An HTTP synchronization request is made by a client following an application start or stop and is used to synchronize personalization data to or from the server. Windows settings and other personalization data may also be synchronized using this request at logon/logoff.

The following counters are available for the synchronization request:

Counter	Description
Synchronization invalid requests	The total number of invalid HTTP synchronization requests processed.
Synchronization max time	The maximum time (ms) taken to process an HTTP synchronization request.
Synchronization min time	The minimum time (ms) taken to process an HTTP synchronization request.
Synchronization process request time	The time (ms) taken to process the latest HTTP synchronization request.
Synchronization total average time	The average time (ms) taken to process an HTTP synchronization request.
Synchronization total time	The total time (ms) taken to process all HTTP synchronization requests.
Synchronization per second	The number of HTTP synchronization requests processed per second.
Synchronization total failed	The total number of failed HTTP synchronization requests processed.
Synchronization total succeeded	The total number of successful HTTP synchronization requests processed.

TraceData Request Counters

A TraceData (HTTP passive) request is made by a client to send data to the server for Application Data Collection.

The following counters are available for the TraceData request:

Counter	Description
TraceData invalid requests	The total number of invalid HTTP passive requests processed.
TraceData max time	The maximum time (ms) taken to process an HTTP passive request.
TraceData min time	The minimum time (ms) taken to process an HTTP passive request.
TraceData process request time	The time (ms) taken to process the latest HTTP passive request.

Counter	Description
TraceData total average time	The average time (ms) taken to process an HTTP passive request.
TraceData total time	The total time (ms) taken to process all HTTP passive requests.
TraceData per second	The number of HTTP passive requests processed per second.
TraceData total failed	The total number of failed HTTP passive requests processed.
TraceData total succeeded	The total number of successful HTTP passive requests processed.

About User Personalization

User Personalization captures application and desktop changes to a central database and reapplies them for the user upon logon or application start, regardless of operating system or delivery mechanism.

Changes made to an application are synchronized when the application starts or stops. This enables changes to be shared between multiple sessions simultaneously, without the need to log off.

Windows Settings, such as wallpaper, keyboard and mouse preferences are managed when the user logs on and off.

User Personalization enables applications to be discovered and settings managed with minimum configuration.

When a log on request is received from a client endpoint, the Personalization Server uses rules configured in the database to determine who the user is in order to provide the correct configuration based on that user's personalization group.

The configuration retrieved by the client session from the database at logon determines which applications are managed and the data that is to be virtualized. If a user who is not matched by personalization group membership rules logs on to the system, they are assigned to the default group and managed according to this group's settings.

An Excluded Users personalization group can be created for users who do not require personalization. By creating a personalization group in which no applications or settings are managed, users matching the membership rules are removed from all user personalization management.

If a known user logs on without any applications configured, no applications are managed.

User Personalization does not work with the Run as command. Personalization relies on a user's logon credentials to determine which applications are managed. Therefore, if a user runs an application as Administrator or other user, that application is not personalized.

User Personalization requires a live connection to the SQL database which means that changes to the configuration in the Environment Manager console, are immediately committed to the database - unless working offline. The changes are reflected on endpoints when the local configuration is updated; at logon, configuration poll (default time of 10 minutes) or when the EM User Virtualization Service is started.

By default, User Personalization data is archived on a daily basis enabling application and Windows Settings to be rolled back to previous states, in the event of profile inconsistencies.

The Personalization Analysis tool is also provided which enables the administrator to monitor which applications are being controlled by Environment Manager, including how much data is being stored for each user and application.

Designing and Implementing Environment Manager Personalization

The following points are recommendations for the design and implementation of Environment Manager User Personalization.

- Install the Personalization Database and Personalization Server on separate devices (physical or virtual).
- Where possible, install the Personalization Database with High Availability in mind. Typically for this, clustering of the Microsoft SQL Server is recommended.
- When required, Personalization Servers will support Network Load Balancing being placed in front of the servers.
- For multiple Environment Manager sites or data centers, it is recommended that Personalization Servers and Databases are installed on these sites and local clients pointed to their local Personalization Server and Databases. This reduces performance issues across WAN links.

Setting Up a Personalization Configuration

The following steps outline how to create a basic configuration to manage and migrate existing user data into the Personalization database.

Step 1 Add Personalization Groups

Create the Personalization Groups required for your organization and add membership rules to represent your users.

See Personalization Groups.

Step 2 Configure Application Data Collection

Enable Application Data Collection to passively gather registry and folder usage data for the applications your users have run.

It is recommended that Application Data Collection is disabled when no longer required.

See Application Data Collection.

Step 3 Add Application Groups and Windows Settings Groups

Use the collected data to create managed Application Groups to manage the applications within your organization.

Add Windows Settings Groups to manage the settings users apply to their endpoints.

See Application Personalization and Windows Personalization.

Step 4 Enable Profile Migration

Use Profile Migration to import data from existing user profiles.

See Profile Migration.

User Personalization Architecture

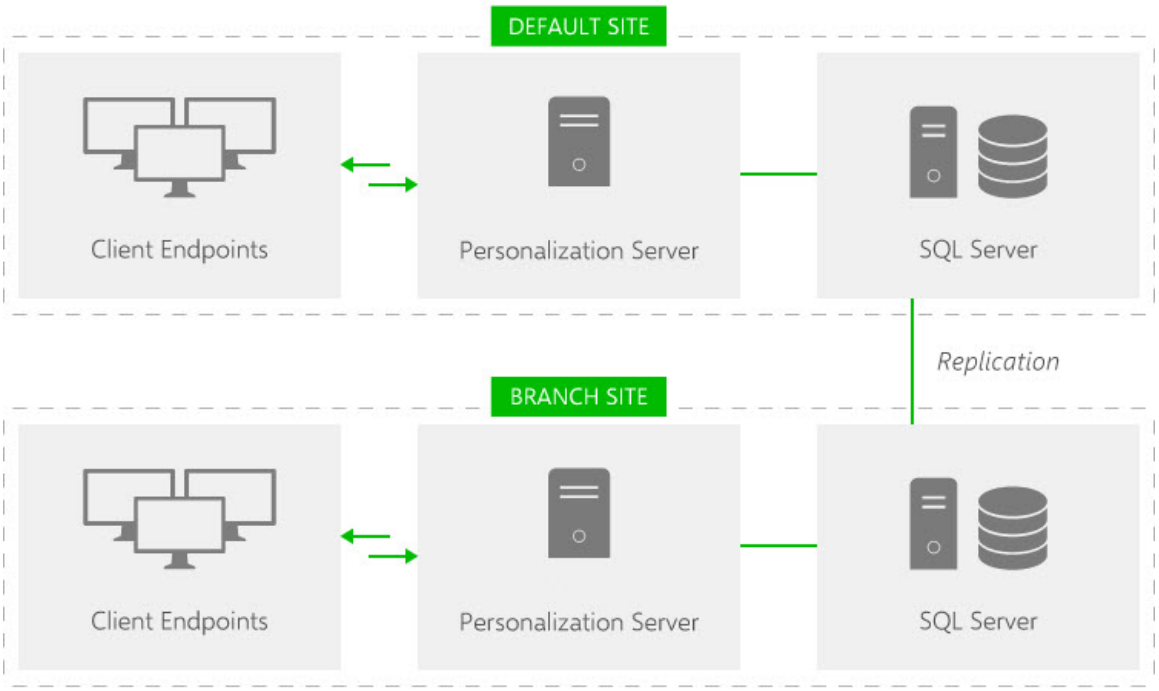
Environment Manager User Personalization utilizes a three tier architecture.

Introduction

Collectively, the components of the standard architecture are known as a site. Sites provide a logical grouping of users; for example, by area of business or geographical location. For organizations with more than one site, the same architecture is used for each site, linked via their SQL servers through replication.

It is not a requirement that each branch site has a dedicated SQL server. However, performance is improved as traffic is contained within the Local Area Network (LAN) and does not have to travel across the Wide Area Network (WAN).

In the diagram below, the system consists of two sites; the default site and an optional branch site.



The client endpoints on a site communicate with their Personalization Server every time one of the following events occurs:

- **Logon** - When a user logs onto a managed endpoint, the Environment Manager Package (AEMP) file is loaded. If user personalization is enabled, the user is connected to the Personalization Server detailed in the configuration. User, endpoint and software version details are passed from the endpoint to the server which determines the site and personalization group that the user belongs to. A personalization configuration is passed back to the client on the managed endpoint by the Personalization Server. This configuration file describes the personalization settings for the user and includes details of managed applications and certificates for the user.

  Windows Settings are synchronized and applied to the endpoint to complete the user personalization logon.

- **Application Start** - When a user launches an application on the endpoint, it is paused briefly to allow Environment Manager to perform the required virtualization actions.

  Details of the application are analyzed and Environment Manager checks to see if User Personalization is enabled and that the application should be managed. For non-managed applications, any policy configuration actions are applied and the application continues without User Personalization settings being managed.

  For those applications which are managed, a configuration file specific to the application is created which details the file and registry inclusions, exclusions and a subset of the Global Properties as configured in the User Personalization database.

  Environment Manager Policy Configuration is notified of the start of the process and any relevant Policy actions are replicated on the virtual cache.
  Whilst the application is running and the user continues to change user personalization settings within it, any changes are virtualized and written to the personalization cache on the endpoint, rather than into the physical registry or file system.

  For application groups configured in Environment Manager, the Personalization database is only synchronized when the first application in the group is started. Synchronization is not performed when the other applications in the group are launched.

- **Application Stop** - When an application is closed, the Personalization Server is notified and a copy of any modified personalization settings is stored in the SQL database. If the process is the last within a group to exit, or the last instance of a managed process of similar applications, synchronization of the cache occurs back to the server.

  If an application is closed when other applications in the same application group are still open, synchronization to the database is not performed. Only when the last application in the group is closed is the database synchronized.

  For more information see Application Groups.

- **Logoff** - When a user logs off any managed applications still running are stopped by Windows and the logoff completes as normal before the Environment Manager logoff screen displays. The application, desktop and certificate settings are synchronized with the database and the local virtual cache is cleared. Once this is complete the Environment Manager logoff screen is removed from display and the Windows logoff is completed as normal.

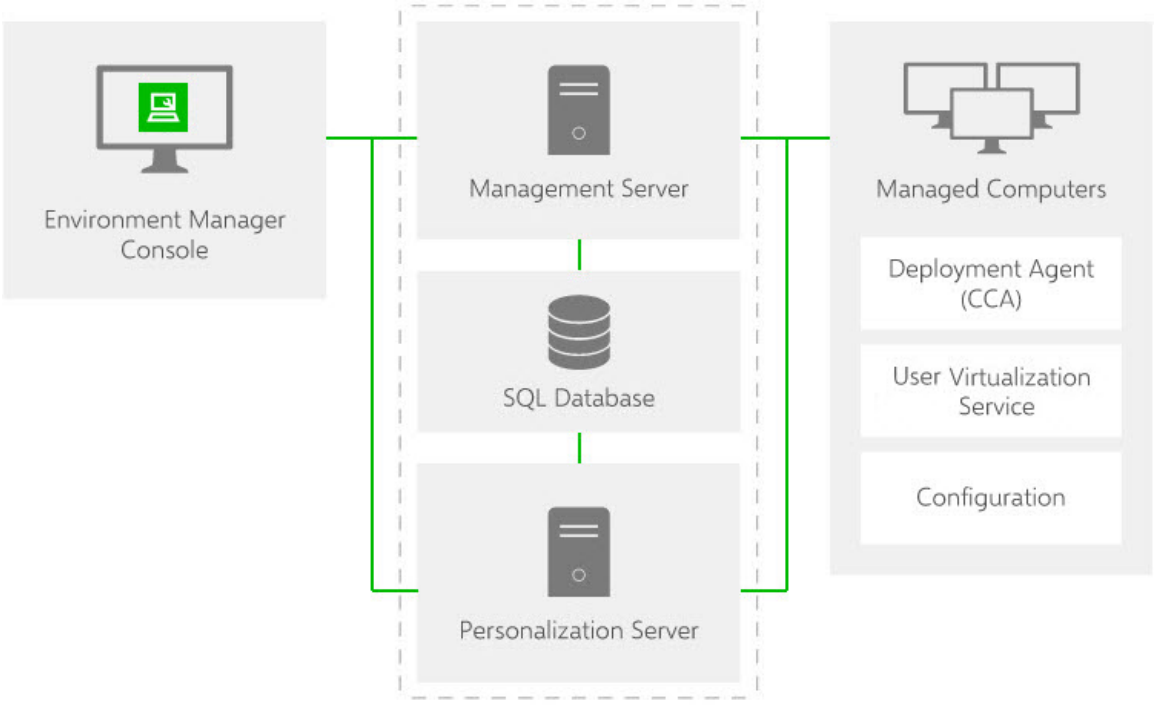
  If **Local Cache** is enabled, the local virtual cache is not cleared to enable the user to maintain their settings once disconnected from the corporate network.

- **Configuration Poll** - Changes can be made to user personalization configurations by administrators whilst users are logged on. A configuration poll is performed at a predefined interval which picks up any configuration changes and applies them to the managed endpoints. The polling interval is set in the console using the Advanced Settings.

The virtual cache on the endpoint is the root folder for all User Personalization data where virtualized files and registry settings are stored prior to synchronization with the Personalization database. The data for each setting and managed application is stored here and kept up to date by synchronization with the Personalization database.

The virtual cache is a hidden folder located at C:\AppSenseVirtual on every managed endpoint.

Each of the above events creates a synchronize request where the client ensures that the local virtual cache is up to date with the SQL database. Every time an application starts or stops, the software ensures that the SQL database and local virtual cache are synchronized.



Tier 1 - Client Endpoint

The client endpoint hosts the user's logon session. Within the session is the Environment Manager software containing the User Personalization modules which monitor changes that the user makes to managed applications and communicates these back to the Personalization Server.

The client endpoints can be any combination of hardware and software that is capable of running a windows session:

- Standalone desktops, laptops and tablet PCs
- Terminal Servers
- Microsoft Hyper-V

Tier 2 - Personalization Server

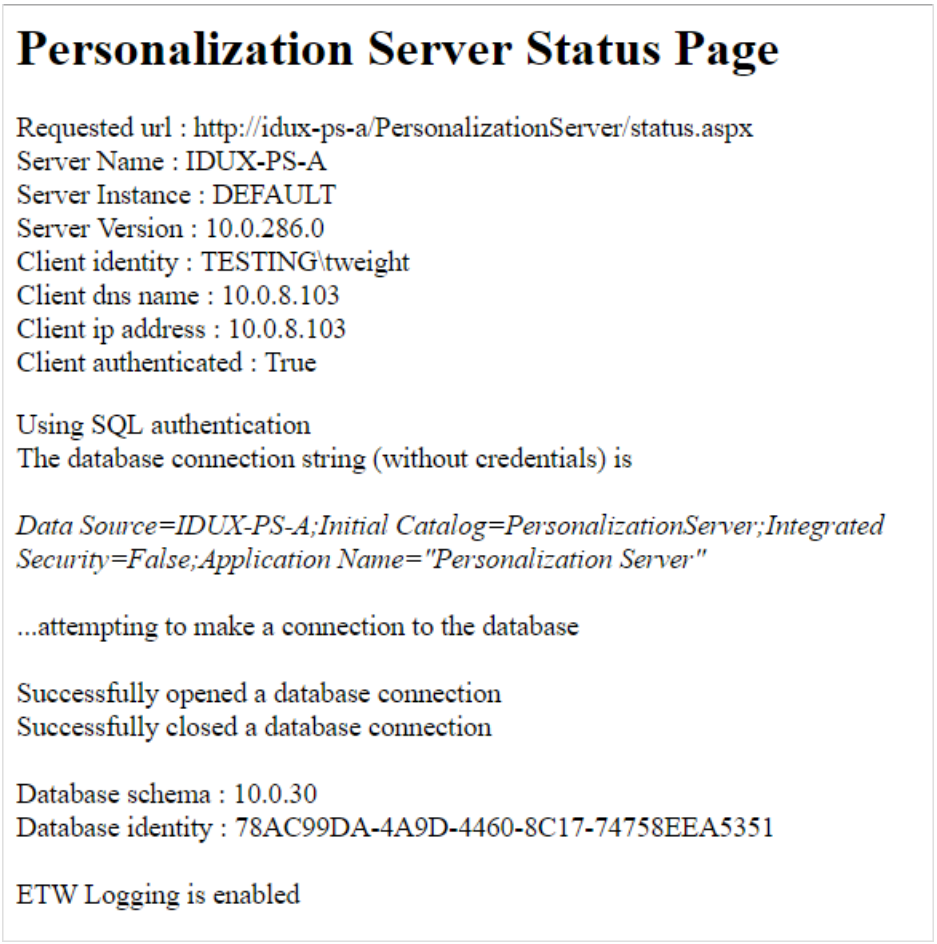
The Personalization Server is implemented as an Internet Information Services (IIS) Website and acts as the broker between the endpoints and the Personalization database. It enables access to the database from multiple clients to be controlled from one place. The Personalization Server can verify the identity of the clients before processing requests so clients do not need to be added as users to the database.

Status Request

To test whether a Personalization Server is installed, running and to test the database connection, enter the following URL in your internet browser, replacing <SERVER> with the name of the required server.

http://<SERVER>**/PersonalizationServer/**

The status.aspx file for a server shows whether the server connection was successful and further details about the connection, database and server.



Personalization Server Status Page

Requested url : http://idux-ps-a/PersonalizationServer/status.aspx
Server Name : IDUX-PS-A
Server Instance : DEFAULT
Server Version : 10.0.286.0
Client identity : TESTING\tweight
Client dns name : 10.0.8.103
Client ip address : 10.0.8.103
Client authenticated : True

Using SQL authentication
The database connection string (without credentials) is

Data Source=IDUX-PS-A;Initial Catalog=PersonalizationServer;Integrated Security=False;Application Name="Personalization Server"

...attempting to make a connection to the database

Successfully opened a database connection
Successfully closed a database connection

Database schema : 10.0.30
Database identity : 78AC99DA-4A9D-4460-8C17-74758EEA5351

ETW Logging is enabled

Load Balancing Status Request

If using a load balancer monitor to check the server status page (status.aspx) where the server is set to Windows Authentication, the monitor must provide Windows credentials in the HTTP headers or the server will respond with an "unauthorized" reply. As an alternative, use one of the following methods, appropriate to your setup should be used.

To check the health of load balanced servers use the following methods, appropriate to your setup.

IIS7 - Windows Server 2008 and R2

Use the following URLs in an internet browser, replacing <SERVER> with the name of the required server:

- **http://<SERVER>/PersonalizationServer/dbmonitor.aspx** - Checks the connection with the database. Returns "OK" if the database can be contacted and "FAIL" if it cannot.
- **http://<SERVER>/PersonalizationServer/pingmonitor.aspx** - Checks whether the personalization server address is reachable returning "OK" if successful. No response indicates an error.

IIS6 - Windows Server 2003

For IIS6, the SetMonitorAnonymousIIS6.vbs script must be used to set up dbmonitor.aspx and pingmonitor.aspx for anonymous access. For further details, contact Support.

Tier 3 - SQL Server

Holds information related to personalization sites and servers, users and groups, applications, endpoint configuration data and user personalization data.

Personalization Server data is organized and stored in tables on the SQL server in the following logical groupings:

- **Personalization Data** - Contains data relating to the user, including group membership details and controls the data for managed applications. Application data is updated here each time a managed application is opened or closed.
- **Site Membership** - Houses the Site Membership information which communicates details of which Personalization Server the user should be connected to. Once connected, configuration information is retrieved including details of includes and excludes for registry items and folders.
- **User Group Assignment** - Defines the group to which a user belongs which in turn controls which applications are managed for the user in addition to their Windows Settings.
- **Authorized Users** - Contains tables which control who is authorized to connect to the Personalization Server and what they are able to do when connected.
- **Archiving** - Stores the archive data from the Daily and Demand archiving SQL Agent jobs in two tables relating to Application Profile and Application Data archives.
- **Auditing** - Used to setup and configure the auditing events that are raised internally and control what and to where, events are raised. From this, the required alerts and reports are generated by the Management Center.

  See the Management Center help for further information.
- **Managed Application Settings** - Contains details of all registry and folder include and exclude paths for each application and application group.
- **General Settings** - Contains system and user defined global properties for key and value pairing including console version, timeouts and archiving information. Installation information including an upgrade history and is maintained by the AppSense System Configuration Utility, is also stored here.

SQL Server AlwaysOn and Mirroring

SQL Server AlwaysOn is the preferred SQL Server technology to support High Availability/Disaster Recovery scenarios and User Workspace Manager 10.x servers have been optimized to support this technology.

SQL mirroring is available for User Workspace Manager 10.1 FR1+ customers who are currently in the process of transitioning to Always On technology. For more information, see the User Workspace Manager help.

Configure Personalization Servers

To configure a personalization server, you must first establish a connection. Once connected you can create a configuration to control personalization for you enterprise. A list of servers can then be created to manage which servers your managed users connect to.

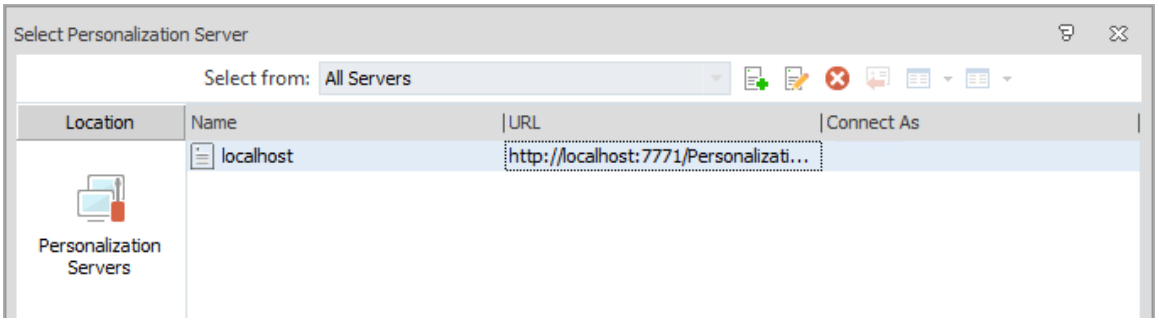
For details about configuring Personalization Servers, see the User Workspace Manager help.

Connection

In order to configure personalization for your users, you must first establish a connection to a Personalization Server. The **Connect** button allows you to list one or more Personalization Servers and connect to the required one.

To configure Personalization, localhost is automatically added to the Select Personalization Server dialog if the following conditions are true:

- A Personalization Server is installed and configured on the same machine as the console.
- A Personalization Server has not previously been configured in the Select Personalization Server dialog



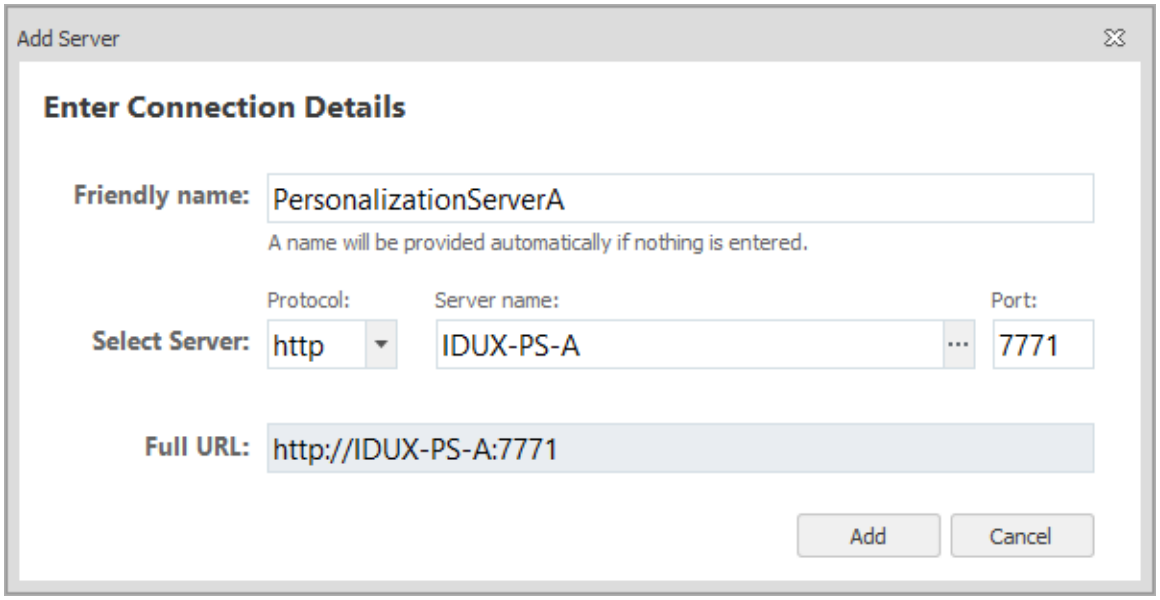
Connect to a Personalization Server

1. Select the **User Personalization** navigation button.
2. From the Server ribbon, click **Connect**.

   The Select Personalization Server dialog displays.

3. Click the new server button .

   The Add Server dialog displays.



4. Enter a Friendly Name for the server. This can be any text but should be something which will enable you to identify the server. If no text is entered, the server name is used.
5. Select the required protocol - **http** or **https**.
6. Enter the server name or browse for the required server by specifying locations and searching for server names.
7. Enter the port number. The port range for Personalization servers is 7771 to 7790 and the default port is 7771.

   Once the server details have been added, the URL for the server is displayed.

8. Click **Add**.

   The server is listed in the Select Personalization Server dialog.

9. Repeat steps **2** to **6** to add more servers.

   Servers in the list can have their details edited or be deleted from the list using the buttons at the top of the dialog.

10. Select the server you want to connect to and click **Connect**.

    When you return to this dialog, any servers you have listed are available for selection.

The Environment Manager and Client Communication agents now perform extra checks during HTTPS communications and will now fail on any certificate errors, for example. self-signed certificates. This can be overridden by the using the IgnoreCertificateErrors registry setting:

- Value Name: **IgnoreCertificateErrors**
- Value Type: **DWORD**
- Location: **HKLM\Software\Appsense\Common**
- Possible values:
  - **0 or not present** - do not ignore certificate errors
  - **1** - Ignore all certificate errors

Personalization Servers in the Combined Console

This feature is only available in the combined console. In the Personalization console, the server list is configured using the Endpoint Server List.

When creating an AEMP configuration in the combined console, a list of personalization servers can be configured. When the configuration is pushed out to endpoints it determines whether endpoints are personalized and if they are, to which server they will connect. It is recommended that multiple personalization servers are listed so alternative servers can be automatically selected for failover purposes.

The first time a user logs on to a managed endpoint, the Environment Manager agent contacts the first Personalization Server to request the actual list of servers the endpoint should use (based on the sites configured in the database). The client then contacts the correct server to pull down the User Personalization configuration, containing the list of the applications which should be personalized for the user.

If all attempts to connect to a Personalization Server fail, then the configuration is not downloaded and Personalization does not take place.

If no servers are configured, endpoints managed by this configuration are not personalized.

To cater for such a scenario it is recommended that the **9661 - Timeout Communicating with Personalization Server** auditing event is enabled.

Configure a Personalization Server List

1. Select the **Policy Configuration** navigation button.
2. From the Manage tab select **Personalization Servers**.

   The Configure Personalization Servers dialog displays.
3. Click the add server button  .

   The Add Server dialog displays.

4. Enter the server name or click the ellipsis to search for the required server by specifying locations and searching for server names.

   Do not select or enter Localhost as the server name. If Localhost is entered as the server name it is added to the configuration.aemp file as the location of the Personalization Server. The client tries connecting to http://localhost/Personalization which is incorrect and User Personalization is disabled.

5. Enter a Friendly Name for the server. This can be any text but should be something which will enable you to identify the server. If no text is entered, the server name is used.
6. Select the required protocol - **http** or **https**.
7. Enter the server name or browse for the required server by specifying locations and searching for server names.
8. Enter a port number. The port range for Personalization servers is 7771 to 7790 and the default port is 7771.

   Once the server details have been added, the URL for the server is displayed.

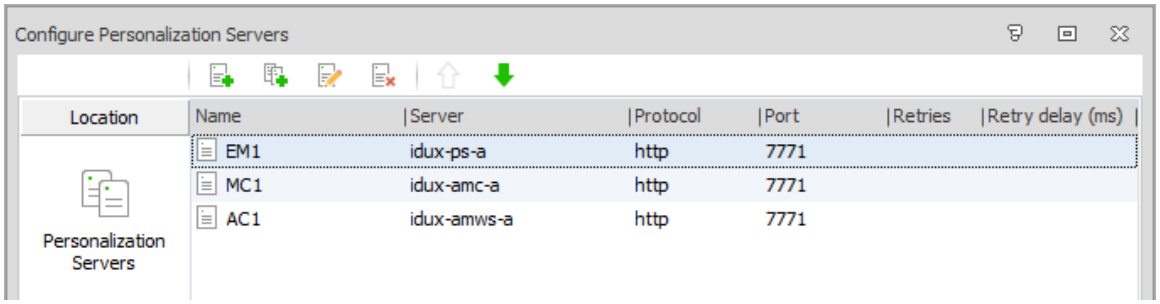
9. Click **OK**.

   The server is listed in the Select Personalization Server dialog.

10. Repeat steps **3** to **9** to add more servers.

    Servers in the list can have their details edited or be deleted from the list using the buttons at the top of the dialog.

11. If you have added more than one server, use the arrow buttons to reorder the list. When the configuration is deployed, endpoints attempt to connect to each server in turn. If a connection cannot be made with any server in the list, Personalization does not occur.



12. Click **OK** to save the server list.

When the configuration is deployed to endpoints, this list is used to determine which servers managed users connect to.

Personalization Servers in the Personalization Console

This feature is only available in the Personalization console. In the combined console, the server list is configured in the Policy side of the console using the Personalization Servers option from the Manage ribbon.

The Endpoint Server List allows you to create an AEMP configuration file containing the Personalization Servers to which endpoints can connect.

It is recommended that, where possible, multiple servers are added to the Select Personalization Server dialog so alternative servers can be connected to for failover purposes.

Environment Manager supports SQL 2012 Always-On functionality.

When a user logs on to a managed endpoint, an attempt is made to connect to the first server on the list. If a connection cannot be made to that server, connection with the next server in the list is attempted and so on until a connection is established.

If all attempts to connect to a server fail, personalization does not take place.
An AEMP configuration created from the Endpoint Server List in the Personalization console can be opened and edited in the combined console.

Likewise, an AEMP configuration with configured servers, created in the combined console, can be opened and edited in the Endpoint Server List in the Personalization console.

You cannot upgrade policy configurations in the Personalization only console. policy configurations can only be upgraded in the combined Policy only consoles.

Configure and Save a Personalization Server List

1. Open the Environment Manager Personalization console.
2. From the Server ribbon, click **Endpoint ServerList**.

   The Personalization configuration dialog displays.
3. Click the new server button  . The Add Server dialog displays.
4. Enter the server name or click the ellipsis to search for the required server by specifying locations and searching for server names.

   Do not select or enter Localhost as the server name. If Localhost is entered as the server name it is added to the configuration file as the location of the Personalization Server. The client tries connecting to http://localhost/Personalization which is incorrect and User Personalization is disabled.
5. Enter a Friendly Name for the server. This can be any text but should be something which will enable you to identify the server. If no text is entered, the server name is used.
6. Select the required protocol - **http** or **https**.

7. Enter the server name or browse for the required server by specifying locations and searching for server names.
8. Enter the port number. The port range for Personalization servers is 7771 to 7790 and the default port is 7771.

   Once the server details have been added, the URL for the server is displayed.
9. Click **OK**.

   The server is listed in the Select Personalization Server dialog.
10. Repeat steps **2** to **6** to add more servers.

    Servers can have their details edited or can be deleted from the list using the buttons at the top of the dialog.
11. If you have added more than one server, use the arrow buttons to reorder the list. When the configuration is deployed, endpoints attempt to connect to each server in turn. If a connection cannot be made with any server in the list, Personalization does not occur.
12. Click **OK** to save the server list.

    When the configuration is deployed to endpoints, this list is used to determine which servers managed users connect to.
13. Click **File** and select the required save option.

Personalization Server Selection Using Group Policy

Environment Manager 8.3 client software allows the personalization server to be selected using group policy. As detailed in the sections above, a list of personalization servers is normally specified in the configuration. However, this can be overridden by the group policy list.

Using group policy templates, a list of servers can be created that will be used by endpoints as a fail-over list. There is also an option to bypass the site processing on the server and use the specified server directly. This provides new configuration options and offers better performance for large numbers of users.

Group policy selection of personalization servers works even if no configuration file is deployed to the client.

The following group policy administrative template files are supplied with the Environment Manager Personalization and combined consoles:

- AppSensePersonalizationServers.admx
- AppSensePersonalizationServers.adml
- AppSensePersonalizationServers.adm

Upgrades for Endpoints with Personalization Applied by Group Policy
If an endpoint with an 8.2 configuration file without personalization servers, is upgraded to software version 8.3 or later, the configuration file should be upgraded by loading it into the console and saving it out again. Errors are not generated if the configuration file is not updated but policy actions will not be applied to managed processes.

Configure a Personalization Server List with Group Policy

1. Navigate to the Group Policy folder:

   C:\Program Files\AppSense\Environment Manager\Console\Templates\Group Policy

   This is the default installation file path. If you have installed to an alternative location, find the Group Policy folder in you install location.

2. Complete the setup action for your operating system:
   - Copy the AppSensePersonalizationServers.admx file to:

     C:\Windows\PolicyDefinitions (where C:\Windows is the system root).
   - Copy the AppSensePersonalizationServers.adml file to:

     C:\Windows\PolicyDefinitions\en-US (where C:\Windows is the system root).
3. Open Group Policy Editor. Policy templates are available for user and computer policies. User policies can be tailored to individual users and computer policies apply to the endpoint.
4. Select **Administrative Templates > AppSense > Environment Manager** for either the user or computer policy.
5. Select the required option:
   - **Specify list of personalization servers** - Specify a list of personalization servers for endpoints to connect to and use as a failover list. The AEMP configuration server list is overridden by the list created.

     Select **Enabled** and enter the required server name(s). Each server must be preceded by http:// and where more than one server is required, separated by a comma. For example, http://server1,https://server2,http://server3:3000.
   - **Bypass server site processing** - Normally, initial contact is made with the server listed in the AEMP file. Once contact is made, the database rules are evaluated to determine which server the client should connect to. Enabling this option means clients ignore the database site rules and connect directly to the server determined by Group Policy.

     Select **Enabled** to bypass server site processing.
6. Click **OK** to save your settings and update personalization server selection to use group policy.

Evaluation Order

When deciding which server to connect to, the following evaluation order is used:

1. User Policy
2. Computer Policy
3. AEMP File

Each source is evaluated in order until a server list is found; if a server is not found, evaluation moves to the next source. If no servers are found, the user is not personalized.

If a server is listed in User Policy, for example, but is unavailable, processing ends and the user is not personalized.

Personalization Servers Policy

Enabling User Personalization is a policy decision and the setting is configured within the Policy Configuration side of the console. It is the deployed configuration which determines whether managed endpoints are subject to User Personalization and to which server endpoints connect.

It is recommended that multiple servers and/or virtual hosts are added to the Select Personalization Server dialog so alternative servers can be easily selected for failover purposes.

Deploy the policy configuration that contains a list of Personalization Servers to the endpoints sending the configuration.aemp to managed computers. The first time a user logs on to a managed endpoint, the Environment Manager agent contacts the first personalization server to request the actual list of servers the endpoint should use (based on the sites configured in the database). The client then contacts the correct server to pull down the User Personalization configuration, containing the list of the applications which should be personalized for the user.

If all attempts to connect to a Personalization Server fail, then the User Personalization configuration is not downloaded and User Personalization does not take place.

For details about configuring Personalization Servers, see the User Workspace Managerhelp.

To cater for such a scenario it is recommended that the **9661 - Timeout Communicating with Personalization Server** auditing event is enabled.

Configure a Personalization Servers List

1. Select the **Policy Configuration** navigation button.
2. From the Manage tab select **Personalization Servers**.

   The Configure Personalization Servers dialog displays.
3. Click the add server button  .

   The Add Server dialog displays.
4. Enter the server name or click the ellipsis to search for the required server by specifying locations and searching for server names.

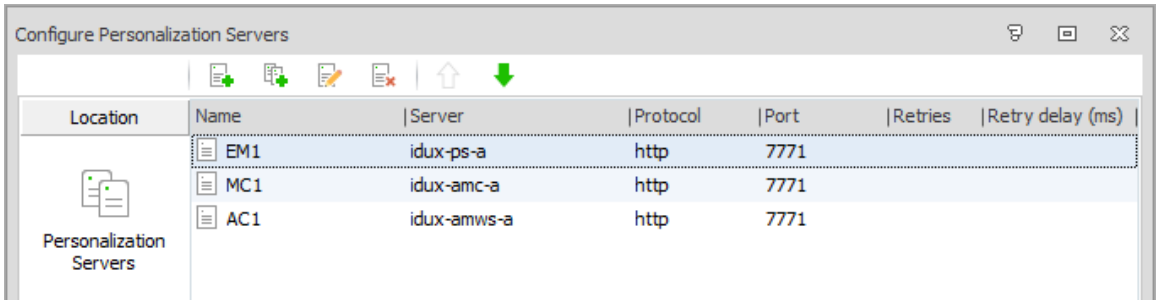
   Do not select or enter Localhost as the server name. If Localhost is entered as the server name it is added to the configuration.aemp file as the location of the Personalization Server. The client tries connecting to http://localhost/Personalization which is incorrect and User Personalization is disabled.
5. Enter a Friendly Name for the server. This can be any text but should be something which will enable you to identify the server. If no text is entered, the server name is used.
6. Select the required protocol - **http** or **https**.

7. Enter the server name or browse for the required server by specifying locations and searching for server names.
8. Enter a port number. The port range for Personalization servers is 7771 to 7790 and the default port is 7771.

   Once the server details have been added, the URL for the server is displayed.
9. Click **OK**.

   The server is listed in the Select Personalization Server dialog.
10. Repeat steps **3** to **9** to add more servers.

    Servers in the list can have their details edited or be deleted from the list using the buttons at the top of the dialog.
11. If you have added more than one server, use the arrow buttons to reorder the list. When the configuration is deployed, endpoints attempt to connect to each server in turn. If a connection cannot be made with any server in the list, Personalization does not occur.



12. Click **OK** to save the server list.

When the configuration is deployed to endpoints, this list is used to determine which servers managed users connect to.

Personalization Groups

Personalization groups enable Environment Manager User Personalization to be configured for multiple users based on common requirements. Membership Rules, based on Environment Manager conditions, define which users are managed by the group. applications, application groups and Windows Settings groups can then be added to determine what is personalized for users in the group.

Settings for application discovery, syncing and caching can also be applied to further control how personalization is managed for the group.

Add a Personalization Group

1. In the User Personalization navigation pane select **Personalization Groups**.

   The work area displays the name and description of all existing personalization groups which can be accessed by double-clicking.

2. Click **Add Personalization Group** from the Personalization ribbon.

   A new personalization group is created at the bottom of the list of personalization groups, immediately above the Default Users group.

3. Add a name for the new group and press **Enter**.

   To rename a personalization group, highlight and click **Rename Group** from the Personalization ribbon.

   If changes are made to personalization group assignment, the affected users should log off and back on to pick up the changes.

Create Group Personalization Membership Rules

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Right-click in the Membership Rules work area and select **Add Condition Group** from the shortcut menu.

4. Highlight a condition type; User, Computer or Directory Membership and select a condition.

   The available conditions are listed in Personalization Group Conditions. The dialog box for the selected condition displays. The following conditions are available for personalization group membership rules:

Type	Condition
User	User Name User Group Is Administrator
Computer	Computer Name Computer Domain Computer NETBIOS Name Computer Group Computer IP Address
Directory Membership	User OU Membership Computer OU Membership Site Membership

5. Configure the condition and click **OK**.

   The new condition group displays under Membership Rules. The title of the condition entered into the Description field in the General tab, is the display name for the condition in the Personalization group. If a description is not entered, the condition details form the display name.

6. To further define group membership for the Personalization group, add more conditions:
   - **AND** Rule - Right-click on an existing condition, select **Insert Condition** and configure the condition as required.
   - **OR** Rule - Right-click in the work area and select **Add Condition Group** and configure the condition as required.
7. Condition groups can be edited and deleted by selecting **Edit Condition** or **Delete Condition** from the shortcut menu.

User Data Partitioning

Prior to Environment Manager 10.0, user data was tied to a user/Personalization Group. This meant that if a user moved between personalization groups, they would have separate data in each group. In 10.0, this mechanism changed so data is tied to the user only, regardless of which personalization group they match, so users will only have one data profile.

Personalization Group Arrangement

Personalization groups can be created based on roles within an organization. For example, Administrators would be managed by a different group to that of a Sales or Marketing department. They have different responsibilities and requirements and therefore require different access rules and settings.

The Personalization Server assigns users to the first personalization group in the Personalization Groups node with matching membership rules. It is therefore important that personalization groups are listed in order of priority with the most relevant group at the top. This ensures users are assigned to the correct group.

Users may match the membership rules of multiple groups at different times and might even be managed by different groups depending on their circumstances at logon. For example, a user working at a different site could have different requirements and can be assigned to a different group for each site.

The Default Users personalization group is automatically included in all Environment Manager Personalization configurations and is always at the bottom of the list of groups. If a user, on an endpoint with the Personalization Agent installed, does not match the membership rules of any other group, that user would be managed by the Default Users group. Membership rules are therefore not required and cannot be defined.

Only applications and Windows Settings that are relevant to a typical user within your organization should be personalized in the default group.

Order a List of Personalization Groups

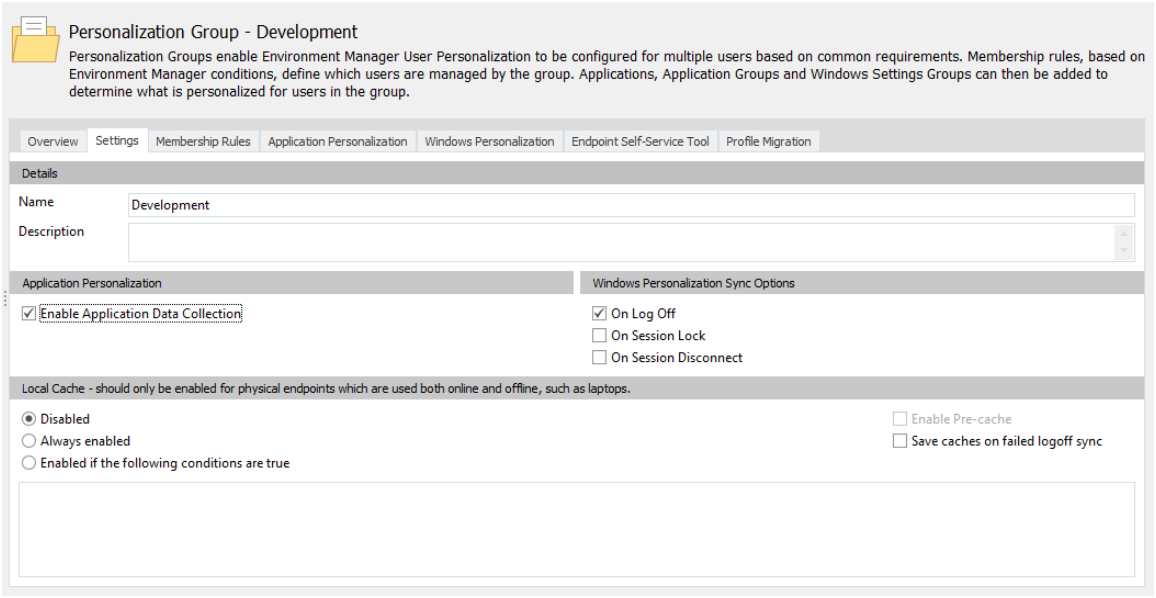
1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. From the Edit ribbon, click **Move Up** and **Move Down** to change the order of the personalization groups.

Default Users is always be the last personalization group and cannot be moved.

Personalization Group Settings

Each personalization group includes settings to define behavior regarding Application Personalization, Windows Personalization and Local Cache settings for users in the personalization group.

In the User Personalization navigation tree, select **Personalization Groups**, choose a Personalization Group and select the **Settings** tab.



Application Personalization Settings

Settings for discovering applications and application data.

Auto-discover user applications

This option enables monitoring of managed endpoints to detect the applications which are being used within an organization. The executable name, version and operating system are captured for every applications launched.

The collected data can be viewed through Personalization Analysis reports where applications can be added to the list of managed applications available to Personalization Groups.

Enable Application Data Collection

This option enables registry and folder usage data to be passively collected from endpoints as users run applications.

Caution: Enabling this option causes a significant increase in system utilization on managed endpoints. It is recommended that Application Data Collection is disabled when no longer required.

This data can be used when adding new applications to the Personalization configuration.

Windows Personalization Sync Options

Select when you want Windows Personalization settings to be saved to the database:

- On Log Off
- On Session Lock
- On Session Disconnect

Any combination of the above settings can be applied.

Scriptable Sync

Windows Personalization settings can be synchronized on demand using a PowerShell cmdlet, installed with the Environment Manager Agent.

Before using the command, import the EmCmdlet.dll - open Windows PowerShell and enter the following:

```
import-module 'C:\Program Files\AppSense\Environment
Manager\Agent\EmCmdlet.dll'
```

If you have changed the default install location, amend the file path accordingly.

Enter `Test-EmUserOperations` to verify that the cmdlet is able to communicate with the server. The response should be `True`.

To synchronize Windows Personalization settings, enter: Sync-DesktopSettings

The Windows Settings for that endpoint are synchronized with the database.

The default timeout for the cmdlet is 30 seconds. However, this can be changed using the `-Timeout` argument. For example, `Sync-DesktopSettings -Timeout 60`

Other standard PowerShell arguments can be used in conjunction with the cmdlet. For example, `-verbose`.

Local Cache

The Local Cache settings manage personalization behavior for users when they are not connected to the corporate network. When Local Cache is enabled, a copy of a user's virtual cache, containing their personalization settings, is retained on the managed endpoint when they log off. When the user subsequently logs on whilst disconnected from the network, their personalization settings are available. The next time the user logs on to the corporate network, any changes to managed applications made offline are synchronized with the database.

For the virtual cache to exist for an application offline, that application must have been opened and closed on the specific endpoint, prior to going offline. If a virtual cache does not exist for an application on the endpoint, personalization settings are not applied and the application opens with its default settings. Not having cache at application start means any changes made are not synchronized to the database and are lost.

It is only necessary to enable local caching for physical devices which may have intermittent connectivity to the corporate network, for example, laptops which are taken home. This ensures that Personalization settings are still available on the endpoint when there is no connection to the Personalization Server. It is generally not required for virtual machines.

There are three Local Cache settings:

- **Disabled** - The virtual cache is deleted when users log off from the corporate network. Any changes a user makes to managed applications whilst offline are lost when they next connect to the network.
- **Always enabled** - Each time a user logs off, a copy of their virtual cache is saved on their endpoint. Whilst working offline, their personalization data is updated locally as changes to managed applications are made and synchronized to the database when online.
- **Enabled if the following conditions are true** - A set of conditions govern the circumstances under which the virtual cache is saved at logoff.

Two further Local Cache options can be selected in addition to the settings above:

- **Enable Pre-cache** - All application personalization data is downloaded to the local cache at logon rather than when each application is run. This option is only available when Local Cache is enabled.

The availability of the Pre-Cache option is dependent on local cache being enabled and any specified conditions being met. If the conditions are not met, pre-caching on the client will not take place.

- **Save caches on failed logoff sync** - If communication between a managed endpoint and the database is interrupted or lost, synchronization of personalization data from the endpoint to the database is retried at regular intervals until communication is re-established. When the connection is restored, personalization data is synchronized to the database.

  If communication is not restored and the user logs off, personalization data for that session or application is lost. However, if Local Cache is enabled the personalization data is saved on the endpoint and is synchronized following successful connection with the database.

Configure Local Cache Conditions

1. Select a personalization group In the User Personalization navigation tree.
2. Select the **Settings** tab.
3. In the Local Cache section of the work area, select, **Enabled if the following conditions are true**. The Conditions ribbon is displayed.

   For a user to be subject to Local Cache rules they must first be a member of the selected personalization group; offline rules are only considered once group membership has been established.
4. Select a condition from the Conditions ribbon.

   The dialog for the selected condition displays.
5. Configure the condition and click **OK**.

   The new condition displays under the Membership Rules tab.
6. To further define group membership for the personalization group, add more conditions. More complex conditions can be configured using AND and OR statements:
   - AND Rule - Right-click on an existing condition, select **Insert Condition** and configure the condition as required.
   - OR Rule - Right-click in the work area and select **Add Condition Group** and configure the condition as required.

   Condition groups can be edited and deleted by selecting **Edit Condition** or **Delete Condition** from the shortcut menu.

Local Cache Conditions

The table below lists the conditions available for the **Enabled if the following conditions are true** option is selected for a Personalization Group.

Type	Condition
User	User Name User Group

Type	Condition
	Is Administrator
Computer	Is Laptop Computer Name Computer Domain Computer NETBIOS Name Computer Group Computer IP Address Operating System Is VDI
Directory Membership	User OU Membership Computer OU Membership Site Membership
Session and Client	Client Connection Protocol

Personalization Group Membership Rules

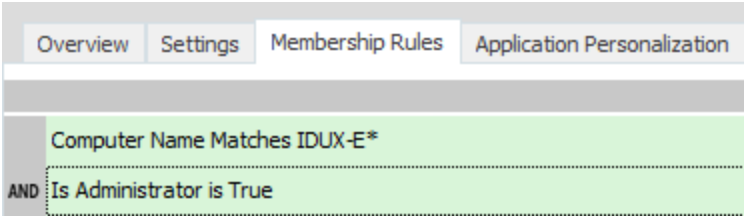
The Membership Rules for a Personalization group are governed by conditions which must be satisfied for a user to be managed by that personalization group. The conditions are based on user attributes, computer specifications and directory membership. Membership can be based on a single condition or a user may have to fulfill a number of conditions to be managed by a Personalization group.

Rule Types

Membership to a Personalization group can be based on two rule types:

- **AND** - Multiple conditions must be satisfied for membership of the Personalization group.

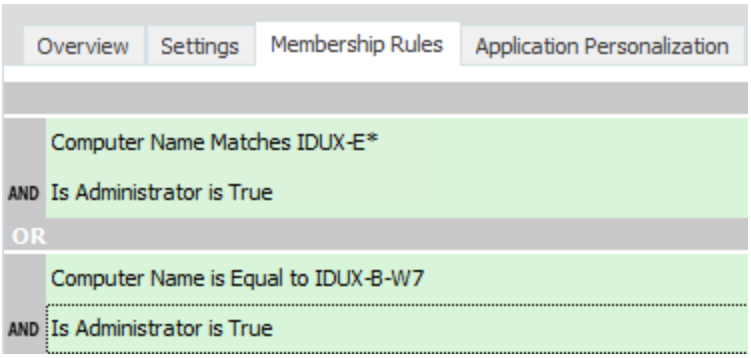
  This is called a condition group.A condition group has been created containing two conditions:



Users must fulfill both conditions to be managed by the Personalization group.

- **OR** - By satisfying the conditions for one of a number of conditions or condition groups, users are managed by the Personalization group.

  A second condition group has been added.

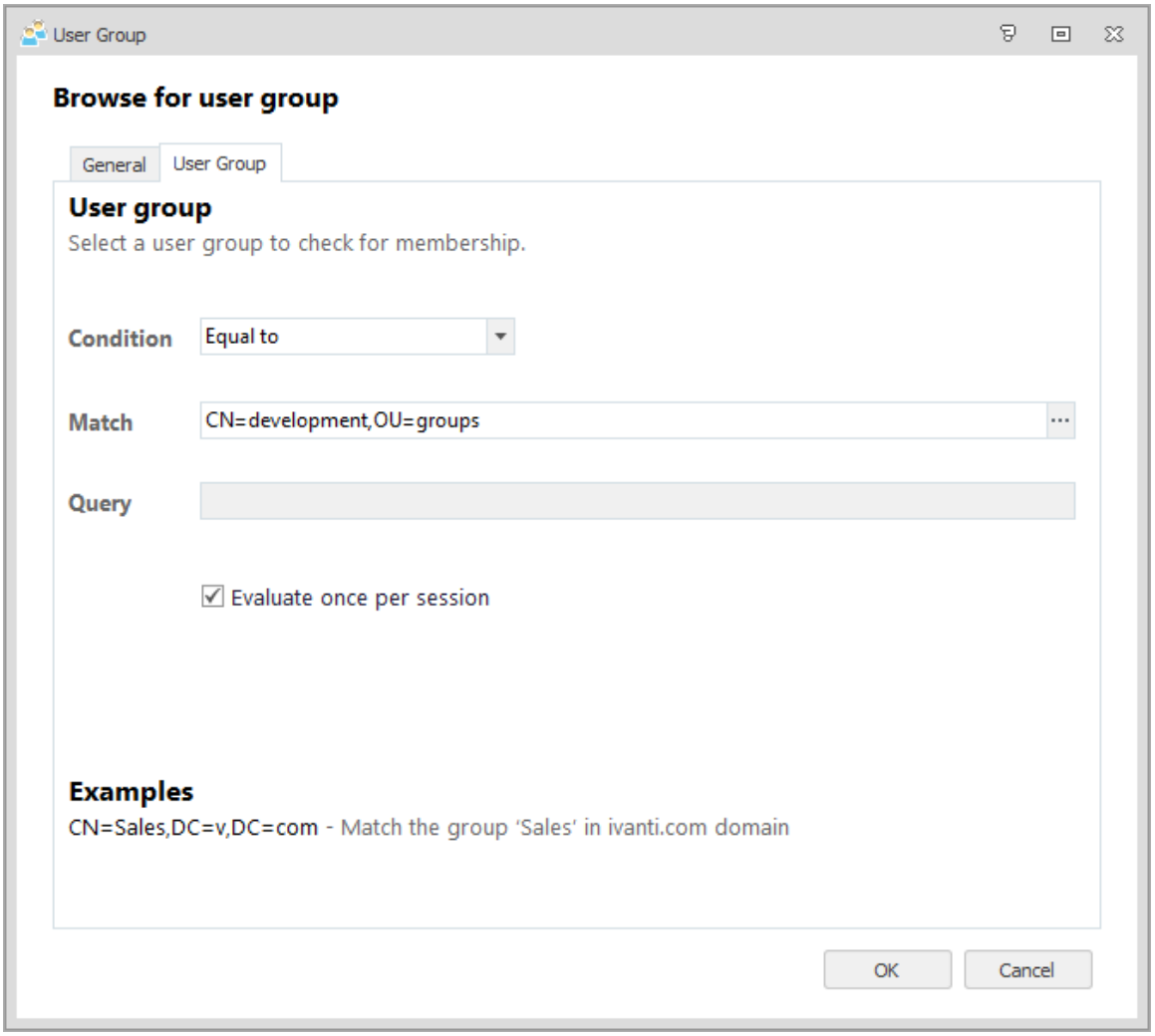


  To be managed by this personalization group, a user must fulfill all the conditions in the first condition group or all the conditions in the second condition group.

Membership Conditions

Personalization Group Membership conditions are a subset of the conditions used in the Environment Manager Policy console. Most of the membership rules conditions use the same fields to set the validation.

The image below shows the User Group condition dialog.



Most conditions use the same fields to create a condition. Select an option from the Condition drop-down. The following options are available:

- **Equal** - A comparison is made against the contents of the Match field to target the users or computers which fulfill those criteria
- **Not Equal** - Targets all users or computers which do not fulfill the criteria in the Match field.
- **Query** - Targets all users or computers which match the criteria specified in the Query field. Using wildcards in the query allows a wide range of matches, for example:
  - *Windows - matches text ending in Windows.
  - Windows* - matches text starting with Windows.
  - *Windows* - matches text containing Windows.

Create Group Personalization Membership Rules

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Right-click in the **Membership Rules** work area and select **Add Condition Group** from the shortcut menu.
4. Highlight a condition type; User, Computer or Directory Membership and select a condition. The available conditions are listed in Personalization Group Conditions. The dialog box for the selected condition displays.

   The following conditions are available for personalization group membership rules:

Type	Condition
User	User Name User Group Is Administrator
Computer	Computer Name Computer Domain Computer NETBIOS Name Computer Group Computer IP Address
Directory Membership	User OU Membership Computer OU Membership Site Membership

5. Configure the condition and click **OK**. The new condition group displays under Membership Rules.

   The title of the condition entered into the **Description** field in the **General** tab, is the display name for the condition in the Personalization group. If a description is not entered, the condition details form the display name.

6. To further define group membership for the Personalization group, add more conditions:
    - **AND** Rule - Right-click on an existing condition, select **Insert Condition** and configure the condition as required.
    - **OR** Rule - Right-click in the work area and select **Add Condition Group** and configure the condition as required.

    Condition groups can be edited and deleted by selecting **Edit Condition** or **Delete Condition** from the shortcut menu.

Application Personalization for Personalization Groups

Application Groups enable applications which interact together, using common registry keys and folders, to be managed as a single group for personalization.

Applications must be in an Application Group before they can be personalized. When creating an application, options are available to add it to a new or existing Application Group. This makes it easier to add new applications that share common settings with existing applications.

Application Groups can be added to a Personalization Group using one of the following methods:

- Add Existing Application Groups
- Add Existing Ungrouped Applications
- Add a New Application to a Personalization Group by Name
- Add a New Application to a Personalization Group from Application Data Collection
- Add a New Application Group to a Personalization Group from Template

Add Existing Application Groups

Add existing Application Groups to be personalized for users who match the membership rules of the Personalization Group.

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Application Personalization** tab.
4. Click **Add Existing**.

    The Select Application Groups dialog displays.
5. Select one or more Application Groups. Multiple Application Groups can be selected using the **Ctrl** or **Shift** keys.
6. Click **OK**.

The selected Application Group is added to the Personalization Group.

Add Existing Ungrouped Applications

Add existing ungrouped applications, that are not part of an Application Group, to be personalized for users who match the membership rules of the Personalization Group.

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Application Personalization** tab.
4. Click **Add Existing**.

   The Select Application Groups dialog displays.
5. Select **Select Ungrouped Applications**.

   The Select Ungrouped Applications option displays only when applications that are not part of an Application Group are available to add.

   Ungrouped applications that are not part of an Application Group display at the bottom of the dialog.
6. Select one or more applications. Multiple applications can be selected using the Ctrl or Shift keys.
7. Click **OK**.

The selected application is added to the Personalization Group.

Add a New Application to a Personalization Group by Name

1. Add a new application, either to a new or existing Application Group, to be personalized for users who match the membership rules of the Personalization Group.
2. In the User Personalization navigation pane select **Personalization Groups**.
3. Select a personalization group.
4. Select the **Application Personalization** tab.
5. Click **New By Name**.

   The Add an Application dialog displays.
6. In the Executable field, enter an application executable name or click the ellipsis (...) to select an application from the file system.
7. Optionally, in the Folder field, enter a folder path or click the ellipsis to select a folder from the file system. The application is managed only if it is located in the specified folder.

   If the field is left blank, all applications matching the entered criteria are managed, regardless of location.

8. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.
9. Optionally, tick **Advanced Details** and, in the Operating System and Application Version fields, enter regular expressions to target a specific operating system and/or application version. Alternatively, use the .* default regular expression to include all operating systems and application versions.

   The specified combination of executable name, operating system and application version must not match existing applications.

   Applications must be added to a new or existing Application Group:
10. **New Application Group** - Specify the Application Group name in the Create New Application Group field. The Application Group name is automatically populated from the application name, however it can be changed as required. Application Groups must not have the same name as existing applications or Application Groups.
11. **Existing Application Group** - Select an existing Application Group in the Add to Existing Application Group field.
12. Click **OK**.

The Application Group is added to the Personalization Group.

Add a New Application to a Personalization Group from Application Data Collection

Application Data Collection passively collects data from managed endpoints as users run applications.

Registry key and folder paths that are written to and read from are recorded for each application. On application close, the data is stored in the Environment Manager Personalization database.

The collected data can be used to create new applications and add to registry and folder inclusions to existing Application Groups.

Application Data Collection can be used in the following modes:

- Add a New Application to a Personalization Group from Automatic Configuration
- Add a New Application to a Personalization Group from Manual Configuration

Add a New Application to a Personalization Group from Automatic Configuration

Environment Manager analyzes the collected data and uses it to create an automatic configuration.

In the automatic configuration, paths are grouped to common parents and paths which are not recommended for inclusion are filtered out.

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Application Personalization** tab.
4. Click **New from Data Collection**.

   The Add Application - Data Collection dialog displays. The dialog lists applications that have been collected by Application Data Collection.
5. Select one of the following radio buttons to target specific application versions:
   - **Use Major Application Version** - Applications are grouped by their major version number. For example, 5.0 and 5.1 are grouped together, but 6.0 is separate.
   - **Use All Application Versions** - Applications are grouped, regardless of their version number. For example, 5.0, 5.1 and 6.0 are grouped together.
6. Select an application from the list.
7. Click **View automatic configuration details**.

   A read-only copy of the configuration displays. From the snapshot taken at each application close, the following statistics are calculated and displayed alongside each registry key or folder path for all users that have run the application:

   - **Occurrences** - The total number of times that the registry path or folder path has been accessed by the application.
   - **Average Size** - The average size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as an average size of 150 bytes.
   - **Peak Size** - The largest recorded size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as a peak size of 200 bytes.

   The cumulative sizes of the Average Size and Peak Size displays at the bottom of the dialog. This information shows the potential profile size per user if the application is personalized.
8. Click **Done** to close the automatic configuration view.

   The automatic configuration closes.
9. Click **OK**.The Enter Details dialog displays.
10. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.

11. Applications must be added to a new or existing Application Group:
    - **New Application Group** - Specify the Application Group name in the Create New Application Group field. The Application Group name is automatically populated from the application name, however it can be changed as required. Application Groups must not have the same name as existing applications or Application Groups.
    - **Existing Application Group** - Select an existing Application Group in the Add to Existing Application Group field.
12. Click **OK**.

The Application Group is added to the Personalization Group.

Add a New Application to a Personalization Group from Manual Configuration

1. Using manual configuration, registry and folder inclusions can be configured from the collected data to create an application configuration to suit your requirements.
2. In the User Personalization navigation pane select **Personalization Groups**.
3. Select a personalization group.
4. Select the **Application Personalization** tab.
5. Click **New from Data Collection**.

   The Add Application - Data Collection dialog displays. The dialog lists applications that have been collected by Application Data Collection.
6. Select one of the following radio buttons to target specific application versions:
    - **Use Major Application Version** - Applications are grouped by their major version number. For example, 5.0 and 5.1 are together, but 6.0 is separate.
    - **Use All Application Versions** - Applications are grouped, regardless of their version number. For example, 5.0, 5.1 and 6.0 are grouped together.
7. Tick **No, I want to configure this application manually (advanced)**.

8. Click **Configure**.

   The dialog lists all registry keys and folder paths which have been collected by Application Data Collection for the selected application.

   From the snapshot taken at each application close, the following statistics are calculated and displayed alongside each registry key or folder path for all users that have run the application:

   - **Occurrences** - The total number of times that the registry path or folder path has been accessed by the application.
   - **Average Size** - The average size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as an average size of 150 bytes.
   - **Peak Size** - The largest recorded size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as a peak size of 200 bytes.

   If required, tick **Hide paths which are rarely personalized** to filter out paths which are not recommended for inclusion.

9. Tick the registry and folder paths to be added as inclusions for the Application Group.

   As paths are selected and deselected, the Application Profile Size updates with the cumulative sizes of the Average Size and Peak Size for the selected paths. This information shows the potential profile size per user if the application is personalized.

10. Click **OK**.

    The Enter Details dialog displays.

11. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.

    Applications must be added to a new or existing Application Group:

    - **New Application Group** - Specify the Application Group name in the Create New Application Group field. The Application Group name is automatically populated from the application name, however it can be changed as required. Application Groups must not have the same name as existing applications or Application Groups.
    - **Existing Application Group** - Select an existing Application Group in the Add to Existing Application Group field.

12. Click **OK**.

The Application Group is added to the Personalization Group.

Add a New Application Group to a Personalization Group from Template

Import one or more Application Groups from the built-in templates or from a template file.

If a template is available, it is recommended that the template is used rather than adding the Application Group either manually or from Application Data Collection.

Templates for commonly used applications are available on community.ivanti.com.

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Application Personalization** tab.
4. Click **Import Template**.

   The Import Application Groups dialog displays.
5. Select one of the following radio buttons:
   - **Import from AppSense templates** - Import from the built-in Application Group templates. Templates are available for commonly personalized applications, such as Microsoft Internet Explorer and Microsoft Office. These templates contain recommended inclusions and exclusions for personalization.
   - **Import from exported configuration** - Import from an exported Application Group template. When selected, a file browser displays for an Environment Manager Personalization configuration to be selected.
6. Select the Application Groups to import. To select all groups, select **Application Groups** at the top of the list.
7. Click **OK**.

The selected Application Groups are imported into the configuration and added to the current Personalization Group.

Personalization Group Application Clashes

Clashes occur when an application exists multiple times in a single personalization group. Environment Manager automatically detects clashes between applications within a personalization group and will notify you of a clash when:

- An application is added to a personalization group which already exists in an application group, assigned to the personalization group
- An application group is added to a personalization group which contains an application which already exists in the applications list for that group

Clashing applications are managed based on the following processing order:

- Application groups
- Applications
- Global application exclusions

Clashing applications can cause unexpected behavior and should be resolved. Resolve application clashes by removing the application from the application group, applications list or Application Exclusions.

Windows Personalization and Personalization Groups

For each personalization group, a list of Windows Settings Groups can be configured to tailor personalization to the requirements of the users managed by that group.

Configure Windows Personalization for a Personalization Group

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Windows Personalization** tab.
4. Click **Add**.

   The available Windows Settings Groups are listed.
5. Select a Windows Settings Group and click **OK**.
6. Select multiple groups using the **Ctrl** or **Shift** keys.

The Windows Settings Groups are added to the Personalization Group.

For information on inclusion logic when adding a Windows Settings Group to a Personalization Group, see Windows Personalization.

Profile Migration

For each Personalization Group, Profile Migration can be configured to either import user profile data into the database from a local profile or network profile or export user profile data from the database back into the local file system.

Importing Profiles

Import Restrictions

During profile Import, files may fail to synchronize in the following scenarios:

- The number of files within a specific profile sync exceeds the IIS MaxHttpCollectionKeys setting - the default value is 1000

- The size of any single file exceeds the IIS maxAllowedContentLength setting - the default value is 30mb

In both scenarios, the profile import for Windows Settings or Application Groups fails and is reported as "failed to copy data to target" for the migration state. Profile Import continues to attempt to sync the remaining Profile settings.

If the issues above are addressed, the import automatically retries at the next logon if the user has not subsequently captured personalization for Windows Settings groups or that specific application group.

If personalization data has been captured subsequently by the user, after fixing the profile source, the captured data for the failed application group or Windows Settings Group must be deleted for it to be imported on next logon.

Files that cannot be read, such as those locked by another application, are not be imported.

Configure Profile Migration to Import Data from a Local Profile

User profile data is copied at logon from the logged on user's local profile to the Environment Manager virtual cache. This data consists of included registry, folder and file paths for managed Application Groups and Windows Settings Groups.

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Profile Migration** tab.
4. Click **Edit**.

   The User Profile Migration Settings dialog displays.
5. Select **Import existing user settings to Personalization**.
6. Select **Local** from the Source drop-down.
7. Click **OK**.

   If settings from a previous import operation exist for the Personalization Group, a dialog displays. The following options are available:

   - **Resume the previous import** - Existing settings are not replaced, but registry, folder or file inclusions which do not have data are imported.
   - **Start a new import** - Existing settings are overwritten with imported user profile data.

Profile Migration Import is enabled for users within the Personalization Group.

At logon, data from included registry, folder and file paths for managed Application Groups and Windows Settings Groups within the user profile is copied into the database.

Configure Profile Migration to Import Data from a Network Profile

User profile data is copied at logon from the profile at the specified network path to the Environment Manager virtual cache. This data consists of all included registry, folder and file paths for managed Application Groups and Windows Settings Groups. AppData can be imported from a separate network path if required.

Advanced Certificates, General Folder Options and Icons Windows Settings, cannot be imported from a network location.

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Profile Migration** tab.
4. Click **Edit**.

   The User Profile Migration Settings dialog displays.
5. Select **Import existing user settings to Personalization**.
6. Select **Network** from the Source drop-down.
7. Enter a UNC path in the Network Path field. Environment Variables within the specified network path are expanded.

   The profile version number is appended to the specified network path where required. The following table shows the profile paths for each operating system if \\server\share\profiles\%USERNAME% is specified:

Operating system	Profile version	Example profile path
Windows 7 Windows Server 2008 R2	V2	\\server\share\profiles\%USERNAME%.V2
Windows 8 Windows Server 2012	V3	\\server\share\profiles\%USERNAME%.V3
Windows 8.1 Windows Server 2012 R2	V4	\\server\share\profiles\%USERNAME%.V4
Windows 10	V5	\\server\share\profiles\%USERNAME%.V5

8. If AppData is stored in a separate location, tick **Enable AppData to be imported from a network location** and specify a UNC path in the AppData Path field.

9. Click **OK**.

   If settings from a previous import operation exist for the Personalization Group, a dialog displays. The following options are available:

   - **Resume the previous import** - Existing settings will not be replaced, but registry, folder or file inclusions which do not have data will be imported.
   - **Start a new import** - Existing settings will be overwritten with imported user profile data.

Profile Migration Import is enabled for users within the Personalization Group.

At logon, data from included registry, folder and file paths for managed Application Groups and Windows Settings Groups within the user profile is copied into the database.

Import Activity for Configuration Updates

After configuring Profile Migration in Import mode, a prompt displays if either:

- Application Groups or Windows Settings Groups are added to the Personalization Group
- Included registry, folder or file paths are added to a managed Application Group or Windows Settings Group.

Select from one of the options below.

Option	Description
Commit the change and restart the Import for the affected groups	The Application Group or Windows Settings Group is added to the Personalization Group or the included registry, folder or file path is added to the managed Application Group or Windows Settings Group. The import is restarted for all users within the Personalization Group, regardless of whether data has already been imported for the user.
Commit the change but only for new users	The Application Group or Windows Settings Group is added to the Personalization Group or the included registry, folder or file path is added to the managed Application Group or Windows Settings Group. The import is started for users in the Personalization Group who do not have existing data.

Exporting Profiles

Export existing data from the Environment Manager Personalization database into user profiles.

Configure Profile Migration to Export Profiles

User profile data is copied at logon from the database to the logged on user's local profile.

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Profile Migration** tab.
4. Click **Edit**.

   The User Profile Migration Settings dialog displays.
5. Select **Export user settings back to their User Profile**.
6. Click **OK**.

Profile Migration Export is enabled for users within the Personalization Group.

At logon, data from the database is copied into the user profile.

Changing Modes

The table below shows the behavior when changing Profile Migration modes.

Operating system	Profile version	Example profile path
Disabled	Import	If settings from a previous import operation exist for the Personalization Group, a dialog displays. The following options are available: • **Resume the previous import** - Existing settings will not be replaced, but registry, folder or file inclusions which do not have data will be imported. • **Start a new import** - Existing settings will be overwritten with imported user profile data. At logon, settings from the logged on user's profile are copied into the database.
Disabled	Export	At logon, settings from the database are copied into the logged on user's profile.
Import	Disabled	The import operation is stopped. It can be resumed, however users who have not been migrated will have their user profile settings overwritten.
Import	Export	The import operation is stopped and cannot be resumed. At logon, settings from the database are copied into the logged on user's profile.
Export	Disabled	The export operation is stopped and cannot be resumed.
Export	Import	The export operation is stopped and cannot be resumed. At logon, settings from the logged on user's profile are copied into the database.

Profile Migration PowerShell Interface

Profile Migration can be scripted to import or export application or Application Group data between the database and the Windows profile on the client.

It is recommended that Profile Migration is configured through the Environment Manager Personalization console. The cmdlet should be used only where granular control is required to migrate individual applications or Application Groups, such as moving data from ungrouped applications to Application Groups. The cmdlet can assist with the careful migration of profile data, such as where multiple versions of Microsoft Office are used concurrently within the environment.

To migrate data from ungrouped applications to Application Groups, export the application to the local profile and then import it into an Application Group.

The PowerShell cmdlet has the following behavior:

- It is supported only when Profile Migration is not enabled on the Personalization Server.
- Migration occurs as many times as the cmdlet is executed. The state is not recorded and it is the responsibility of the administrator to ensure it is used only as required.
- To ensure data integrity, the migration occurs only if there is no instance of an application running for the specified application or Application Group.
- Errors are presented through the raising of an exception after execution.

Help

Further help is available by entering the following command:

```
get-help <cmdlet name>
```

Load the Profile Migration PowerShell Module

The module is installed in the Environment Manager Agent directory. Use the following command to load the PowerShell module:

Import-Module "C:\Program Files\AppSense\Environment Manager\Agent\EmCmdlet.dll"

If you have changed the default install location, amend the file path accordingly.

Alternatively, use the following command to load the PowerShell module from the current installation directory:

Import-Module ((Get-ItemProperty 'HKLM:\SOFTWARE\AppSense\Environment Manager').ClientPath + 'EmCmdlet.dll'

Import Profiles Using the Profile Migration PowerShell Interface

The `Import-EMPManagedAppData` cmdlet performs a migration of profile data from the Windows Profile into a Managed Application profile.

The Managed Application's configured registry, folder and file inclusions and exclusions are used as the locations to import data from.

The Windows profile can be either the local profile or a roaming profile stored on a network location.

The following parameters are available:

Parameter	Description
`-App` (Mandatory)	The name of the managed application or managed Application Group against which to perform the import. This is the Display Name as seen in the Personalization Console.
`-ProfilePath` (Optional)	The path to the Windows Profile to use as the source of the data as an alternative to importing from the local profile. This path must be a Windows Profile Version agnostic path and so should not include any version suffix such. For example, a profile path of *\\server\share\user1.V2* should be entered as *\\server\share\user1*. Only profile versions that match the current operating system or earlier are supported. For example, it is not possible to import from a Windows 10 profile when running on a Windows 7 machine. An appropriate profile is selected at the configured location by looking for a version that matches the current operating system. If a matching profile is not found, then an earlier profile version is used. The use of Environment Variables specific to the current user session is supported.
`-ProfileAppDataPath` (Optional if ProfilePath is supplied)	When importing from a network profile, this parameter can be used to specify the path to Roaming AppData folder when it is not part of the user's profile location. The use of Environment Variables specific to the current user session is supported.
`-Merge` (Optional switch)	If specified, the action merges the personalized data with the data from the Windows Profile. The personalized data takes precedence and is not replaced. If not specified, the action clears the existing profile data before the import takes place.
`-Verbose` (Optional switch)	Provides verbose output of the PowerShell command for diagnostic purposes.

When application profiles are imported using the `Import-EMPManagedAppData` command, HIVE files are created in user's managed application profile and local AppSensevirtual cache. This is the behavior regardless of whether the UpgradeFBRtohive advanced setting is set to 'true' or 'false'. If set to false, managed applications continue to use the FBR method to virtualize and synchronize data. However, as HIVE files exist in user's managed application profile, data contained within the synchronized FBR file is not visible in Environment Manager Personalization Analysis. Therefore, applications do not appear to be synchronizing.

To continue using the Profile Migration PowerShell Interface, the UpgradeFBRtohive Advanced Setting must be set to 'true'.

If you do not want to continue using the HIVE files, they should be removed using the script in this Ivanti Community document: DOC-62059.

For more information about the UpgradeFBRtohive setting, see Advanced Settings.

Examples

The following shows an example of importing data from the local Windows Profile for the Managed Application Notepad:

```
Import-Module ((Get-ItemProperty 'HKLM:\SOFTWARE\AppSense\Environment Manager').ClientPath + 'EmCmdlet.dll')

Import-EMPManagedAppData -App Notepad
```

The following shows an example that could be used inside an Environment Manager Policy Custom Condition where the exit code of the script is used to determine if the condition result:

```
try
{
  Import-Module ((Get-ItemProperty 'HKLM:\SOFTWARE\AppSense\Environment Manager').ClientPath + 'EmCmdlet.dll')
  Import-EMPManagedAppData -App Notepad
}
catch
{
  # Exit with an error
  [System.Environment]::Exit(1)
}
```

Export Profiles Using the Profile Migration PowerShell Interface

The `Export-EMPManagedAppData` cmdlet performs a migration of profile data from a managed application or Application Group back to the Windows Profile.

The following parameters are available

Parameter	Description
`-App` (Mandatory)	The name of the managed application or managed Application Group against which to perform the export. This is the Display Name as seen in the Personalization

Parameter	Description
	Console.
`-Verbose` (Optional switch)	Provides verbose output of the PowerShell command for diagnostic purposes.

Excluded Users

If personalization is enabled, all users are assigned to a Personalization Group. Users with an Environment Manager agent installed and configuration deployed who do not fulfill the membership rules for any other group, are managed by the Default Users group.

However, personalization may not be required for all users. For example, you may not wish to save the personalization settings for system administrators who routinely log onto multiple users' machines. It is unlikely they would require their own desktop settings to roam with them onto each machine they log onto.

In order to exclude a specific user or computer from personalization create a Personalization Group with each option on the Settings tab disabled and with no managed applications, Application Groups or Windows Settings Groups configured. This effectively removes group members from user personalization.

By creating an appropriate membership rules, the users and computers which do not require personalization, can be excluded.

Endpoint Self-Service Tool

The Endpoint Self-Service tool provides monitoring and management of certain Environment Manager settings and data. It is available to users and managed endpoints for Personalization Groups which have it enabled.

The Endpoint Self-Service tool is available from the Environment Manager Information icon in the Windows System Tray. Right-click on the icon to access the functionality.

The Endpoint Self-Service Tool requires .NET4 to run. If this is unavailable, local audit event 9680 is created.

The options available from the Endpoint Self-Service tool vary depending on whether the user is a standard or administrative user. To accommodate these user types, the Endpoint Self-Service Tool has two operational modes:

- **Basic** - For standard users.
- **Advanced** - For users that are assigned an administrative role in the Personalization Database.

Enable the Endpoint Self-Service Tool

This process explains how to enable the Endpoint Self-Service tool for Personalization Groups.

1. In the User Personalization navigation pane select **Personalization Groups**.
2. Select a personalization group.
3. Select the **Endpoint Self-Service** tab.
4. Select one of the following options:
    - **Disabled** - The Endpoint Self-Service tool is not available for users in the selected Personalization Group.
    - **Enabled for all users in group** - The Endpoint Self-Service tool is available for members of the selected Personalization Group.
    - **Enabled if the following conditions are tru**e - The Endpoint Self-Service tool is only available for members of the selected Personalization Group, if certain conditions are met.

Any users or computers that have been specified in the Membership Rules for a Personalization Group have access to the tool when they log on.

Endpoint Self-Service Functionality for Standard Users

Any endpoints where the Endpoint Self-Service Tool is enabled for a Personalization Group can perform the following basic tasks:

- Rollback or delete Personalization data archives
- Show policy action progress

Archiving

The Archive Management dialog displays when a user selects the Archiving option from the Environment Manager Information System Tray icon. The dialog displays a list of all associated Applications, Application Groups and Windows Settings Group archives for that user.

Rollback

Select an Application or Windows Settings Group archive and click Rollback. All Personalization settings are returned to the state they were when the previous archive was created. Users are prompted to confirm that the rollback action is to be performed and are informed when the rollback is complete.

Delete

Select an Application or Windows Settings Group archive and click Delete. Any user settings contained within the selected archive are deleted.

Policy Action Progress

The Show Policy Action Progress option displays the percentage progress of any triggered copy folder actions.

Endpoint Self-Service Functionality for Administrative Users

Users that have the Environment Manager User role of Master Administrator or Administrator can access the tool locally on a managed endpoint or remotely.

For information on User Roles and how they are assigned, see User Roles.

Administrative users have access to both the basic and the advanced functionality of the Endpoint Self-Service tool. Administrators have access to Session Information, can use archive functionality, update settings and alerts and refresh the local cache.

Session Information

Select the Session Information option from the Environment Manager Information Windows System Tray icon from where you can view details of the managed endpoint and user.

The dialog has four information categories:

- **General Information** - Displays the User name, Personalization Server, the Personalization Group associated with the currently logged on user and the build version of the current Environment Manager agent. The status of the license and whether Offline cache mode is enabled is also displayed.
- **Application Personalization** - Displays details of any Application Groups and associated Applications that are assigned to the managed endpoint.
- **Windows Personalization** - Displays details of the Windows Settings Groups that are personalized on the managed endpoint and the date that Windows Personalization settings were last archived.
- **Global Includes and Excludes** - Displays the registry, folder and file includes and excludes that are applied on the managed endpoint.

Archiving

Select the Archiving option from the Environment Manager Information Windows System Tray icon to access the Archive Manager dialog. Use this dialog to perform the following tasks:

- **Create Archive** - Click **Create** to archive any current Application, Custom or Windows Settings Groups. To prevent the archive from being automatically deleted, select the **Protected** check box before you click **OK**.

Only one archive can be protected, if another is already set to be protected the most recent one is automatically set and any previous protection removed.

- **Edit Archives** - Select an archive and click **Edit** to amend the description of an Application Group archive. To prevent the archive from being automatically deleted, select the Protected check box before you click **OK**.
- **Rollback Archive** - Select an Application or Windows Settings Group archive and click **Rollback**. All Personalization settings are returned to the state they were when the selected archive was created. You will be prompted to confirm that the rollback action is to be performed and will be informed when the rollback is complete.
- **Delete Archives** - Select an Application, Custom or Windows Settings Group archive and click **Delete**. Any settings contained within the selected archive are deleted. To delete a protected archive, protection must first be removed.

Settings and Alerts

Use the Settings option from the Environment Manager Information Windows System Tray icon to select which action balloon notifications are displayed on managed endpoints. The Settings dialog can also be used to select a border color to surround the window frame of any managed application when in use.

Alerts

Alert notifications are displayed as standard balloon type notifications when actions are triggered. Select the required notification types:

- **Server link state** - Displays the status of the connection to the Personalization Server and the Personalization Server URL.
- **Sync to server** - Displays when the Application Settings or Application Groups Settings, on the managed endpoint have synchronized with those on the Personalization Server.
- **Sync from server** - Displays the Applications or Application Groups Settings on the Personalization Server have updated those on the endpoint.
- **Sync failure** - Displays when an attempted synchronization fails.
- **Managed Process start/stop** - Displays when a managed process starts and stops.
- **Virtualization service starts/stop** - Displays when the virtualization service is started or the service has stopped. If the service has stopped, the icon in the Windows System Tray displays a yellow warning icon. Any Applications or Application Group Settings previously handled are no longer being managed.
- **Virtualization service not running** - This alert notification displays if the virtualization service has not been started or is not running. If the service has stopped, the icon in the Windows System Tray displays a yellow warning icon. Any Applications or Application Group Settings previously handled are no longer being managed.
- **New configuration applied** - This information notification displays when a new configuration is applied to the managed endpoint.

- **Pre-cache complete** - This information notification displays when pre-caching is complete for all Applications and Applications Groups assigned to the managed endpoint. Pre-Caching is the process by which you download existing Application data from the Personalization Server to the local cache.
- **Folder copy/mirror/sync complete** - This information notification displays when folder copy actions are complete.

Windows Frame

To clearly identify a managed application on the endpoint, a colored border can be placed around the application window. Select **Show managed application frame** and chose the color from the **Border Color** drop-down list. When a managed application is in use the application has a colored border.

Refresh Local Cache

Use the **Refresh Local Cache** option to help speed up network access to data files by taking a copy of the data stored on the Personalization Server and refreshing the cached data on the managed endpoint. This will ensure the local Personalization cache is in sync with the Personalization Database

Using the Endpoint Self-Service Tool Remotely

Users assigned the Master Administrator or Administrator role can use this tool remotely for troubleshooting purposes. When remotely logged onto a machine, authorized users can run the **EndpointSelfService.exe** from the Environment Manger installed location, input their credentials and access all the administrator functionality from the Environment Manager Information dialog.

Application Personalization

The Application Personalization area of the console is used to configure a list of applications and Application Groups which can be included for personalization.

Application Processing Rules

When an application is opened on a managed endpoint, processing rules determine if it is managed and how it is managed. Applications can be marked as follows:

- **Managed** - The application or process is managed, either individually or as part of an Application Group.
- **Discovered** - The application is not managed or excluded but the Personalization Group settings has *Auto-discover user applications* applied.
- **Excluded** - The application has been added to the Application Exclusions list or is the child process of an excluded application. It will not be discovered or managed when run on a managed endpoint.
- **Passive** - The application is not managed but usage data is collected for analysis by the Application Data Collection.

Unless virtualization is disabled for the process, a Personalization Virtualization Component (PVC) configuration is created to redirect registry reads and writes and file and folder access to the virtual cache so that the process is virtualized.

Application Groups

Application Groups enable applications which interact together, using common registry keys and folders, to be managed as a single group for personalization.

Applications must be in an Application Group before they can be personalized. When creating an application, options are available to add it to a new or existing Application Group. This makes it easier to add new applications that share common settings with existing applications.

Inclusions and exclusions must be set at Application Group level. This ensures consistency across all applications within a group.

Applications in an Application Group share the same virtual cache. Personalization settings are only synchronized with the Personalization Server when:

- The initial application in the group is opened
- The last, open application in the group is closed

For example, if all Microsoft Office applications are managed within one group and Outlook, Word and Excel are opened in that sequence, synchronization occurs only when Outlook is opened. If Word, Outlook and Excel are closed in that sequence, synchronization occurs only when Excel is closed.

Add an Application Group

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Group**.
2. In the Personalization ribbon, click **Add Application Group**.

   The Add Application dialog displays.
3. Enter a name for the Application Group. Application Groups must not have the same name as existing applications or Application Groups.
4. Click **OK**.
5. The Application Group is created in the navigation pane.

Add Existing Applications to an Application Group

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Group**.
2. Select an application group.
3. From the Personalization ribbon, click **Add Application** > **Select Application**.

   The Select Applications dialog displays.
4. Select the required applications. Multiple applications can be selected using the Ctrl or Shift keys.
5. Click **OK**.

The selected applications are added to the Application Group.

Add a New Application to an Application Group from Application Data Collection (Automatic)

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Groups**.
2. Select an application group.
3. From the Personalization ribbon, click **Add Application** > **Select Application**.

   The Select Applications dialog displays.
4. Click **New** > **From Application Data Collection**.

   The Add Application - Data Collection dialog displays. The dialog lists applications that have been collected by Application Data Collection.

5. Select one of the following radio buttons to target specific application versions:
    - **Use Major Application Version** - Applications are grouped by their major version number. For example, 5.0 and 5.1 are grouped together, but 6.0 is separate.
    - **Use All Application Versions** - Applications are grouped, regardless of their version number. For example, 5.0, 5.1 and 6.0 are grouped together.
6. Select an application from the list.
7. Click **View automatic configuration details**.

    A read-only copy of the configuration displays.
8. From the snapshot taken at each application close, the following statistics are calculated and displayed alongside each registry key or folder path for all users that have run the application:
    - **Occurrences** - The total number of times that the registry path or folder path has been accessed by the application.
    - **Average Size** - The average size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as an average size of 150 bytes.
    - **Peak Size** - The largest recorded size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as a peak size of 200 bytes.

    The cumulative sizes of the Average Size and Peak Size displays at the bottom of the dialog. This information shows the potential profile size per user if the application is personalized.
9. Click **Done** to close the automatic configuration view.

    The automatic configuration closes.
10. Click **OK**.

    The Enter Details dialog displays.
11. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.
12. Click **OK**.
13. Select the new application in the list and click **OK**.

The application is created and added to the Application Group.

Add a New Application to an Application Group from Application Data Collection (Manual)

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Group**.

2. Select an application group.
3. From the Personalization ribbon, click **Add Application** > **Select Application** from the Personalization ribbon.

   The Select Applications dialog displays.

4. Click **New** > **From Application Data Collection**.

   The Add Application - Data Collection dialog displays. The dialog lists applications that have been collected by Application Data Collection.

5. Select one of the following radio buttons to target specific application versions:
6. **Use Major Application Version** - Applications are grouped by their major version number. For example, 5.0 and 5.1 are grouped together, but 6.0 is separate.
7. **Use All Application Versions** - Applications are grouped, regardless of their version number. For example, 5.0, 5.1 and 6.0 are grouped together.
8. Tick **No, I want to configure this application manually (advanced)**.
9. Click **Configure**.

   The dialog lists all registry keys and folder paths which have been collected by Application Data Collection for the selected application.

10. From the snapshot taken at each application close, the following statistics are calculated and displayed alongside each registry key or folder path for all users that have run the application:
    - **Occurrences** - The total number of times that the registry path or folder path has been accessed by the application.
    - **Average Size** - The average size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as an average size of 150 bytes.
    - **Peak Size** - The largest recorded size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as a peak size of 200 bytes.
11. If required, tick **Hide paths which are rarely personalized** to filter out paths which are not recommended for inclusion.
12. Tick the registry and folder paths to be added as inclusions for the Application Group.
13. As paths are selected and deselected, the Application Profile Size updates with the cumulative sizes of the Average Size and Peak Size for the selected paths. This information shows the potential profile size per user if the application is personalized.
14. Click **OK**.

    The Enter Details dialog displays.

15. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.
16. Click **OK**.

    The application is created and is listed in the Select Applications dialog.

17. Select the new application in the list and click **OK**.

    The application is added to the Application Group.

Add a New Application by Name to an Application Group

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Groups**.
2. Select an application group.
3. From the Personalization ribbon, click **Add Application** > **Select Application** from the Personalization ribbon.

   The Select Applications displays.

4. Click **New** > **By Name**.
5. In the Application field, enter an application executable name or click the ellipsis (...) to select an application from the file system.
6. Optionally, in the Folder field, enter a folder path or click the ellipsis to select a folder from the file system. The application is managed only if it is located in the specified folder.

   If the field is left blank, all applications matching the entered criteria are managed, regardless of location.

7. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.
8. Optionally, in the Operating System and Application Version fields, specify regular expressions to target a specific operating system or application version. Alternatively, use the **.*** default regular expression to include all operating systems and application versions.

   The specified combination of executable name, operating system and application version must not match existing applications.

9. Click **OK**.

   The application is created and is listed in the Select Applications dialog.

10. Select the new application in the list and click **OK**.

The application is added to the Application Group.

Path Based Configuration of Application Groups

When configuring an application group, a file path to a folder can be specified so that any application run from that location is managed. This means that applications do not need to be individually added to a group if those applications are in the managed folder.

For example, rather than adding each individual Microsoft Office application to a group, you can define the path to the Microsoft Office folder. When Word, Excel and Outlook are opened from this location, they are managed by the Microsoft Office application group.

Configure an Application Group Using Managed Folders

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Groups**.
2. Select an application group.
3. From the Personalization ribbon, click **Add Managed Folder**.

   The Add Managed Folder dialog displays.
4. Enter a valid path or browse to the required folder.

   Paths must adhere to the following rules:

   - Local and mapped drives are supported
   - UNC paths are not supported
   - For the applications to be personalized, the path must exist on the managed endpoint
   - CSIDL paths are supported and are expanded to suit the target operating system
   - All paths act as wildcards; an asterisk (*) is not required
   - Standard application group rules apply regarding synchronization with the Personalization Server.
5. Enter an Operating System. Alternatively, to include all operating systems, use the default regular expression (.*)
6. Select the **Manage all subfolders** checkbox as required.

   If unchecked, only applications in the top level folder will be managed.
7. Click **OK** to add the folder to the Managed Folders for the personalization group.

Application Group Templates

Application Group templates contain configuration details about the Application Groups and applications within the group.

Export an Application Group

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Groups**.
2. Right-click an application group and select **Export Application Group Template**.

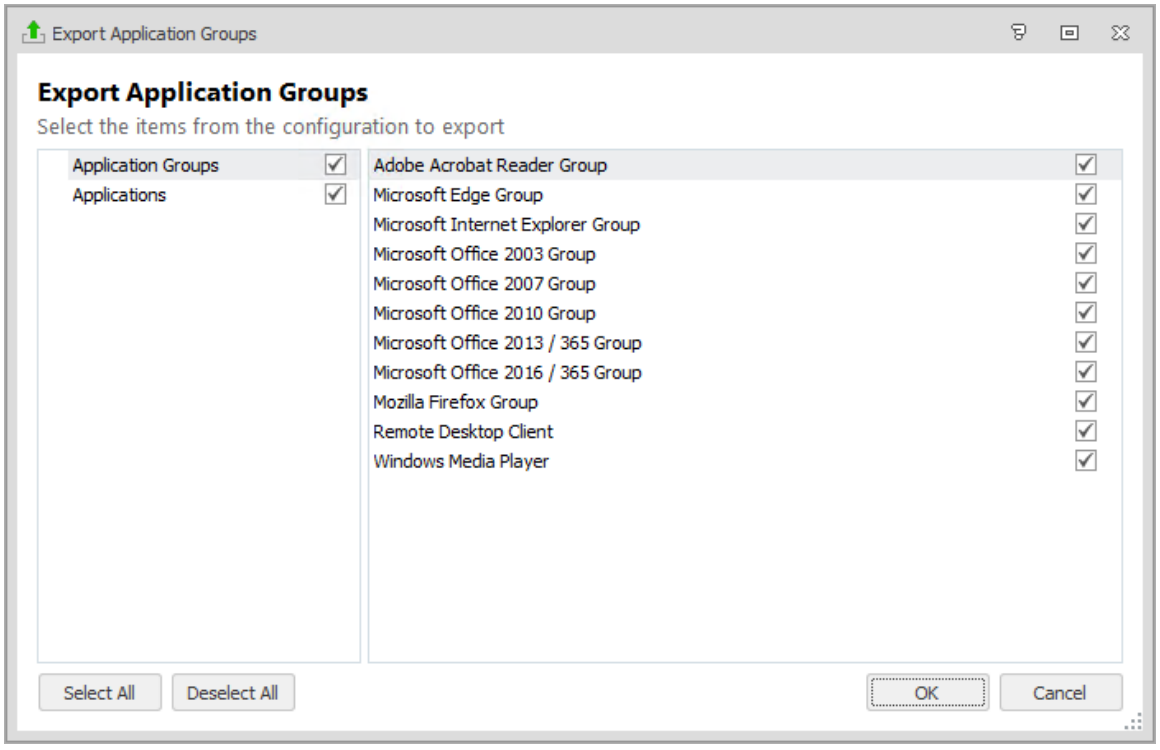
   The Save As dialog displays.
3. Select a location to save the template and click **OK**.

An XML file containing the configuration details about the Application Group and applications within the group is created in the specified location.

Export multiple Application Groups

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization**.
2. Right-click **Application Groups** and select **Export Application Group Template** from the context menu.

   The Export Application Groups dialog displays.



   You can view individual applications and application groups by selecting the appropriate item in the left-hand column of the dialog.

3. Select the Applications and Application Groups to export - you can select a combination of applications and groups.
4. Click **OK**.

   The Save As dialog displays.
5. Select a location to save the template and click **OK**.

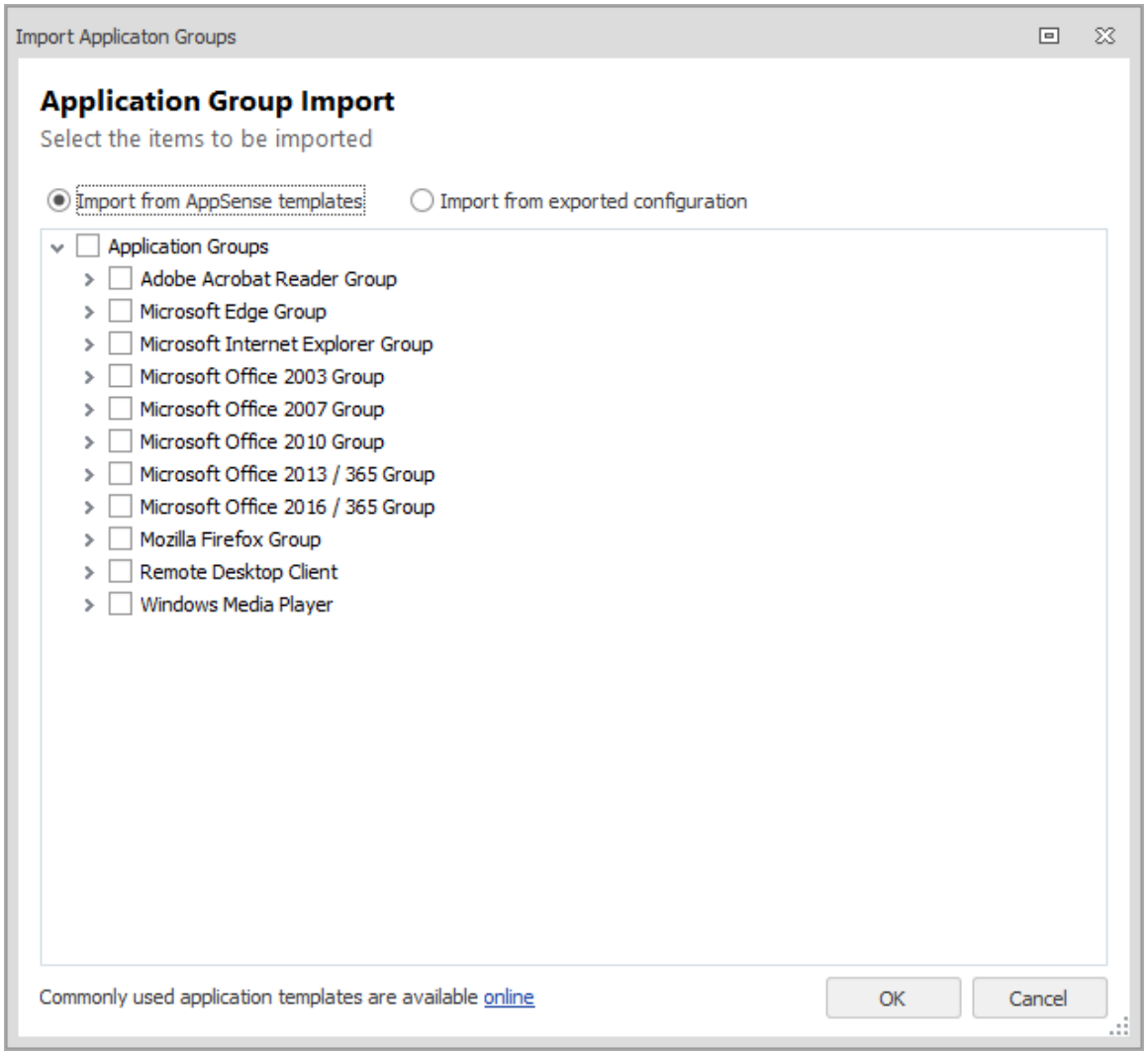
An XML file containing the configuration details about the selected Application Groups and applications within the groups is created in the specified location.

Import Application Groups

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization**.

2. Right-click **Application Groups** and select **Import Application Group Template**.

   The Import Application Groups dialog displays.



3. Select one of the following radio buttons:
    - **Import from AppSense templates** - Application group templates are available for commonly personalized applications, such as Microsoft Edge and Adobe Acrobat Reader. These templates contain recommended inclusions and exclusions for personalization.
    - **Import from exported configuration** - Application groups can be imported from an exported personalization configuration or Application Group Template. When selected, a file browser displays for a personalization configuration or application group template to be selected.

    You can also download the latest templates from the Ivanti Community by selecting the link at the bottom of the dialog.
4. Select the Applications Groups to import. To select all Application Groups, select **Application Groups** at the top of the list.
5. Click **OK**.

The selected Application Groups are imported into the configuration.

Applications

The applications list allows a library of applications to be configured which can be quickly added to Application Group and Personalization Groups for personalization.

Applications can be specified by version and operating system allowing different instances of the same application to be personalized independently, even when the executable has the same name.

Add a New Application from Application Data Collection (Automatic)

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Applications**.
2. In the Personalization ribbon, click **Add Application** > **From Application Data Collection**.

    The Add Application - Data Collection dialog displays. The dialog lists applications that have been collected by Application Data Collection.
3. Select one of the following radio buttons to target specific application versions:
    - **Use Major Application Version** - Applications are grouped by their major version number. For example, 5.0 and 5.1 are grouped together, but 6.0 is separate.
    - **Use All Application Versions** - Applications are grouped, regardless of their version number. For example, 5.0, 5.1 and 6.0 are grouped together.
4. Select an application from the list.

5. Click **View automatic configuration details**.

   A read-only copy of the configuration displays.

   From the snapshot taken at each application close, the following statistics are calculated and displayed alongside each registry key or folder path for all users that have run the application:

   - **Occurrences** - The total number of times that the registry path or folder path has been accessed by the application.
   - **Average Size** - The average size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as an average size of 150 bytes.
   - **Peak Size** - The largest recorded size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as a peak size of 200 bytes.

   The cumulative sizes of the Average Size and Peak Size displays at the bottom of the dialog. This information shows the potential profile size per user if the application is personalized.

6. Click **Done** to close the automatic configuration view.

   The automatic configuration closes.

7. Click **OK**.

   The Enter Details dialog displays.

8. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.

   Applications must be added to a new or existing Application Group:

   - **New Application Group** - Specify the Application Group name in the Create New Application Group field. Application Groups must not have the same name as existing applications or Application Groups.
   - **Existing Application Group** - Select an existing Application Group in the Add to Existing Application Group field.

9. Click **OK**.

The application is created and is visible within the Applications work area.

The registry and folder paths from the Application Data Collection automatic configuration are added as inclusions for the application. The global registry, folder and file path inclusions are added as exclusions for the application to ensure that unexpected data is not captured for the application.

Add a New Application from Application Data Collection (Manual)

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Applications**.
2. In the Personalization ribbon, click **Add Application** > **From Application Data Collection**.

   The Add Application - Data Collection dialog displays. The dialog lists applications that have been collected by Application Data Collection.
3. Select one of the following radio buttons to target specific application versions:
   - **Use Major Application Version** - Applications are grouped by their major version number. For example, 5.0 and 5.1 are together, but 6.0 is separate.
   - **Use All Application Versions** - Applications are grouped, regardless of their version number. For example, 5.0, 5.1 and 6.0 are grouped together.
4. Tick **No, I want to configure this application manually (advanced)**.
5. Click **Configure**.

   The dialog lists all registry keys and folder paths which have been collected by Application Data Collection for the selected application.

   From the snapshot taken at each application close, the following statistics are calculated and displayed alongside each registry key or folder path for all users that have run the application:

   - **Occurrences** - The total number of times that the registry path or folder path has been accessed by the application.
   - **Average Size** - The average size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as an average size of 150 bytes.
   - **Peak Size** - The largest recorded size of the data in the registry key or folder from each application close. For example, a size of 100 bytes at the first application close and a size of 200 bytes at the second application close displays as a peak size of 200 bytes.
6. If required, tick Hide paths which are rarely personalized to filter out paths which are not recommended for inclusion.
7. Tick the registry and folder paths to be added as inclusions for the Application Group.

   As paths are selected and deselected, the Application Profile Size updates with the cumulative sizes of the Average Size and Peak Size for the selected paths. This information shows the potential profile size per user if the application is personalized.
8. Click **OK**.

   The Enter Details dialog displays.

9. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.

   Applications must be added to a new or existing Application Group:

   - **New Application Group** - Specify the Application Group name in the Create New Application Group field. Application Groups must not have the same name as existing applications or Application Groups.
   - **Existing Application Group** - Select an existing Application Group in the Add to Existing Application Group field.

   The application is created and is visible within the Applications work area.

10. Click **OK**.

The registry and folder paths from the Application Data Collection manual configuration are added as inclusions for the application. The global registry, folder and file path inclusions are added as exclusions for the application to ensure that unexpected data is not captured for the application.

Add a New Application by Name

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Group**.
2. Select an application group.
3. From the Personalization ribbon, click **Add Application** > **Select Application**.

   The Select Applications displays.

4. Click **New** > **By Name**.

   The Add an Application dialog displays.

5. In the Application field, enter an application executable name or click the ellipsis (...) to select an application from the file system.
6. Optionally, in the Folder field, enter a folder path or click the ellipsis to select a folder from the file system. The application is managed only if it is located in the specified folder. If the field is left blank, all applications matching the entered criteria are managed, regardless of location.
7. In the Name field, enter a name to uniquely identify the application within the Environment Manager console. Applications must not have the same name as existing applications or Application Groups.
8. Optionally, in the Operating System and Application Version fields, specify regular expressions to target a specific operating system or application version. Alternatively, use the **.*** default regular expression to include all operating systems and application versions.

9. Click **OK**.

   The application is created and is listed in the Select Applications dialog.

10. Select the new application in the list and click **OK**.

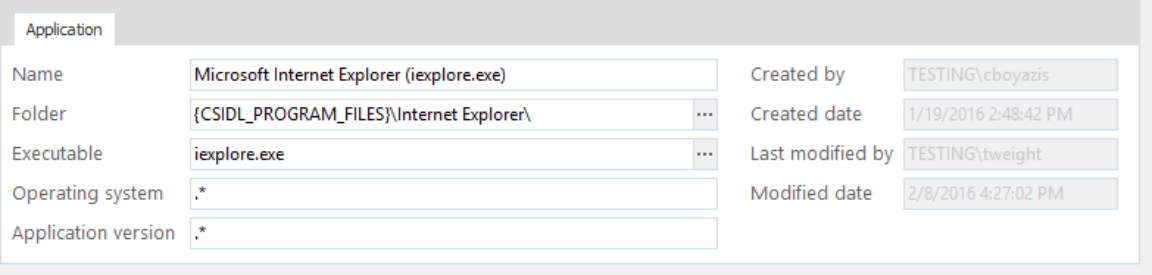
The application is added to the Application Group.

Edit Application Properties

Once an application has been added to the Applications list, its details can be amended as required.

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application**.;
2. The available applications are listed in the work area.
3. Select the application you want to edit.

   Details of the application are displayed at the bottom of the work area.



4. Update the required properties:
   - **Name** - The name given to the application which appears in the application list. This can be changed as required but must not duplicate an existing application name.
   - **Folder** - The folder path specified for the application. Only matching applications in this folder are managed. The path can be amended or deleted.
   - **Executable** - The name of the executable file for the application. This can be entered directly or browsed for using the ellipsis. Unlike the application name, the executable name can be a duplicate of an existing executable. This enables different versions and operating systems to be catered for.
   - **Operating System** - Make the application specific to an operating system using regular expressions or by entering a specific OS. The default regular expression (.*) matches all operating systems
   - **Application Version** - Manage a specific version of the application by entering a specific version number or by using a regular expression. The default regular expression (.*) matches all version numbers.

The combination of Application executable name, Operating System and Application Version must be unique.

Adding a regular expression such as 11.* matches anywhere in the version string, for example, in 11.1.2.3 and 4.5.11.2.

To match only the start of the string, prefix the regular expression with a caret (^). For example, ^11.* matches 11.1.2.3 but does not match 4.5.11.2.

The Application tab also includes creation and modification dates and details of the user who performed the actions.

The regular expressions used in Environment Manager conform to Microsoft CAtIRegExp Class framework.

5. Click away from the fields, such as within the work area, to automatically update the edited details in the Application - User list.

Delete an Application from the Applications List

To delete an application, select it from the applications list, right-click and select **Delete**.

Environment Manager checks where the application is referenced in the configuration and displays any dependencies the application has, such as belonging to an application or personalization group. Use this information to amend your personalization configuration if required.

Deleting an application removes every instance of that application; it will be removed from all application and Personalization groups

Inclusions and Exclusions

Specific registry keys, registry values, folders and files can be included in or excluded from Personalization at the following levels:

- Application Group - Inclusions and exclusions that apply to all applications in an Application Group. It is recommended that inclusions and exclusions are added at Application Group level.
- Global - Inclusions and exclusions that apply to all managed applications, unless contradicted at Application Group or application level.
- Application - Inclusions and exclusions that apply to individual applications. Application level inclusions and exclusions can be viewed or edited only when ungrouped applications exist that are not part of any Application Group.

Application Group inclusions and exclusions take precedence over those set at global and application levels. This ensures consistency across all applications within a group.

Files with .tmp extensions are excluded by default. This can cause issues with some managed applications if the virtual cache is on a different drive than the user's profile. If you want to use the virtual cache on a different drive, remove .tmp from the global file exclusion list.

Files and folders, registry keys and values can be excluded using Personalization Analysis reports.

Inclusion and Exclusion Rules

The following rules apply to inclusions and exclusions:

- Everything is excluded by default - to personalize something, it must be explicitly included.
- Exclusions take priority over inclusions, except where the include path is deeper.
- Inclusions and exclusions apply to the path and all sub-folders, subject to the rules.
- A filename added to exclusions will exclude that file from all locations. For inclusions, the full file path must be specified. For example, File.tmp is a valid exclusion but an invalid inclusion.
- Wildcards can be used anywhere in a registry path inclusion and exclusion. However, for files, wildcards can be only be used for the filename - the path cannot include wildcards.

Using wildcards in includes and excludes can affect performance by increasing processing times.

Inclusion and Exclusion Examples

The two tables below show examples of inclusions and exclusions and the behavior displayed in certain situations for files, folders and registry keys.

Registry

Include Path	Exclude Path	Behavior
		Exclude everything Nothing is personalized as to personalize something, it must be explicitly included.
HKCU\Software\Key	HKCU\Software\Key	**Exclude HKCU\Software\Key** The registry exclusion is applied as exclusions take priority over inclusions.
HKCU\Software\Key	HKCU\Software	**Exclude HKCU\SoftwareInclude HKCU\Software\Key** Although the inclusion is within the exclusion path, the registry inclusion is applied as its path is deeper.

Include Path	Exclude Path	Behavior
HKCU\Software	HKCU\Software\Key	**Include HKCU\SoftwareExclude HKCU\Software\Key** Although the exclusion is within the inclusion path, the registry exclusion is applied as its path is deeper.
HKCU\Software\Key\Value	HKCU\Software\Key\Value	**Exclude HKCU\Software\Key\Value** The registry exclusion is applied as exclusions take priority over inclusions.
HKCU\Software\Key\Value	HKCU\Software\Key	**Include HKCU\Software\Key\ValueExclude HKCU\Software\Key** Although the inclusion is within the exclusion path, the registry inclusion is applied as its path is deeper.
HKCU\Software\Key	HKCU\Software\Key\Value	**Include HKCU\Software\KeyExclude HKCU\Software\Key\Value** Although the exclusion is within the inclusion path, the registry exclusion is applied as its path is deeper.

File and Folder

Include Path	Exclude Path	Behavior
		Exclude everything Nothing is personalized as to personalize something, it must be explicitly included.
C:\Folder	C:\Folder	**Exclude C:\Folder** The folder exclusion is applied as exclusions take priority over inclusions.
C:\Folder\AppSense	C:\Folder	**Exclude C:\FolderInclude C:\Folder\AppSense** Although the inclusion is within the exclusion path, the folder inclusion is applied as its path is deeper.
C:\Folder	C:\Folder\AppSense	**Include C:\FolderExclude C:\Folder\AppSense** Although the

Include Path	Exclude Path	Behavior
		exclusion is within the inclusion path, the folder exclusion is applied as its path is deeper.
C:\File.tmp	C:\File.tmp	**Exclude C:\File.tmp** The file exclusion is applied as exclusions take priority over inclusions.
C:\Folder\File.tmp	File.tmp	**Exclude C:\File.tmp** The file exclusion is applied as full paths are not required for exclusions and they take priority over inclusions
C:\Folder\File.tmp	C:\Folder	**Include C:\Folder\File.tmp** The file inclusion is applied as the path is deeper. As everything is excluded by default, it is not recommended that whole folders are excluded as this requires unnecessary processing which has a negative effect on performance.
C:\Folder	C:\Folder\File.tmp	**Exclude C:\Folder\File.tmp** The file exclusion is applied as the path is deeper.

Application Group Inclusions and Exclusions

Inclusions and exclusions for registry, folder and file paths can be added that apply to all applications within an Application Group.

It is recommended that inclusions and exclusions are added at Application Group level.

Add Application Group Inclusions using Application Data Collection

Application Data Collection passively collects data from managed endpoints as users run applications.

Registry key and folder paths that are written to and read from are recorded for each application. On application close, the data is stored in the Environment Manager Personalization database.

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Group**.
2. Select an application group.

3. From the Personalization ribbon, click **Add Application** > **Select Application**.

   The Select Applications dialog displays.

4. Click **New** > **From Application Data Collection**.

   The Add Application - Data Collection dialog displays. The dialog lists applications that have been collected by Application Data Collection.

5. Select the application from which to add the folder or registry inclusions.
6. Tick **No, I want to configure this application manually (advanced)**.
7. Click **Configure**.

   The dialog lists all registry keys and folder paths which have been collected by Application Data Collection for the selected application. Existing inclusions are selected.

8. Tick the registry and folder paths to be added as inclusions for the Application Group. Unless explicitly excluded, child paths are included with their parent path. When a parent path is selected, the child paths are automatically deselected and disabled.
9. Click **OK**.

   The Enter Details dialog displays. The Application name is read-only.

10. Click **OK**.

The selected registry and folder paths are added as inclusions to the Application Group.

Add Application Group Registry Inclusions or Exclusions Manually

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Groups**.
2. Select an application group.
3. Select the **Registry** tab.
4. In either the Include or Exclude area and select **Add Registry Key**.

   The Select Registry Key dialog displays.

5. In the Key field, select the ellipsis (...) to browse for the registry key or manually enter the path and key name into the field.

   Wildcards can be used anywhere in a registry path to represent one or more characters. For example, adding *.0 to the path for Microsoft Outlook means all versions of Outlook can be included or excluded with one entry.
   HKCU\Software\Microsoft\Office*.0\Outlook

   The Browse Registry dialog displays. You can select from your local computer, current user or click Connect to display the Active Directory Select Computer dialog to select another computer to browse.

6. Locate the required Registry Key and click **OK**.

   The selected registry key is entered in the Select Registry Key dialog.

7. Click **OK**.

The registry key is added as an inclusion or exclusion for the Application Group.

Add Application Group Folder Inclusions or Exclusions Manually

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Group**.
2. Select an application group.
3. Select the **Folder** tab.
4. In either the Include or Exclude area and select **Add Folder**.

   The Select Folder dialog displays.

5. In the Path field, select the ellipsis (...) to browse for the folder. The path can also be entered manually into the field.

   The Browse for Folder dialog displays. You can select an existing folder from your local computer or click the **Make New Folder** button to create a new folder for inclusion or exclusion.

6. Locate the required folder and click **OK**.
7. The selected folder path is entered in the Select Folder dialog.
8. Click **OK**.

The folder path is added as an inclusion or exclusion for the Application Group.

Add Application Group File Inclusions or Exclusions Manually

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Application Group**.
2. Select an application group.
3. Select the **File** tab.
4. In either the Include or Exclude area and select **Add File**.

   The Select File dialog displays.

5. In the Path field, select the ellipsis (...) to browse for the file. The path can also be entered manually into the field.
6. Locate the required file and click **OK**.

The selected file path is entered in the Select File dialog.

7. Click **OK**.

The file path is added as an inclusion or exclusion for the Application Group.

Global Inclusions and Exclusions

Inclusions and exclusions for registry, folder and file paths can be added that apply to all managed applications, unless contradicted at Application Group or application level.

It is recommended that inclusions and exclusions are added at Application Group level.

Add Global Registry Inclusions or Exclusions

1. Select the User Personalization navigation button.
2. From the Manage ribbon, click **Global Application Settings**.
3. Select the **Registry** tab.
4. Right-click in either the Include or Exclude area and select **Add Registry Key**.

   The Select Registry Key dialog displays.

5. In the Key field, select the ellipsis (...) to browse for the registry key or manually enter the path and key name into the field.

   Wildcards can be used anywhere in a registry path to represent one or more characters.
   For example, adding *.0 to the path for Microsoft Outlook means all versions of Outlook can be included or excluded with one entry.
   HKCU\Software\Microsoft\Office*.0\Outlook

   The Browse Registry dialog displays. You can select from your local computer, current user or click Connect to display the Active Directory Select Computer dialog to select another computer to browse.

6. Locate the required Registry Key and click **OK**.

   The selected registry key is entered in the Select Registry Key dialog.

7. Click **OK**.
8. The registry key is added as a global inclusion or exclusion.

Add Global Folder Inclusions or Exclusions

1. Select the User Personalization navigation button.
2. From the Manage ribbon, click **Global Application Settings**.

3. Select the **Folder** tab.
4. Right-click in either the **Include** or **Exclude** area and select **Add Folder**.

   The Select Folder dialog displays.
5. In the Path field, select the ellipsis (...) to browse for the folder. The path can also be entered manually into the field.

   The Browse for Folder dialog displays. You can select an existing folder from your local computer or click the **Make New Folder** button to create a new folder for inclusion or exclusion.
6. Locate the required folder and click **OK**.

   The selected folder path is entered in the Select Folder dialog.
7. Click **OK**.

The folder path is added as a global inclusion or exclusion.

Add Global File Inclusions or Exclusions

1. Select the User Personalization navigation button.
2. From the Manage ribbon, click **Global Application Settings**.
3. Select the **File** tab.
4. Right-click in the **Include** or **Exclude** areas and select **Add File**.

   The Select File dialog displays.
5. In the Path field, select the ellipsis (...) to browse for the file. The path can also be entered manually into the field.
6. Locate the required file and click **OK**.

   The selected file path is entered in the Select File dialog.
7. Click **OK**.

The file path is added as a global inclusion or exclusion.

Application Inclusions and Exclusions

Where ungrouped applications exist that are not part of any Application Group, inclusions and exclusions for registry, folder and file paths can be added to an individual application.

It is recommended that inclusions and exclusions are added at Application Group level.

Add Application Registry Inclusions or Exclusions

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Applications**.
2. Select an application in the work area.
3. Select the **Registry** tab.
4. Right-click in either the Include or Exclude area and select **Add Registry Key**.

   The Select Registry Key dialog displays.
5. In the Key field, select the ellipsis (...) to browse for the registry key or manually enter the path and key name into the field.

   Wildcards can be used anywhere in a registry path to represent one or more characters.
   For example, adding *.0 to the path for Microsoft Outlook means all versions of Outlook can be included or excluded with one entry.
   HKCU\Software\Microsoft\Office*.0\Outlook

   The Browse Registry dialog displays. You can select from your local computer, current user or click Connect to display the Active Directory Select Computer dialog to select another computer to browse.
6. Locate the required Registry Key and click **OK**.

   The selected registry key is entered in the Select Registry Key dialog.
7. Click **OK**.

The registry key is added as an inclusion or exclusion for the application.

Add Application Folder Inclusions or Exclusions

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Applications**.
2. Select an application in the work area.
3. Select the **Folder** tab.
4. Right-click in either the **Include** or **Exclude** area and select **Add Folder**.

   The Select Folder dialog displays.

5. In the Path field, select the ellipsis (...) to browse for the folder. The path can also be entered manually into the field.

   The Browse for Folder dialog displays. You can select an existing folder from your local computer or click the **Make New Folder** button to create a new folder for inclusion or exclusion.

6. Locate the required folder and click **OK**.

   The selected folder path is entered in the Select Folder dialog.

7. Click **OK**.

The folder path is added as an inclusion or exclusion for the application.

Add Application File Inclusions or Exclusions

1. In the User Personalization navigation tree, select **Personalization Settings** > **Application Personalization** > **Applications**.
2. Select an application in the work area.
3. Select the **File** tab.
4. Right-click in the **Include** or **Exclude** areas and select **Add File**.

   The Select File dialog displays.

5. In the Path field, select the ellipsis (...) to browse for the file. The path can also be entered manually into the field.
6. Locate the required file and click **OK**.

   The selected file path is entered in the Select File dialog.

7. Click **OK**.

The file path is added as an inclusion or exclusion for the application.

Application Data Collection

Application Data Collection passively collects data from managed endpoints as users run applications. The collected data can be used to create new applications and add to registry and folder inclusions to existing Application Groups.

Registry key and folder paths that are written to and read from are recorded for each application. On application close, the data is stored in the Environment Manager Personalization database.

The registry and folder paths from the Application Data Collection configuration are added as inclusions. The global registry, folder and file path inclusions are added as exclusions for the Application Group to ensure that unexpected data is not captured.

Note: Application Data Collection does not capture Microsoft Edge settings. To personalize Microsoft Edge, import the Application Group Templates.

Caution: Enabling Application Data Collection causes an increase in system utilization on managed endpoints.
It is recommended that Application Data Collection is disabled when no longer required.

Add New Applications

New applications can be added to the below locations using Application Data Collection.

Location	Process
Personalization Groups	Add a New Application to a Personalization Group from Application Data Collection
Application Groups	Add a New Application to an Application Group from Application Data Collection (Automatic)Add a New Application to an Application Group from Application Data Collection (Manual)
Applications	Add a New Application from Application Data Collection (Automatic)Add a New Application from Application Data Collection (Manual)

Add Inclusions

Registry and folder inclusions can be added to existing Application Groups using Application Data Collection.

See Add Application Group Inclusions using Application Data Collection

Windows Personalization

Windows Settings, such as wallpaper selection, mouse options and accessibility features, can be personalized for managed users through Environment Manager Windows Personalization. This is achieved by personalizing the appropriate registry keys and values, files and folders. The settings a user applies to their desktop are saved to the personalization database when a user logs off and restored when the user logs onto any managed endpoint.

Windows Settings Groups

Windows Settings can be grouped together in Windows Settings Groups and added to Personalization Groups in order to personalize the appropriate settings for groups of users. This allows a higher level of granularity, enabling settings to be personalized and rolled back in individual groups. Further control can be achieved by adding conditions that specify how groups of Windows Settings are applied.

Environment Manager contains default Windows Settings Groups that personalize the most common Windows Settings. When you expand Windows Personalization, the pre-configured Windows Settings Groups are displayed with any groups you have added yourself.

All groups can be used as they are, edited to your requirements or new groups, containing existing or Custom Windows Settings, can be created. Groups can also be cloned to create a new group based on the settings of an existing one.

Windows Settings Groups and Inclusion Logic

When you assign a Windows Settings Group containing registry or file inclusions to a Personalization Group, this automatically excludes those included locations from application virtualization for that Personalization Group. When a condition has been configured for a Windows Settings Group, the following logic applies on the endpoint:

- If the condition evaluates as True, the Windows Settings Group data is applied to the user's session and the inclusion paths are excluded globally from application virtualization.
- If the condition evaluates as False, the Windows Settings Group data is preserved in the database but is not applied to the user's session. The inclusion paths in the Windows Settings Group are still excluded from the app bubble. When the user roams back to the machine with a passing condition, the data is applied.

Create a Windows Settings Group

1. In the User Personalization navigation tree, select **Windows Personalization**.
2. From the Personalization ribbon, click **Add Windows Settings Group**.

3. Enter a name and an optional description and click **OK**. The Windows Settings Group name must not be a duplicate of an existing group or a reserved name, for example, W7 and W8.

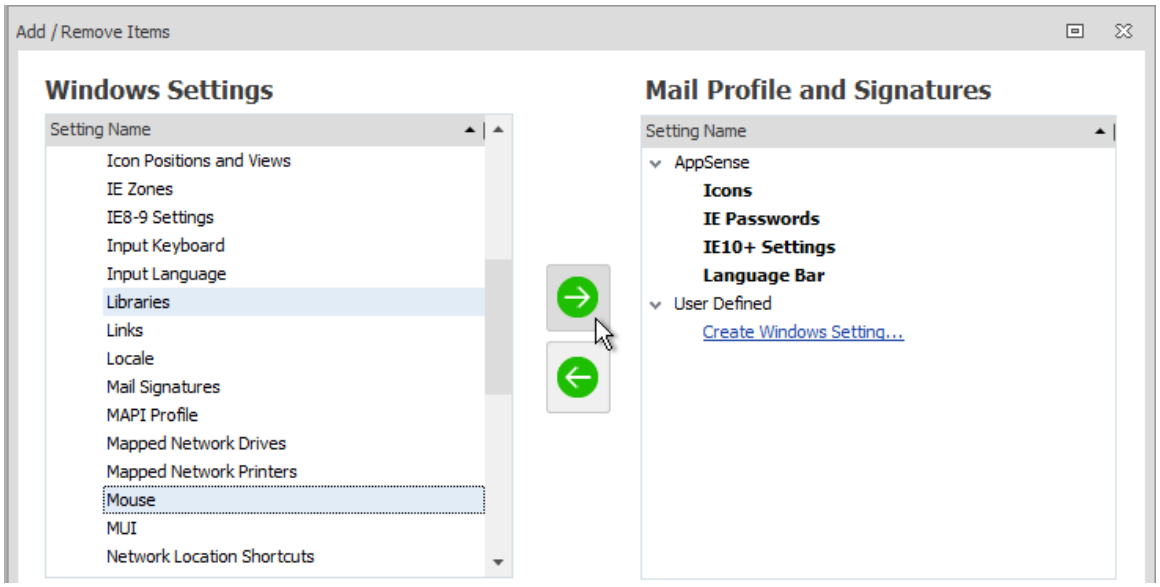
   The Windows Settings Group displays in the work area.

4. Click **Add/Remove**.

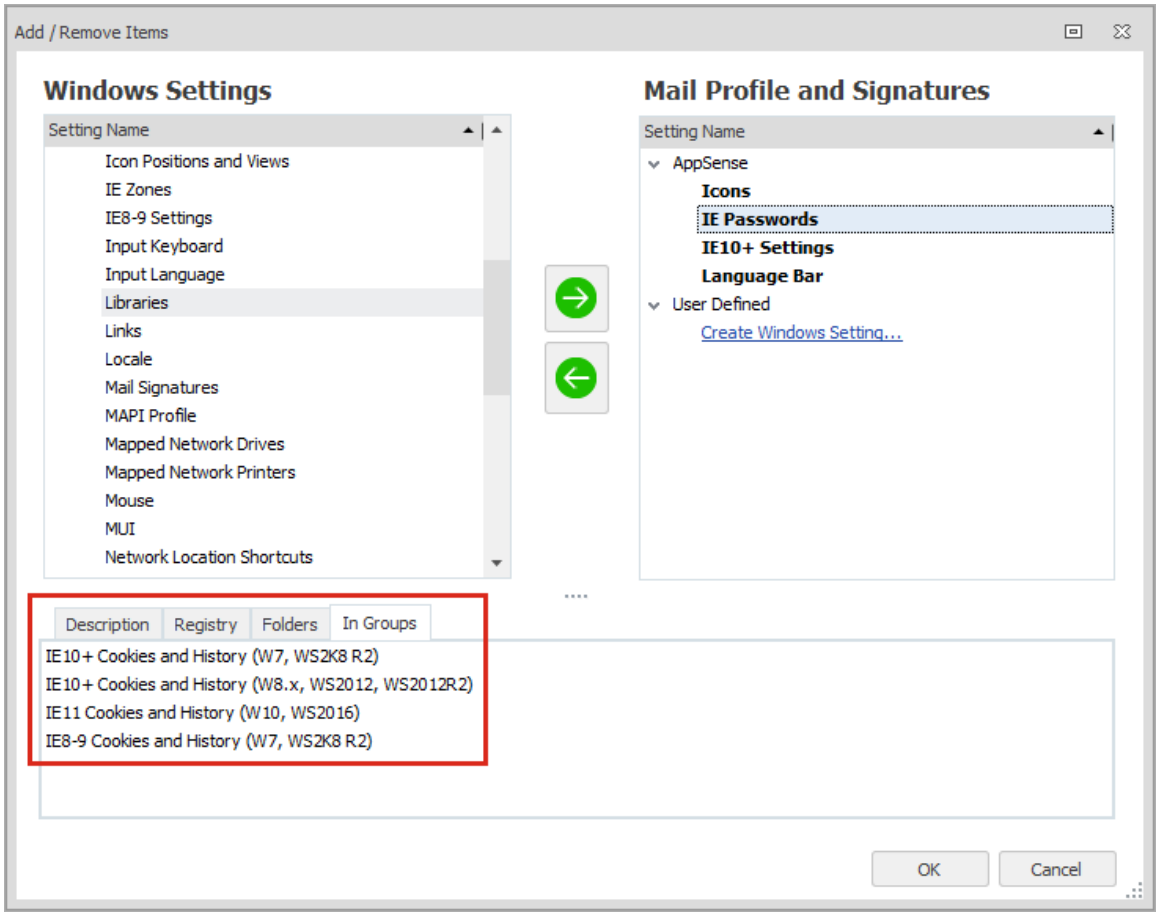
   The Add/Remove Items dialog displays.

5. Select the required settings from the left pane and click the right arrow to add them to the Windows Settings Group.

6. Multiple settings can be selected using the **Ctrl** or **Shift** keys.



An emboldened setting means that the setting is used in another Windows Settings Group. To see which groups it is used in, highlight the setting and select the **In Groups** tab at the bottom of the dialog.



To see which registry keys and values, files and folders are personalized, highlight a Windows Setting on either side of the dialog and select the appropriate tab.

If the setting you want to personalize is not available, click the **Create Windows Setting** link to configure a Custom Windows Setting.

7. Once you have added all the required settings, click **OK** to save the Windows Settings Group.

The settings you have added for the group are displayed in the work area.

Settings can be deleted from the group or you can click the **Add/Remove** button to fully edit the group.

Add Conditions to a Windows Setting Group

1. Create conditions to determine when Windows Settings are applied, for example, when a particular registry key or folder exists.
2. Select a Windows Settings Group.
3. Click **AddCondition**.

4. Enter a name for the Windows Settings Group Condition. If you want to use the condition in another Windows Settings Group, you must enter a name. If you are adding conditions for this group only, a name is not required.
5. Select the **Make available for reuse** checkbox if you want the condition to be available for other Windows Settings Groups.

   To apply an existing Windows Settings Group Condition, select the **Use existing condition** radio button and choose the required condition from the drop-down. The list includes conditions you have already configured and built-in conditions for Windows 7 and Windows 8. Conditions for Windows 10 operating systems are only available as custom conditions.
6. Click the **Conditions** drop-down and select a **condition**.
7. You can add multiple conditions and utilize AND/OR statements to create a configuration of conditions to apply to the Windows Settings Group as required. Move, remove and edit conditions using the toolbar.
8. Click **OK** to save the Windows Settings Group Condition. The condition is applied to the Windows Settings Group and displayed in the work area.
9. Edit a Windows Settings Group
10. Select a Windows Settings Group to edit the settings managed by that group and to manage its conditions. The following options are available:
11. **Add/Remove** - Open the Add/Remove Items dialog to configure the Windows Settings for the group.
12. **Delete** - Delete the selected Windows Setting.
13. **Delete All** - Delete all Windows Settings for the group.
14. **Edit Condition** - Open the Windows Settings Group Condition dialog to configure conditions for the group. If there are no current conditions for the group, the click the **Add Condition** button.
15. **Remove Condition** - Remove the condition that applies to the Windows Settings.

Clone a Windows Settings Group

Select a Windows Settings group and click **Personalization** > **Clone Windows Settings Group**.

A copy is made of the selected group and can be edited as required.

Custom Windows Settings

Using the Custom Windows Settings Editor, you can create your own Windows Settings by selecting registry keys, values, folders and individual files to personalize or exclude from personalization. Once created, the setting can be added to Windows Settings Groups.

From the Personalization ribbon, select **Custom Windows Settings Editor**. The Custom Windows Settings dialog is displayed. Any existing custom settings are listed.

The following options are available:

- **Add** - Configure a setting which can then be added to Windows Settings Groups and personalized.
- **Edit** - Update the selected custom setting.
- **Remove** - Delete the selected setting from the list. If you attempt to remove a setting which is referenced in a Windows Setting Group, you will be asked to confirm the delete. Each group in which the setting is referenced is listed. This helps to ensure that a setting is not removed in error.
- **Clone** - The clone function makes a copy of an existing Windows setting and allows the configured registry keys and folders to be updated as required.

Certificate, Credentials and Start Menu Windows Settings cannot be cloned.

Windows Settings are configured using the following properties:

Property	Description
Name	The name that appears in the Windows Personalization list.
Description	An optional description used to tell users more about the setting and what it does.
OS	The operating system to which the setting applies. Separate tabs are created for each selected operating system so specific folders and keys can be configured for each. This allows differences between operating systems can be taken into account when the setting is applied. If you want to configure one setting, managing the same folders and keys across all operating systems, select **All**. If you change a setting from individual operating systems to All, select whether to inherit the settings applied to one of the operating systems or configure new settings. The **All** tab and individual operating system tabs cannot be displayed simultaneously. However, when you clone some Windows Settings, multiple OS tabs, including the **All** tab, may initially be shown. Before you save the setting either keep the **All** tab and remove the individual operating systems tabs or remove the **All** tab. If you do not remove any of the tabs, the OS tabs are automatically removed leaving only the **All** tab.
Folder	The folder to personalize or to exclude from personalization. Enter a folder path or select the ellipsis (**...**) and browse to the folder. Folder paths must start with a CSIDL, a system variable, or a letter. Wildcards are not supported. If an item is required for more than one operating system, highlight the required item select an operating system from the drop-down and click **Copy To**. If you do not want to personalize an item and it is included in personalization because a parent item it its folder or registry path is included, select the **Exclude** checkbox for that item.
File Name	The file to personalize or to exclude from personalization. Click the ellipsis in the

Property	Description
	File Name field to browse to a file or enter the folder path and file name manually. You can use the following wildcards in the file name: *, ?, and [ ]. When using wildcards to include or exclude items, be aware that the more specific folder or registry path takes priority. If paths are of equal length, the exclusion takes priority. For more information see, Inclusions and Exclusions.
Key	The registry key to personalize or to exclude from personalization. Click the ellipsis in the Key field to open a registry browser and select the key. Or enter the registry key path manually. You can use the following wildcards: *, ?, and [ ].
Value	Enter the registry key value to personalize or to exclude from personalization. You can use the following wildcards: *, ?, and [ ]. It is not possible to enter the backslash character \ in the registry key Value text.

Default Windows Settings Groups

The following Windows Settings Groups are available by default. Click on a group to view which Windows Settings are managed by that group.

Accessibility

- Accessibility Keyboard
- Audio and Sounds
- Tablets
- Visual Settings

Action Center

- Action Center Settings

Active Setup

- ActiveSetup

Explorer Settings

- General Folder Options
- Libraries
- Links
- Mapped Network Drives
- Mapped Network Printers

- Network Location Shortcuts
- Search Folder Options
- View Folder Options

IE10+ Cookies and History (W7, WS 2K8 R2)

- IE Passwords
- IE Zones
- IE10+ Settings

IE10+ Cookies and History (W8.x, WS 2012, WS 2012 R2)

- IE Passwords
- IE Zones
- IE10+ Settings

IE11 Cookies and History (W10, WS 2016)

- IE Passwords
- IE Zones
- IE10+ Settings

IE8-9 Cookies and History (W7, WS 2008 R2)

- IE Passwords
- IE Zones
- IE8-9 Settings

Input Devices

- Input Keyboard
- Mouse

Mail Profile and Signatures

- Mail Signatures
- MAPI Profile

Region and Language

- Input Language
- Language Bar
- Locale
- MUI

Security

- Certificates

- Credentials

Start Menu (W10, WS 2016)

- Start Menu

Taskbar (W10, WS 2016)

- Notification Area
- Taskbar
- Toolbars

Taskbar and Start Menu (W7, W8, WS 2008 R2, WS 2012, WS 2012 R2)

- Notification Area
- Start Menu
- Start Menu - Recently Launched Applications
- Taskbar
- Toolbars

Windows Appearance (W10, WS 2016)

- Icons
- Themes
- Window Color and Appearance

Windows Appearance (W7, WS 2008 R2)

- Icons
- Themes
- Window Color and Appearance

Windows Appearance (W8.x, WS 2012, WS 2012 R2)

- Icons
- Themes
- Window Color and Appearance

Windows Desktop

- Account Picture
- ClearType
- Icon Positions and Views
- Screen Saver
- Visual Effects
- Wallpaper

As a user moves between managed endpoints with different operation systems and applications, some configured shortcuts are not valid for all environments. If users are managing folders using Windows Settings Groups, Environment Manager manages the following temporarily invalid shortcuts:

Shortcut or Link	Supported Operating System
Standard shortcuts in the Windows file system that point to a target does not exist	All supported operating systems
Items pinned to the Taskbar that point to nonexistent paths	All supported operating systems
Items pinned to the Start menu that point to nonexistent paths	Windows 7, Windows Server 2008 R2

Sites

Larger organizations typically utilize multiple sites to manage the User Personalization requirements of their users. Sites can be based on areas of the organization such as different departments, geographical location or any other logical division.

An Environment Manager site is made up of the following components:

- Client Endpoints
- Personalization Server(s)
- SQL Server

Each site uses this standard three-tier architecture and can be linked via their SQL servers through replication.

Within the Environment Manager console, sites are configured in the Sites node in the User Personalization navigation tree. All personalization configurations include a Default Site which contains the Personalization Server and database on which the software was installed and configured. This is typically set up as the main site for an organization, adding additional branch sites as required. If no further sites are configured, the Default Site is used.

Once a site has been created in the console, membership rules are used to define which endpoints have their personalization managed by that site. Personalization Servers and virtual hosts can then be added to the site as required.

When a user logs on to an endpoint, they connect to the Personalization Server listed in the AEMP configuration file. Once connected, the Personalization Server gathers details of the user, the endpoint and software to determine which site and personalization group the user belongs.

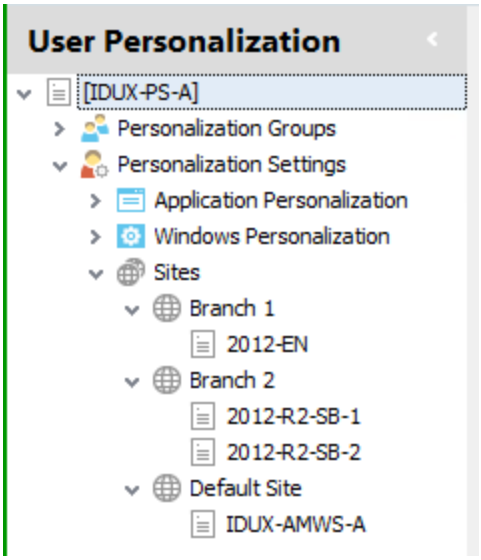
Add a Personalization Site

1. In the User Personalization tree, select **Personalization Settings** > **Sites**.
2. Select **Add Site** on the Server ribbon.

A New Site node is created and highlighted ready to be renamed in the navigation tree and the Site work area displays.

Environment Manager Sites Hierarchy

Environment Manager Sites are created in the User Personalization navigation tree. Users are assigned to the first site in the list where membership rules match. It is therefore important that sites are listed in order of priority to ensure users are assigned to the most relevant site.



An endpoint can match the membership rules of more than one site but will be assigned to the first matching site only.

To change the order, select a site and click **Move Up** and **Move Down** on the Edit ribbon.

Default Site

The Default Site is automatically included in all Environment Manager Personalization configurations. Any endpoint which does not match the membership rules for another site is assigned to the default site. Because of this, membership rules for the group cannot be defined. Servers and virtual hosts should be set up for this site which will be the default for a standard user within your organization.

Environment Manager Site Membership Rules

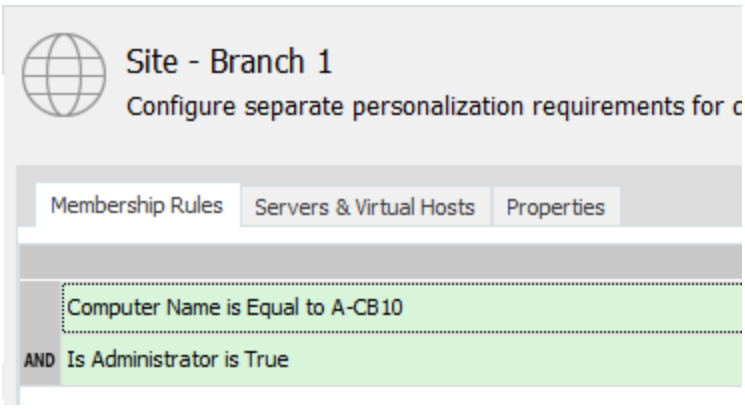
The membership rules for a site are governed by conditions which must be satisfied for an endpoint to use that site. The conditions are based on users, computer specifications and directory membership. Membership can be based on a single condition or a user may have to fulfill a number of conditions for membership of a site.

Similar to Personalization Groups, membership of a site can be based on two rule types:

- **AND** - Multiple conditions must be satisfied for membership of the site. This is called a condition group.
- **OR** - Membership is determined by satisfying the conditions for one of a number of conditions.

Example 1

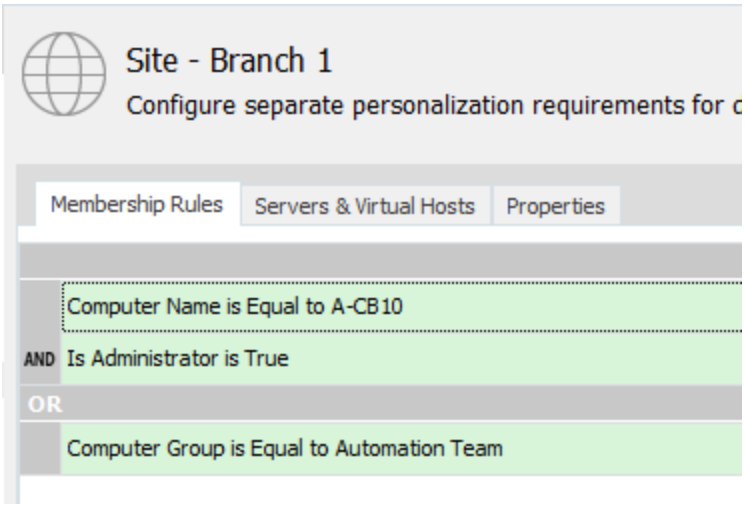
A condition group has been created containing two conditions:



Users must fulfill both conditions to be members of the site.

Example 2

A second condition group has been added:



To be a member of this site, a user must fulfill all the conditions in the first condition group or the condition in the second condition group.

Create Site Membership Rules

1. In the User Personalization tree, select **Personalization Settings** > **Sites**.
2. Select a site.
3. Click in the **Membership Rules** work area.

   The Memberships > Conditions ribbon is added and selected.

4. In the Conditions ribbon, select the required condition. User, Computer, and Directory Membership are available.

   See Environment Manager Site Conditions for details.

   The dialog box for the selected condition displays.

5. Configure the condition and click **OK**. The new condition group displays under **Membership Rules**.
6. To further define group membership for the site, add more conditions:
   - **AND** Rule - Right-click on an existing condition, select **Insert Condition** and configure the condition as required.
   - **OR** Rule - Right-click in the work area and select **Add Condition Group** and configure the condition as required.

   Condition groups can be edited and deleted by selecting **Edit Condition** or **Delete Condition** from the shortcut menu.

Environment Manager Site Conditions

Using membership rules for sites enables you configure the conditions which govern who connects to which site in your organization. For example, if you set a User condition for a site you can ensure that when a user logs on, they are connected to the same site regardless of where they are and what computer they are logging onto.

If site membership rules are not configured, all managed users are assigned to the Default Site.

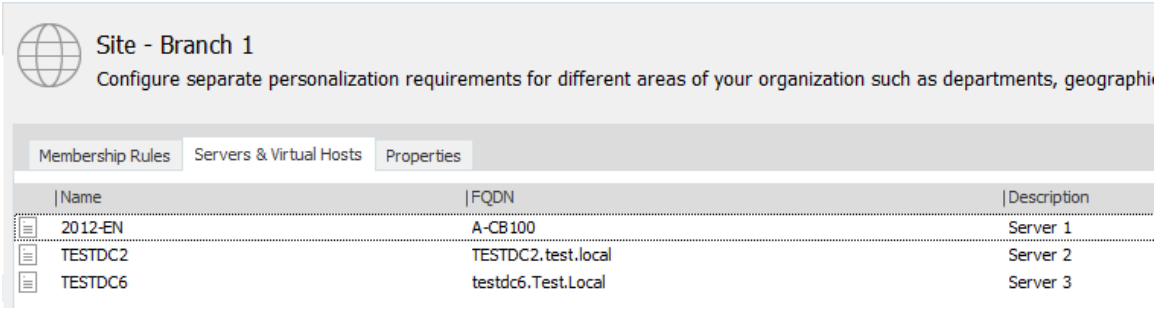
The table below list the available conditions for sites.

Type	Condition
User	User Name User Group Is Administrator
Computer	Computer Name Computer Domain Computer NETBIOS Name Computer Group Computer IP Address
Directory Membership	User OU Membership Computer OU Membership Site Membership

Servers and Virtual Hosts

Sites can be made up of multiple Personalization Servers and virtual hosts as defined by their individual requirements.

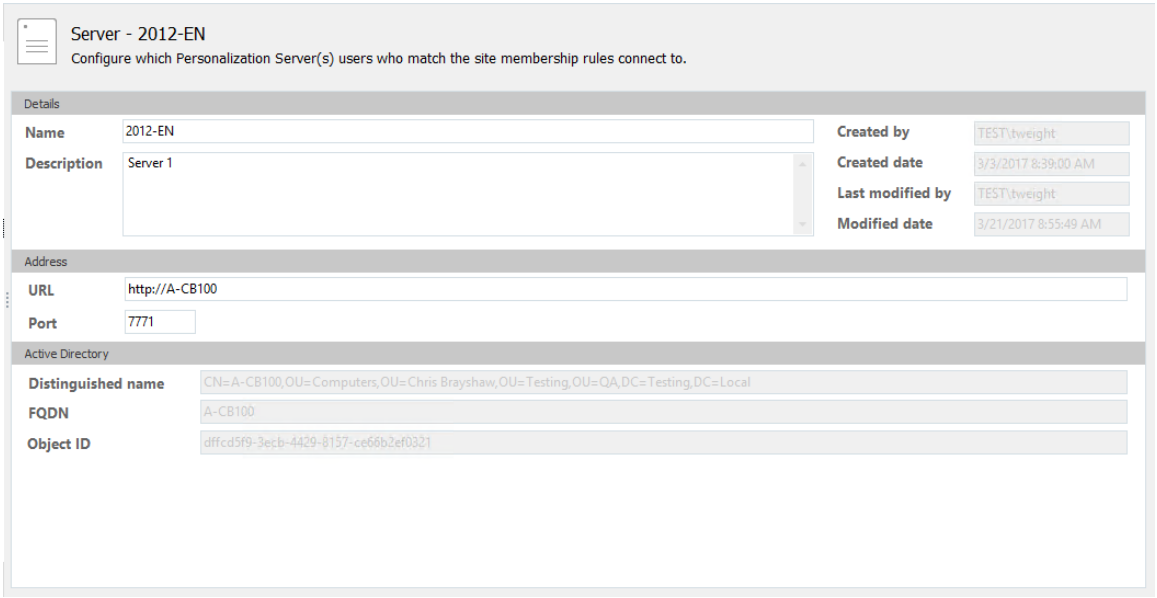
The servers and virtual hosts which have been set up for a site can be viewed by selecting the required site in the navigation tree and the **Servers & Virtual Hosts** tab.



Servers and virtual host can be deleted by selecting and clicking the appropriate button from the Edit ribbon.

Virtual Hosts should be added to a site to support network load balancing.

View and Edit Server and Virtual Host Properties



Select a server or virtual host from the navigation tree to display details in the work area. The display is the same for both virtual hosts and servers.

From the work area, the following properties can be edited for virtual hosts and servers:

- **Name** - A name what can easily identify the server or virtual host. This displays in the list of Servers & Virtual Hosts when a site is selected in the navigational tree.
- **Description** - A description for the server or virtual host.
- **URL** - The location of the server or virtual host. A valid URL must start with HTTP or HTTPS.
- **Port** - The connection method to the server or virtual host. The port range for is 7771 to 7790 and the default port is 7771.

Add Personalization Servers to a Site

1. In the User Personalization tree, select **Personalization Settings** > **Sites**.
2. Select a site.
3. Click **Add Server** from the **Personalization** ribbon. The **Select Computers** dialog box displays.

   The **Select Computers** dialog box enables criteria to be used to search for servers by name or description and in specified directories, if required. The **Advanced** search button expands the dialog enabling the search to be further defined.
4. Locate the server and click **OK**. The server is added as a new node under the site in the navigation tree.

Add Virtual Hosts to a Site

1. In the User Personalization tree, select **Personalization Settings** > **Sites**.
2. Select a site.
3. Click **Add Virtual Host** from the **Server** ribbon. The **Add Virtual Host** dialog box displays.
4. Enter the **FQDN** (Fully Qualified Domain Name) for the virtual host.
5. Click **OK**. The virtual host is added as a new node under the site in the navigation tree.

Personalization Tools

Import and Export Personalization Configurations

In the Personalization console, you can export a configuration as an XML template. Whole configurations, individual items, or groups of items from a configuration can be exported to an XML file. You can copy the full and partial configurations from one personalization database to another.

To create a new configuration or to update an existing one, you can import the exported XML configuration into a personalization database.

Caution: Importing configurations makes changes to your database which cannot be undone. It is recommended that you back up your database prior to using the Import feature.

Personalization imports and exports are performed for the following groupings, represented by nodes in the import and export dialogs:

- Application Groups
- Applications
- Windows Settings Groups
- Custom Windows Settings
- Windows Settings Conditions
- Personalization Groups
- Sites
- Global Application Exclusions
- Settings

You can further define the import and export by selecting individual items from any group.

Two cmdlets within the EMPImportExport Powershell module can also be used to import and export configuration data from personalization server databases.

Import and Export Rules

When importing or exporting personalization configurations the following rules apply:

- Any configuration item that has a dependency with another item is automatically included in the import or export and cannot be deselected. For example, when you select an Application Group, all the associated User Applications are automatically selected. The same is true of any Windows Settings Conditions that are required for the Windows Settings being imported or exported.
- The Default Site and Default Users personalization group are the last elements in their respective nodes and always maintain this position on import.

- Imported User Applications and Application Groups are placed in alphabetical order in the configuration. For example, if Application Groups A, C and E already exist in a configuration and groups B and D are imported, the order following import is A, B, C, D, E.
- Order numbers are not exported for Personalization Groups. This means that imported Personalization Groups are placed after any existing groups in the configuration but before the Default User group. For example, if groups A, C, E and Default User already exist in a configuration and groups B and D are imported, the order following import is A, C, E, B, D, Default User. The same behavior applies for Sites.
- Environment Manager XML configuration files that were not generated by the Export feature - such as some of the templates supplied by Ivanti Professional Services, or XML files that have been edited outside of Environment Manager - can be imported. However, because these files have been created or edited outside of the Environment Manager console, any errors are not validated and could impact the configuration on the database.
- The following settings can be merged on import:
    - Global registry inclusions & exclusions
    - Global file path inclusions & exclusions
    - User Applications added to an existing Application Group
    - Application Group registry inclusions and exclusions
    - Application Group file path inclusions and exclusions
    - Servers added to an existing site
- The following settings cannot be merged on import and result in an overwrite:
    - User Applications that already exist
    - Personalization groups that already exist
    - Servers added to a site which already exist in that site
    - Windows Personalization Servers
- When merging sites, the Membership Rules, Servers & Virtual Hosts, and Properties are always updated with the settings from the imported site.
- When importing Windows Settings Groups, the following apply:
    - Windows Settings Groups are always merged (or can be skipped)
    - Windows Settings Conditions are always replaced (or can be skipped)
    - Individual (customized) Windows Settings are always replaced (or can be skipped)

Export a Personalization XML Template

1. In the Personalization console of Environment Manager, connect to the database that contains the configuration you want to export.

2. From the Tools ribbon, click **Export**.

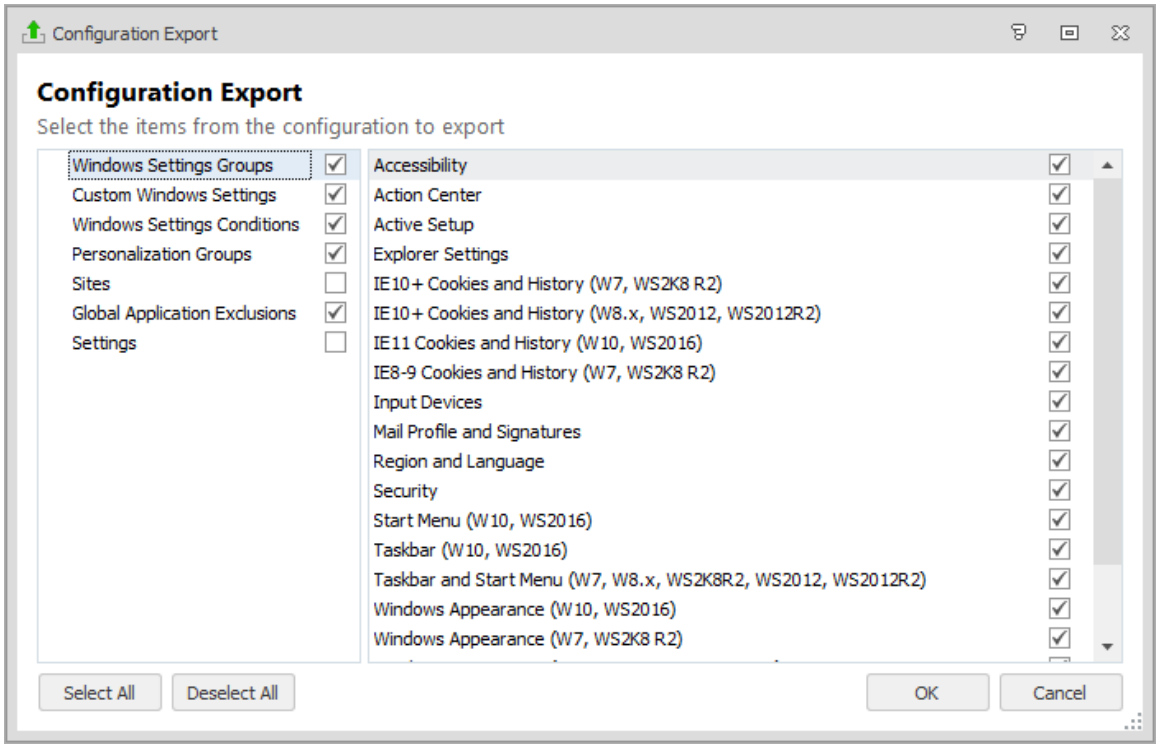
   The Export Configuration dialog displays.

   The left-hand column of the dialog displays the nodes under which the configuration elements are grouped. Highlighting a node displays all associated elements for that node in the right-hand pane. By default, all nodes and elements are selected.

   Clearing the User Applications checkbox excludes all managed applications from the export. However, if an application is a member of a selected Application Group, it cannot be deselected unless the group has first been deselected.

3. Select the checkboxes for elements of the configuration that you want to export.

   In the example below, all Application Groups, Personalization Groups, User Applications have been selected for export.



4. Click **OK** to open a Save As Windows browser dialog.
5. Navigate to where you want to save the configuration file. Enter a file name, accept the default file type setting (**Configuration Files *.xml**), and click **OK**.

An XML file containing the selected elements is created. For whole configurations or large portions thereof, this may take a few seconds. When complete a confirmation dialog displays.

Import a Personalization XML Template

Caution: Importing User Personalization configurations makes changes to your database that cannot be undone. It is recommended that you back up your database prior to using the Import feature

1. In the Personalization console of Environment Manager, connect to the database into which you want to import configuration items. This could be a new configuration or an existing one that you want to overwrite or add to.
2. From the Tools ribbon, click **Import**.

   A Windows browser dialog displays.
3. Navigate to the configuration file that you want to import.
4. Select the file and click **Open**.

   The Configuration Import dialog displays. This dialog contains the configuration elements in the file for import. Only those nodes that were exported are included.

   The left-hand column of the dialog box displays the categories under which the configuration elements are grouped. Highlighting a category displays all associated elements for that node in the right-hand pane. By default, all nodes and elements are selected.
5. Use the checkboxes or buttons to select the elements that you want to import into the configuration and click **OK**.

   Deselecting the User Applications checkbox excludes all managed applications from the import. However, if an application is a member of a selected Application Group, it cannot be deselected unless the group has first been deselected.
6. When an existing item is encountered that has the same name as that in the file being imported, a conflict occurs. Conflicts are displayed in the Resolve Conflicts dialog, which enables you to select an action to resolve each conflict.

   If there are no conflicts, go to step **8**.

7. From the Resolve Conflicts dialog select the action required for each element:
    - **Replace** - The element in the current configuration is deleted and the one from the new configuration added.
    - **Skip** - The new element is not imported and the existing one remains unchanged.
    - **Merge** - Combines the contents of the two elements to include the contents of both. For example, when importing an application group that already exists in the database but contains different applications, those applications are added to the existing configuration to expand that application to include all the applications from both application groups.

    If you are importing default (out-of-the-box) Windows Settings Groups, you can only **Merge** or **Skip** a group. If you are importing customized Windows Settings Groups, you can only **Replace** or **Skip**. Conditions always import in **Replace** mode, or you can **Skip** them.

    Multiple conflicts can also be resolved at category level by selecting **Replace All**, **Skip All** or **Merge All**, where available.
8. Click **OK**.
9. A warning states that you are making irreversible changes. Click **OK** to proceed.

All selected elements are added to the personalization configuration on the connected database. All elements are subject to normal behavior and can be edited as required.

Global Options

Access Rights

Control the authorized users for administration of the Personalization Server and define who can access and change Environment Manager console settings.

The user that configures the Personalization Server Configuration Portal is automatically added to the database as a Master Administrator. Initially this is the only user that can connect to the database through the console. This user can then add users to the database.

Any user can be added and deleted but at least one Master Administrator must always be defined. Users who are not defined here cannot connect their console to the Personalization Server. This only applies to the console and not managed users logging onto endpoints.

- User Roles
- Permissions
- Configure Console Access Rights

User Roles

Administrator

The Administrator role provides access to the functionality in the Environment Manager Console. Administrators also have access to the Advanced Mode of the Endpoint Self-Service Tool when the tool is enabled for a Personalization Group. Administrators cannot manage or assign other user roles.

Master Administrator

The Master Administrator role allows the user to manage roles assignment and provides full access to the Environment Manager Console and Browser Interface functionality. Master Administrators also have access to the Advanced Mode of the Endpoint Self-Service Tool when the tool is enabled for a Personalization Group. At least one Master Administrator must always be defined.

Support Console

The Support Console provides read-only access to Environment Manager Personalization configurations and allows users to view Personalization Analysis reports. Support Console users can also use the associated analysis functionality, such as rolling back application settings. Using this role, support teams can safely carry out routine maintenance for end users in a restricted environment, without full access to modify the configuration.

When a user with a Support Console role connects, functionality to modify the personalization configuration is automatically disabled and the console changes to a blue color scheme.

Application Team

The Application Team console offers limited access to Environment Manager Personalization configurations and allows users to add, modify and delete applications and Application Groups and view Personalization Analysis reports. Application Team users can also use Personalization Analysis functionality, such as rolling back application settings and converting discovered applications.

When a user with the Application Team role connects, functionality to modify some of the personalization configuration is automatically disabled and the console changes to a blue color scheme.

Permissions

Environment Manager Console

Action	Admin	Master Admin	Support Console	Application Team
Create New Personalization Groups	✓	✓	–	–
Configure Personalization Group Settings	✓	✓	–	–
Configure Personalization Group Membership Rules	✓	✓	–	–
Configure Personalization Group Applications	✓	✓	–	✓
Configure Personalization Group Windows Personalization	✓	✓	–	–
Configure Application and Application Groups	✓	✓	–	✓
Configure Windows Personalization	✓	✓	–	–
Configure Sites	✓	✓	–	–
Configure User Roles	–	✓	–	–
Configure Advanced Settings	✓	✓	–	–
Access Personalization Analysis	✓	✓	✓	✓
Read Access to Console	–	–	✓	✓

Endpoint Self-Service Tool

Action	Admin	Master Admin	Support Console	Application Team
Run in Basic Mode	➖	➖	✔	✔
Run in Advanced Mode	✔	✔	➖	➖

Configure Console Access Rights

1. Select the **User Personalization** navigation button.
2. Click **Access Rights** from the Manage ribbon.
3. The Access Rights dialog displays.
4. Click **Add**. The Select User or Group dialog box displays which searches the Active Directory for users and groups which match entered criteria. The **Advanced** search button expands the dialog enabling the search to be further defined.
5. Select the required user or group and click **OK**. The user or group will be assigned the User role by default.
6. Click the **Role** column for the user or group to change the role to one of the following:
    - Master Administrator
    - Administrator
    - Support Console
    - Application Team
7. The list can be updated as follows:
    - Click **Remove** to remove a user or group from the list
    - Click the ellipsis in the name column of any group or user to change the group or user
    - Click the role column for a user or group to change the role
8. When all users and groups are configured as required, click **Close**.

Advanced Personalization Settings

Advanced Settings enable an administrator to make changes to specific database and communications settings. Changes made to any setting within here will affect the operation of user personalization for all managed endpoints. Advanced Settings should only be added as advised by Support.

With this option, new settings can be created whilst existing ones can be removed, edited or restored to their original install value.

Manage Advanced Settings

1. Select the **User Personalization** navigation button.
2. From the Manage ribbon, click **Advanced Settings**.

   The Advanced Settings dialog displays. Any settings displayed in bold are those which have been edited or added to the default settings.
3. Change the Advanced Settings list as required:
   - Change value - Click in the value for the required setting enter a new one.
   - Add an Advanced Setting - Click **Add**, enter the Name, Value and optional Description for a new Advanced Setting and click Close.
   - Remove an Advanced Setting - Highlight an Advanced Setting and click **Remove**.
   - Restore the Advanced Settings list - Click **Restore** to reset the list to its initial install state; all values are reset and any created entries are removed.

Caution: If VirtualizationFiles or VirtualizationRegistry are set to false, personalization will not function correctly.
Adjusting the setting for offline_restorerate and offline_samples can impact on personalization performance.
Do not change these values unless advised by our Support team.

Advanced Settings List

Environment Manager contains the following global settings:

Group	Default Value	Description
ArchiveLocalProfilesOnly	true	Set whether to archive all or local profiles.
AutomaticeArchiveEndTime	07:00	The time (hh:mm) at which automatic archiving and purging finishes. The timezone settings from the personalization database will be utilized.
AutomaticArchiveIntervalDays	1	The number of days between automatic archives
AutomaticArchiveStartTime	01:00	The time (hh:mm) at which automatic archiving and purging takes place. The timezone settings from the personalization database will be utilized.

Group	Default Value	Description
		If the time is not in the correct format, archiving will not work and an error message will appear in the Windows Application log on the Personalization Server. If there are multiple Personalization Servers error messages will appear on all servers. The time zone of this time is the time zone of the SQL Server machine - not the Personalization Server machines. This is to match the 8.0 behavior (when archiving was done by SQL Server Agent).
commsloggingenabled	false	Enables or disables communications logging on the managed endpoints. True or false. When set to true, all clients produce logs of communications with the personalization server. These logs show all personalization activity to give confidence that personalization is working correctly. The logs are by default written to the user's local application data folder, for example, C:\Users\username\AppData\Local\AppSense\Environment Manager\CommsLogs, but if diagnostic logging is enabled the logs are written instead to logdirectory\user'ssid\CommsLogs. Comms logging may be enabled for an individual endpoint by defining the registry DWORD value **HKEY_LOCAL_MACHINE\Software\Appsense\Environment Manager\CommsLoggingEnabled** on the endpoint and setting it to 1. To enable for a single user define **HKEY_CURRENT_USER\Software\Appsense\Environment Manager\CommsLoggingEnabled** instead. When diagnostic logging is enabled on an endpoint, all the information that appears in the comms logs will also appear in the diagnostic logs too - the comms logs merely provide a short summary of personalization activity.

Group	Default Value	Description
configpoll	86400	The interval (in seconds) in which the managed endpoints poll the personalization server for configuration changes Setting this value to 60 seconds or less leads to a large increase in memory from the WinHTTP code.
daysofcommslogtokeep	3	When communications logging is enabled (using the *commsloggingenabled* option), this setting specifies the number of days logs to retain.
debug	false	Enables logging of synchronizer activity for each application on all endpoints. These logs are written to the profile cache for each application in the logs subdirectory directory. For example, C:\appsensevirtual\S-1-5-21-3975584332-491336430-3592548699-1104\{58A6B7A8-C2F6-43E1-88AC-07531B5D53A8}\notepad\logs.
desktopinclusions	jpg;jpeg;bmp;ico;cur;ani	File types to be included for personalization of desktop settings for a user.
DNS_Resolve_Timeout	5	The timeout (in seconds) for the managed endpoint to resolve the personalization server name when attempting synchronization of data.
HTTP_Connect_Timeout	5	The managed endpoint to personalization server reconnect timeout (in seconds). This setting is only valid once the managed endpoint has received and loaded the personalization configuration for the first time.
HTTP_Receive_Timeout	30	The managed endpoint to personalization server receive timeout (in seconds). This setting is only valid once the managed endpoint has received and loaded the personalization configuration for the first time.
HTTP_Send_Timeout	30	The managed endpoint to personalization server send timeout (in seconds). This setting is only valid once the managed endpoint has received and loaded the personalization configuration for the first time.

Group	Default Value	Description
InactiveProfileExpiryDays	180	The expiry time (in days) for inactive profiles, after which time they are deleted. Set to 0 to disable this option.
InactiveUserExpiryADCheck	true	If set to true, users are only deleted if they no longer exist in active directory. This setting is only applicable if the InactiveUserExpiryDays is non-zero.
InactiveUserExpiryDays	180	The expiry time for inactive users. If a user does not log in within the specified time, their profile is deleted. Set to 0 to disable this option.
jpgquality	80	The amount of compression to apply (as a percentage) used when converting a desktop wallpaper from BMP to JPG for personalization database storage. 100 = best quality, no compression. 0 = worst quality, maximum compression.
LegacyDeleteDelayDays	30	The number of days after which legacy data, if present, is deleted. To disable this setting, apply a 0 value.
LegacyFbrDeleteDelayDays	30	The number of days after which legacy FBR files are deleted from a profile where a hive file has been created by a later client. To disable this setting, apply a 0 value. This setting is only applied if the UpgradeFbrHive property is enabled following an upgrade.
linkfailretrypolltimescales	90	The configuration poll period (in seconds) used by the managed endpoint when communication with the personalization server is lost.
ManagePersistentDat	false	Enable management of the persistent.dat file on the client. If set to false, persistent.dat is not saved to the database.
maxlinkfailbackoffsecs	1800	Used with minlinkfailbackoffsecs to create a random offline config polling time for clients. This ensures that when clients go offline, they do not poll the server simultaneously, which could

Group	Default Value	Description
		result in spike in the server load.
minlinkfailbackoffsecs	300	Used with maxlinkfailbackoffsecs to create a random offline config polling time for clients. This ensures that when clients go offline, they do not poll the server simultaneously, which could result in spike in the server load.
MonthsOfUsageDataToKeep	6	The number (in months) of usage data to keep for user applications. Usage data older than this value are deleted by the daily archiving job.
Network_Path_Support	False	Enables or disables the personalization of application settings stored on network paths and mapped drives. These must also have been configured as inclusions within personalization. When set to **False** network drives are not personalized and application settings are not written to the virtual cache. Change the setting to **True** to personalize any application settings written to included network folders.
NumberOfArchivesToKeep	5	Used by the daily archive job, this defines the number of daily archives to retain.
offline_restorerate	100	The communication rate (in kb/second) above which the managed endpoint considers communication with the personalization server to be restored and hence online. This value must be higher than the offline_failrate value. Adjusting the Global Settings can impact on Personalization performance. This value is provided for support purposes and should not be modified by the end user.
offline_samples	4	The number of samples, in a moving average, used by the managed endpoint to measure the link transfer rate and detect an offline condition.

Group	Default Value	Description
		Adjusting the Global Settings can impact on Personalization performance. This value is provided for support purposes and should not be modified by the end user.
PingWebServerTimeOfDayLocal	01:05	Local time that background services ping corresponding servers. It should be set to a time after the personalization server's daily recycle time.
ProfileCleanupDelayDays	30	The delay before endpoints clean extraneous data from profiles after a change to inclusions or exclusions. Set to 0 for no delay or -1 to disable the cleanup function.
pvcdebug	0	The Personalization Virtualization Component (PVC) debug level for all managed endpoints. 0 is disabled. 10 is verbose. Setting this value will enable PVC debugging on all endpoints and will have a detrimental effect on performance as well as heavy use of disk space. It is recommended instead to enable debugging on a per-endpoint basis using registry settings.
ReplicationType	none	Used in replicated SQL environments to identify master / slave / none for archiving purposes. This value is set by the archiving script and is not recommended to be changed by the user.
syncpoll	900	The interval (in seconds) between managed endpoint retries of failed synchronizations when offline resiliency is enabled.
transport	http	Transport Type. Only required for backwards compatibility with older versions of the Environment Manager Agent. This value is provided for support purposes and should not be modified by the end user.

Group	Default Value	Description
UpgradeFbrToHive	true	When true, endpoints upgrade '.fbr' registry files to '.hive' registry files. Once set to 'true', this setting cannot be set back to 'false'. For information about using this setting with the Profile Migration PowerShell Interface, see UpgradeFBRtohive Advanced Setting.
version	3.0	The file exchange protocol to be used during client-server communication. This value is no longer used and will be removed in future versions of Environment Manager.
virtualzationfiles	true	Enable or disable User Personalization of files for all managed endpoints. True or false. This value is provided for support purposes and should not be modified by the end user.
virtualizationregistry	true	Enable or disable User Personalization of registry settings for all managed endpoints. True or false. This value is provided for support purposes and should not be modified by the end user.

Application Exclusions

Applications in the Application Exclusions list are not managed if they are started as child process of a managed application. However, exclusions can be overridden by adding an excluded application to the managed applications list for a personalization group.

Child processes of a managed application are personalized by default. Some child processes may not be suitable for personalization. It could be that a child process continues to run when the managed parent application is closed; preventing the parent application from synchronizing with the database. By adding the child process to the Application Exclusions, the parent application will synchronize correctly when closed.

The Applications Exclusions list is pre-populated with applications recommended for exclusion from personalization. The list includes common applications which are not necessarily suitable for personalization, such as registry editing tools and system administration utilities.

The Application Exclusion list can be updated by adding new applications and removing existing ones. From the Manage ribbon, select **Application Exclusions** to display the currently excluded applications. Amend the list of applications using the **Add** and **Remove** buttons.

Data Collection Settings

Global settings for Application Data Collection are available to specify registry and folder inclusions and exclusions and to clear all collected data.

Application Data Collection Inclusions and Exclusions

Registry and folder inclusions and exclusions determine which registry keys and folders are passively monitored by Application Data Collection.

Add Registry Inclusion or Exclusion for Application Data Collection

1. Select the **User Personalization** navigation button.
2. From the Manage ribbon, click **Data Collection Settings**.

   The Application Data Collection Settings dialog displays.
3. Select the **Registry** tab.
4. Right-click in either the **Include** or **Exclude** area and select **Add Registry Key**.

   The Add Registry Key dialog displays.
5. In the Key field, select the ellipsis (...) to browse for the registry key or manually enter the path and key name.

   Wildcards can be used anywhere in a registry path to represent one or more characters. For example, adding *.0 to the path for Microsoft Outlook means all versions of Outlook can be included or excluded with one entry: HKCU\Software\Microsoft\Office*.0\Outlook

   The Browse Registry dialog displays. You can select from your local computer, current user or click **Connect** to display the Active Directory Select Computer dialog to select another computer to browse.
6. Locate the required Registry Key and click **OK**.

   The selected registry key is entered in the Add Registry Key dialog.
7. Click **OK**.

   The selected Registry Key is added to the Include or Exclude list in the work area.
8. Click **Close**.

Add Folder Inclusion or Exclusion for Application Data Collection

1. Select the **User Personalization** navigation button.
2. From the Manage ribbon, click **Data Collection Settings**.

   The Application Data Collection Settings dialog displays.

3. Select the **Folder** tab.
4. Right-click in either the **Include** or **Exclude** area and select **Add Folder**.

   The Select Folder dialog displays.
5. In the Path field, select the ellipsis (...) to browse for the folder. The path can also be entered manually.

   The Browse for Folder dialog displays. You can select an existing folder from your local computer or click the **Make New Folder** button to create a new folder for inclusion or exclusion.
6. Locate the required folder and click **OK**.

   The selected folder path is entered in the Select Folder dialog.
7. Click **OK**.

   The folder path is added to the Include or Exclude list in the work area.
8. Click **Close**.

Remove Collected Data from Application Data Collection

Remove all data collected for Personalization Groups which have, or have had, Application Data Collection enabled. This removes all registry and folder data for collected applications.

Caution: Clearing collected data is permanent. Data cannot be recovered.

1. Select the **User Personalization** navigation button.
2. From the Manage ribbon, click **Data Collection Settings**.

   The Application Data Collection Settings dialog displays.
3. Click **Clear all Data Collection**.

   A confirmatory prompt is displayed.
4. Click **Yes**.

The collected data is cleared.

GeoSync

GeoSync provides a method of synchronizing user data and Environment Manager Personalization configurations between personalization server SQL server databases. This lets users access their data and settings at multiple locations, providing them with a consistent experience wherever they log on. Any changes they make are synchronized back to the published on the next sync.

GeoSync requires two or more personalization server databases - one to act as the publisher and the others as subscribers. Publishers and subscribers are associated using PowerShell Cmdlets provided when Environment Manager is installed. Subscribers are then assigned to personalization groups in the Environment Manager console, to determine which databases are synchronized.

Any changes that are made to the Users Data are synchronized between Publisher and Subscriber(s) to ensure that the latest changes are available. Whereas the User Data publication is a 'two-way' sync, Configuration is a One-Way sync from the Publisher to Subscriber(s). This is to enable a centralized configuration management, Administrators make any configuration updates on the Publisher Database which is then replicated out to Subscribers at next scheduled sync.

For example, an organization has offices in different locations throughout the world, each with their own personalization database. Staff who frequently move between offices are managed by a personalization group with GeoSync configured to synchronize daily. Their data is kept up to date and is available to them wherever they log in.

Configuration-only syncs can be performed. This is useful for organizations that maintain one configuration over multiple databases. You can choose to only synchronize configurations. An organization may use configuration-only syncs if they use one configuration over multiple databases. Each change to the configuration can be quickly synced to all the required subscribers without affecting user data.

Synchronized configuration items from the publisher are highlighted in purple when viewed in an Environment Manager console connected to a subscriber. The synchronized items cannot be edited in the subscriber.

For High Availability or Disaster Recovery of Personalization Server Databases, we recommend that you view our current Best Practice guide: https://community.ivanti.com/docs/DOC-46245

Depending on the customer environment different setup steps may be required. Below are the three scenarios supported by GeoSync:

New Subscriber Databases

For new subscriber databases, follow the steps in the sections below. If you are looking at setting up local-only Personalization Groups on your new subscriber (a Personalization Group on the subscriber which will not be managed by GeoSync on the publisher), they must be created after GeoSync has been successfully configured and the subscriber synchronized with the publisher.

Existing Subscriber Databases

If you intend to set up GeoSync on a subscriber that already contains a personalization configuration and data, the configuration and data must already exist on the publisher - either the subscriber is a backup of the publisher, or a database previously synchronized via SQL Server merge replication.

The following additional steps are required for the above scenario.

Caution Setting up GeoSync on an existing subscriber that contains a configuration or data that is not on the publisher will result in data loss and is not supported in this release. If you wish to use local-only Personalization Groups on your remote subscriber(s) these should only be set up after GeoSync has been configured.

1. Associate the publisher and subscribers as described in Associate Publishers and Subscribers.
2. In the personalization console on the publisher, configure GeoSync for your Personalization Group(s).
3. Run an initial synchronization from the console.

   If duplicate Windows Settings Groups (WSGs) are identified on the subscriber, continue to step 5.

   If no duplicates are identified, configuration is complete - the listed WSGs will prevent GeoSync synchronizing.
4. Make a note of the current **ProfileCleanUpDelayDays** advanced setting and change to **-1** on the subscriber. This ensures that, should the Background Service run its daily job, it will not attempt to clean up orphaned WSGs during the GeoSync setup
5. On the subscriber remove the identified WSGs - do not remove any application groups from the subscriber.
6. Re-run step 3.

   Once initial sync has successfully completed, the subscriber should now has the WSGs identified as duplicates restored and associated with the synced personalization group
7. Restore **ProfileCleanUpDelayDays** setting back to its original value.

Satellite Database as a GeoSync Subscriber

This procedure addresses a situation where a personalization server database has been created by exporting some or all of the configuration from a larger, master database (using import/export functionality) and is used remotely for a smaller number of users. The customer wants to use GeoSync to automatically synchronize a subset of users between the master and satellite by making them GeoSync publisher and subscriber respectively. This wasn't possible using the existing merge replication scripts as they sync all of the database.

For full details about this scenario, see Satellite Database as a GeoSync Subscriber.

Associate Publishers and Subscribers

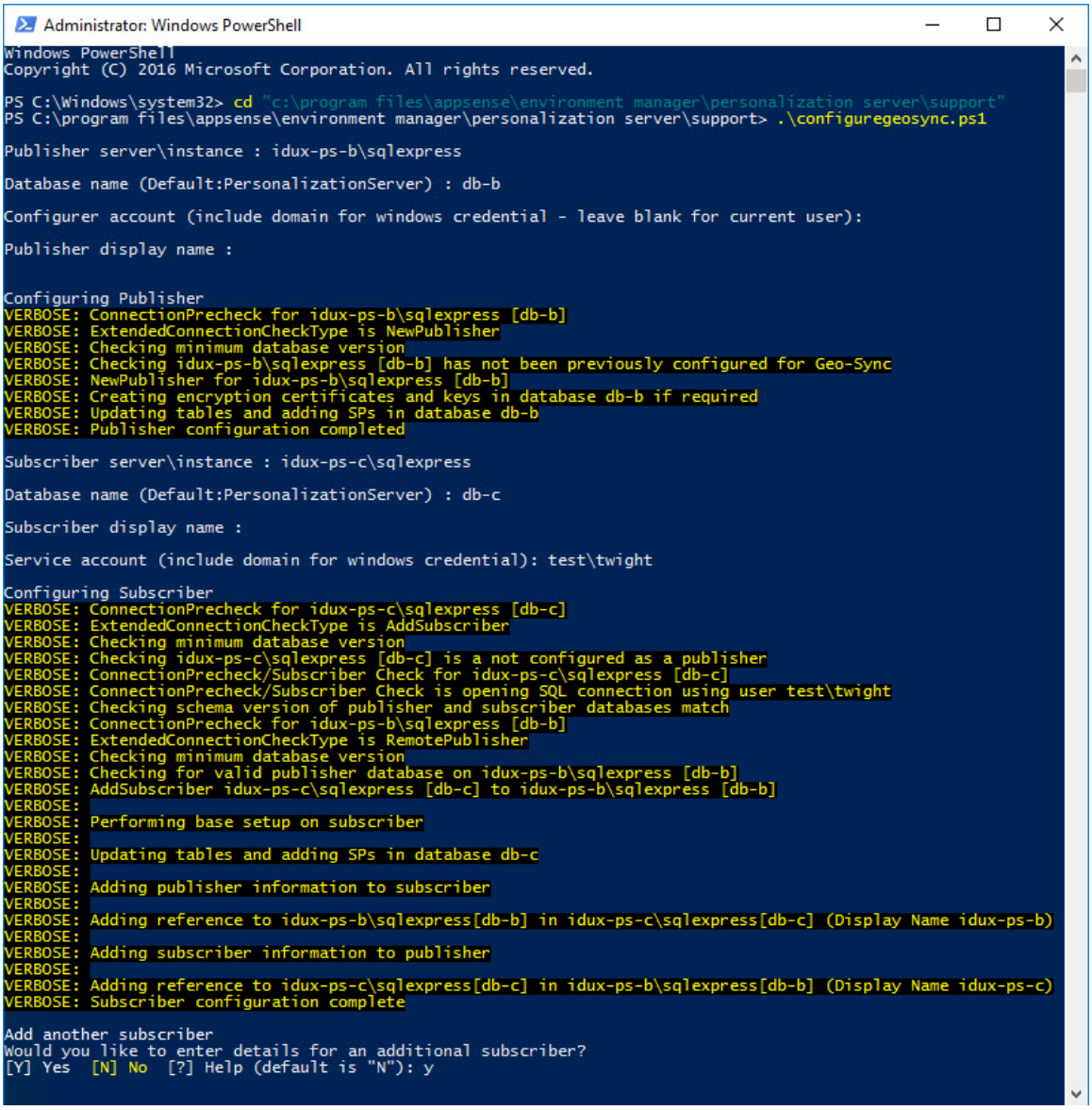
Set up GeoSync for your publisher and associate your subscribers using the ConfigureGeoSync.ps1 script. Set up can also be performed using the cmdlets supplied during Environment Manager installation. Some actions, such as adding new subscribers to existing publishers, can only be done using the cmdlets.

For further information about using the GeoSync cmdlets and how to use them in generated scripts, see GeoSync cmdlets.

If you are using SQL Express, TCP/IP protocol must be enabled in the SQL Server Configuration Manager prior to performing the following process. This applies to both publishers and subscribers.

1. Run Windows PowerShell as Administrator.
2. Enter `cd "C:\Program Files\AppSense\Environment Manager\Personalization Server\Support"` to set the location of the scripts.
3. Enter `.\ConfigureGeoSync.ps1`
4. Enter the following details when prompted:
   - Publisher server\instance
   - Publisher database name
   - Configurer account - if using Windows credentials, include the domain name and leave blank to use the currently logged in user
   - Publisher display name - this is optional, leave blank to use the SQL server name
   - Subscriber server\instance
   - Subscriber database name
   - Subscriber display name - this is optional, leave blank to use the SQL server name
   - Service account - if using Windows credentials, include the domain name and leave blank to use the currently logged in user

   If successful, confirmation that configuration is complete displays. Further subscribers can be configured if required.
5. Enter `Y` to add another subscriber or `N` to finish.



Configure GeoSync for a Personalization Group

Select subscribers for personalization groups, add conditions and configure sync types.

1. Select a Personalization group.

   If GeoSync has been successfully configured, you should see the GeoSync tab - you might need to refresh your Environment Manager configuration.

2. Select the **GeoSync** tab.

3. Click **Add** and select the required subscribers from the Display Name drop-down.

   All configured subscribers can be selected.

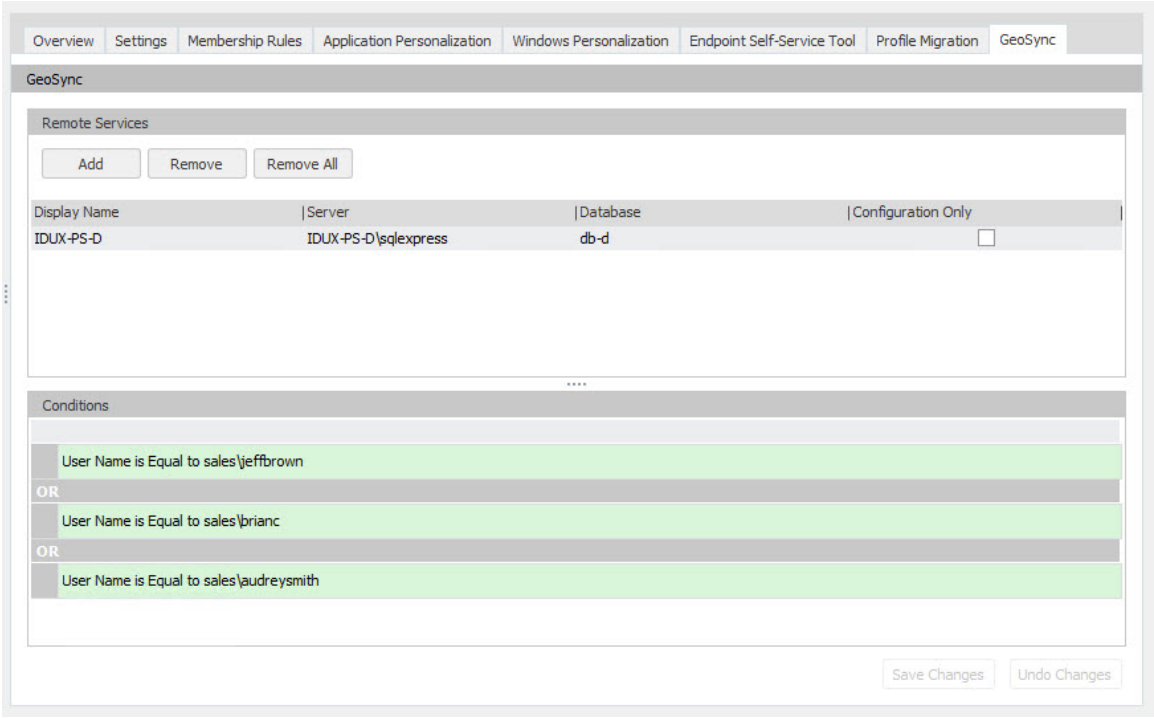
4. Select the **Configuration Only** checkbox as required.

5. Optionally add user conditions to the personalization group.

   This allows the sync to be further targeted, beyond personalization group membership rules.

6. Click **Save Changes**.

   GeoSync is now set up for the personalization group.



Manage Syncs and Schedules

Configure, edit, and cancel sync schedules for subscribers or manually start a sync.

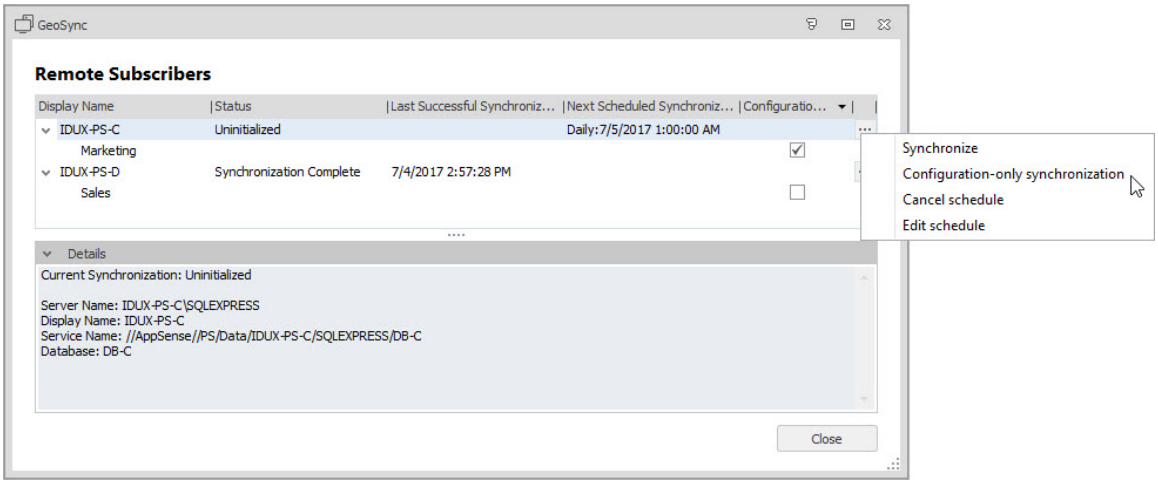
1. In the Environment Manager console, connect to the personalization server for your publisher.

2. Select **Manage** > **GeoSync**.

   The GeoSync dialog displays the available subscribers. Any personalization groups that have already been set up for GeoSync are listed beneath the subscriber. The dialog also shows the sync status, details of the last and next scheduled syncs, and the sync type for each subscriber.

3. Click the ellipsis for a subscriber and select the required option:
   - **Synchronize** - Initiate an immediate sync of data and configuration for the selected subscriber.
   - **Configuration-only synchronization** - Initiate an immediate configuration-only sync.
   - **Schedule synchronization** - Set the start time and whether the sync is run once or every 24 hours at the selected time.

   Where a schedule exists for a subscriber, edit and cancel options are available.



Backup and Restore GeoSync Databases

The backup and restore of a GeoSync enabled Personalization Server database requires additional steps to that of a Personalization Server without GeoSync enabled. The Database Master Key, used for encrypting data in the database, requires backing up and depending on the conditions may be required when restoring the database. If a GeoSync enabled database is restored to a different SQL Server instance then a full reset and configuration is required. This is due to the database using specific server, instance, and database names in the synchronization settings.

It is recommended that the publisher and all subscriber databases are backed up and restored together.

Backup GeoSync Databases

1. Backup each of the subscriber databases.
2. Backup the publisher database.

3. Once the database backup is complete, backup the publisher's Database Master Key to a file using the following method:
    a. Using SQL Management Studio connect to the SQL Server instance containing the publisher database.
    b. Create a new query targeting the publisher database.
    c. Choose a secure password to encrypt the backup file. This password is required to restore the Database Master Key and is subject to complexity checks.
    d. Run the `BACKUP MASTER KEY` SQL command, for example:

```
BACKUP MASTER KEY TO FILE = 'c:\backup\DatabaseMasterKey_
PersonalizationServer.bak'
ENCRYPTION BY PASSWORD = 'ruygn@KiHHas14m;%qG';
```

> When setting up SQL Always On Group for a Publisher Database, you must ensure that all replicas within the group contain the same Master key. This can be achieved by following the same Backup/Restore procedure detailed within this section.

4. Copy the database backups and Database Master Key backup file to a secure backup location.

Restore GeoSync Databases

Additional steps are required if the Personalization Server databases are to be restored to different SQL Server instances, or if the database has been renamed during the restore. Both processes are outlined below.

Restore to the same SQL Server Instances

Use this process if all the publisher and subscriber databases are being restored to the same SQL Server instances from which their backup where taken.

1. Obtain the database backups and the Database Master Key backup file.
2. Restore each of the subscriber databases from their backups.
3. Restore the publisher database from its backup.

4. Once restored, on the publisher SQL Server instance, enable the Service Broker using the following method:
    a. Using SQL Management Studio, connect to the SQL Server instance containing the publisher database.
    b. Create a new query targeting the publisher database.
    c. Enable the Server broker using the command appropriate to your circumstances:
        - This command requires exclusive access to the database - any other connections to the restored database have a shared lock on it, even when idle, thus blocking the ALTER DATABASE from completing. Close all connections to the database for the operation to complete: `ALTER DATABASE [PersonalizationServerDatabaseName] SET ENABLE_BROKER`
        - If there are active connections to the database, the following command will roll-back any current transactions and close all existing sessions: `ALTER DATABASE [PersonalizationServerDatabaseName] SET ENABLE_BROKER WITH ROLLBACK IMMEDIATE`
        - The following command creates a new Server Broker GUID. This command clears any messages waiting in the queue: `ALTER DATABASE [PersonalizationServerDatabaseName] SET NEW_BROKER WITH ROLLBACK IMMEDIATE`
5. Restore the Database Master Key from its backup file using the following method:
    a. Using SQL Management Studio, connect to the SQL Server instance containing the publisher database.
    b. Create a new query targeting the publisher database.
    c. Run the following RESTORE MASTER KEY SQL command targeting the publisher database. The decryption password is the one used in the BACKUP MASTER KEY SQL command, for example:

```
RESTORE MASTER KEY

FROM FILE = 'c:\backup\DatabaseMasterKey_
PersonalizationServer.bak'

DECRYPTION BY PASSWORD = 'ruygn@KiHHas14m;%qG'

ENCRYPTION BY PASSWORD = 'Gq%;m41saHHiK@ngyur'

FORCE;
```

    The encryption password is used by SQL Server to re-encrypt the Database Master Key. There is no requirement to remember this encryption password.

Step 5. is not always required if the Service Master Key has not changed since the last backup. In such cases running this command will not return an error. Instead, SQL Server will report: *The old and new master keys are identical. No data re-encryption is required*.

Restore to a different SQL Server Instance

Use this process if any of the publisher or subscriber databases are being restored to a different SQL Server instance or the name of a database has changed.

1. Follow all the steps in Restoring to the same SQL Server Instances.
2. For the publisher and each of the subscriber databases, call the PowerShell cmdlet Reset-EMPSGeoSyncDatabase to remove the old GeoSync settings from each database. See GeoSync cmdlets for details on how to run this command.
3. Set up GeoSync by following the steps in the Associate Publishers and Subscribers.
4. Configure the required subscribers for each personalization group by following the steps in Configure GeoSync for a Personalization Group.
5. Configure GeoSync schedule settings by following the steps in Manage Syncs and Schedules.

GeoSync cmdlets

GeoSync setup is performed by cmdlets shipped with the personalization server. The cmdlets are automatically imported into a PowerShell session when the *Import-ApsInstance* module is executed.

If the default Environment Manager install location is used, the cmdlets are here: C:\Program Files\AppSense\Environment Manager\Personalization Server\Support

Cmdlet	Description	Parameters
New-EMPSPublisher	Sets up the specified database as a publisher for GeoSync. This cmdlet operates in two modes - Live and Export. In Export mode, it exports a script which can be applied to a database to perform the operation. The script can be tailored for advanced requirements.	**Common parameters:** -PublisherServer -PublisherDatabase -DisplayName -Verbose -ConfigurerCredential **Live parameters:** -ConfigurerCredential **Export parameters:** -ExportScript -ScriptFolder *folder* -Force
Remove-EMPSPublisher	Removes publisher functionality from a specified database.	**Common parameters:** -PublisherServer

Cmdlet	Description	Parameters
	This cmdlet removes the publisher setup from a database, providing all subscribers have already been removed. If subscribers cannot be removed in the normal way, use the Reset-EMPSGeoSyncDatabase cmdlet. This cmdlet operates in live mode or export mode.	-PublisherDatabase -Verbose -ConfigurerCredential PSCredential **Live parameters:** -ConfigurerCredential PSCredential **Export parameters:** -ExportScript -ScriptFolder *folder* -Force
Add-EMPSSubscriber	Adds a subscriber database to a publisher. In live mode both the publisher and subscriber must be accessible. In export mode three scripts are produced: • The subscriber base setup script, "Subscriber-subscriberid.sql" performs the basic setup on the subscriber. It requires a certificate folder specified for the subscriber certificate(s) created to be saved. • The add publisher reference script, "AddPublisherTo-subscrberid.sql" adds a reference to the publisher on the subscriber. It requires the publisher certificates(s) to be copied to a specified certificate folder on the subscriber.	**Common parameters:** -PublisherServer -PublisherDatabase -SubscriberServer -SubscriberDatabase -ServiceCredential *PSCredential* -DisplayName -Verbose **Live parameters:** -ConfigurerCredential *PSCredential* The configurer credentials must be the same for both the subscriber and publisher databases.

Cmdlet	Description	Parameters
	• The add subscriber reference script, "Add-subscriberIdToPublisher.sql", adds a reference to the subscriber on the publisher. It requires the subscriber certificates(s) to be copied to a specified certificate folder on the publisher.	**Export parameters:** -ExportScript -ScriptFolder folder -Force -PublisherDisplayName
Remove-EMPSSubscriber	Removes subscriber from publisher and cleans up subscriber. In live mode both the publisher and subscriber need to be accessible. In export mode two scripts are produced: • RemoveSubscriber-subscriberid.sql • Remove-subscriberid.sql.	**Common parameters:** -PublisherServer -PublisherDatabase -SubscriberServer -SubscriberDatabase -RemoveUsers -Verbose (optional) **Live parameters:** -ConfigurerCredential *PSCredential* The configurer credentials must be the same for both subscriber and publisher databases. **Export parameters:** -ExportScript -ScriptFolder *folder* -Force
Get-EMPSSubscribers	Returns list of subscribers for a publisher.	-PublisherServer -PublisherDatabase

Cmdlet	Description	Parameters
	This cmdlet writes a list of objects to the output pipeline with the string properties 'ServerInstance' and 'Database'.	-ConfigurerCredential *PSCredential*
Reset-EMPSGeoSyncDatabase	Removes GeoSync setup from a single database where linked databases may not be available. Used to remove GeoSync information if subscribers or publisher are not available. This only runs in live mode. If -SubscriberDisplayName is specified, reference to that subscriber is removed from a publisher database. Otherwise removes all GeoSync objects from any database (publisher or subscriber).	-Server -Database -ConfigurerCredential -SubscriberDisplayName -Force
Start-EMPSBatchSync	Programmatically starts a batch sync from the specified publisher database to a specified subscriber database. Used to initiate a batch sync for any matching subscriber. This is the same as triggering a batch sync from the console. This command is asynchronous. It will return an object reflecting the status of the request but will not block until the sync has completed.	-SubscriberDisplayName -ConfigOnly
Stop-EMPSBatchSync	Stops an executing batch sync.	-SubscriberDisplayName

Cmdlet	Description	Parameters
	Used to stop a running batch sync for any matching subscriber. This is the same as canceling a batch sync from the console. This command is asynchronous. It will return an object reflecting the status of the request but will not block until the cancel has completed.	
Get-EMPSBatchSyncStatus	Retrieves the status of a sync. Used to return the sync status for any matching subscriber. This is the same status that is displayed in the console. It will return an object reflecting the status of the request.	-SubscriberDisplayName

Parameter Definitions

Parameter	Description
-PublisherServer	Server name for publisher server. For non-default instance use server\instance format.
-PublisherDatabase	Name of publisher database.
-SubscriberServer	Server name for subscriber server. For non-default instance use server\instance format.
-SubscriberDatabase	Name of subscriber database.
-DisplayName	Optional display name refers to the publisher in subscriber databases and the subscriber in publisher databases. If omitted, it defaults to the leftmost component of the server name. If this does not result in a unique name when the subscriber is set up an error is displayed.
-Verbose	Verbose output displayed - optional.
-ConfigurerCredential *PSCredential*	Credential to use for configuration. If omitted, the current windows credential is used. If the username contains a backslash, the credential is treated as a windows credential. Otherwise it is treated as a SQL

Parameter	Description
	credential.
-ServiceCredential *PSCredential*	Credential for service access on the subscriber (used for initial batch sync). This must be an existing service account on the subscriber. If the username has a backslash it is considered to be a windows credential, otherwise a SQL credential.
-ExportScript	Specifies export mode.
-ScriptFolder *folder*	Optionally specify a folder that the script is written to. This may be an absolute or relative path. If the folder doesn't exist it is created - provided that its parent folder exists.
-Force	If specified, an existing script of the same name will be overwritten. When a subscriber display name or pattern is specified, prevents the cmdlet from prompting for confirmation before each subscriber is removed.
-PublisherDisplayName	Optional display name of publisher for subscriber database. This should match the display name created at the publisher end.
-Server	Server name. For non-default instances, use server\instance format.
-Database	Database name.
-SubscriberDisplayName	If specified removes subscriber(s) matching the display name from a publisher. Name may include wildcards * and ?. If not specified all GeoSync setup is removed from the database (whether publisher or subscriber).
-ConfigOnly	Will initiate a configuration only sync.

Generate scripts to configure GeoSync

The GeoSync cmdlets can be used to generate SQL scripts for setting up and tearing down GeoSync. This is useful if the user does not have enough privileges to modify the respective databases. Instead the scripts can be passed to a database administrator to be executed.

Export mode is available by specifying the -ExportScript parameter with the cmdlets New-EMPSPublisher, Add-EMPSSubscriber, Remove-EMPSSubscriber, and Remove-EMPSPublisher. The other cmdlets do not have an export feature.

The cmdlets are loaded by executing Import-Apsinstancemodule. This may produce a warning if the user is not an administrator but it doesn't affect the script generation.

New-EMPSPublisher

If -ExportScript is specified, -ConfigurerCredential is not used and additional parameters are available:

- -ScriptFolder specifies a folder where the script is written - if omitted a script is written to the current folder
- -Force tells the cmdlet to overwrite a script with the same name if it exists.

The script produced is named Publisher-<server>-<instance>-<database>.sql. This script can be run using sqlcmd against the publisher database. If SQL Server Management Studio is used, the query window used must be in sqlcmd mode.

Unlike running the cmdlet 'live', no checks are made to see if the database has already been set up.

Add-EMPSSubscriber

If -ExportScript is specified, -ConfigureCredential is not used and -ScriptFolder and -Force are available as for New-EMPSPublisher. The -ServiceCredential must be specified. Add-EMPSSubscriber produces three scripts:

- **Subscriber-<server>-<instance>-<database>.sql** - This script should be run first against the subscriber database to do the base setup. Server/instance/database refer to the subscriber
- **Add-<server>-<instance>-<database>ToPublisher.sql** - Run on the publisher server to add a reference to the subscriber.
- **AddPublisherTo<server>-<instance>-<database>.sql** - Run on the subscriber server to add a reference to the publisher.

Remove-EMPSSubscriber

Similar to Add-EMPSSubscriber in ExportScript mode, but -ServiceCredential is not required. Two scripts are produced:

- **Remove-<server>-<instance>-<database>FromPublisher.sql** - Run on the publisher server to remove the reference to the subscriber.
- **RemoveSubscriber<server>-<instance>-<database>.sql** - Run on the subscriber server to remove publisher reference and remove the base setup.

Remove-EMPSPublisher

As above, -ExportScript comes with -Force and -ScriptFolder and -ConfigurerCredential is not relevant. Produces a single script:

- **RemovePublisher-<server>-<instance>-<database>FromPublisher.sql** - Run on the publisher server to remove the publisher and revert the database to a standard personalization database.

Satellite Database as a GeoSync Subscriber

This procedure addresses a situation where a personalization server database has been created by exporting some or all of the configuration from a larger, master database (using import/export functionality) and is used remotely for a smaller number of users. The customer wants to use GeoSync to automatically synchronize a subset of users between the master and satellite by making them GeoSync publisher and subscriber respectively. This wasn't possible using the existing merge replication scripts as they sync all of the database.

The import/export of a configuration alters the database IDs (GUIDs) that the GeoSync feature relies on to match the publisher and subscriber. This problem is solved by modifying all the GUIDs in the subscriber to match the publisher. To do this, downtime is needed at the subscriber - no affected user can be logged on, and any offline caches on user machines will be invalidated as they cannot be saved back to the modified database on the next connection. Also, if any Windows Settings Groups 'OriginalName' columns don't match on the publisher and subscriber, a sync cannot be performed.

The GUID mapping is performed by a PowerShell script (PrepareGeoSubscriber.ps1), which uses the sqlcmd utility and two SQL scripts (CheckMapping.sql and MapUgs.sql) which are required to be in the same folder.

The scripts are located here: *:\Program Files\AppSense\Environment Manager\Personalization Server\Support*

Limitations

If the publisher and subscriber databases were not created using the same software version, the following issues may arise:

- Due to the introduction of Windows 10 and Server 2016, some Windows Settings Group (WSG) names changed between database versions. If groups are exported and imported to the subscriber, and the subscriber has both old and new names, synchronization of WSGs is not possible as the OriginalName columns in the DesktopSettings.[Group] table will differ. Original names cannot be easily changed as it would require a scan of both the ApplicationData and ApplicationDataArchives tables. The mapping process described in this topic does not support this.
- If the same users to be synchronized exist in both the publisher and subscriber databases and the users were initially created with versions of Personalization Server prior to 8.4, they cannot be synchronized. This is because, prior to 8.4, user identities (UserPK column) were randomly allocated according to the usual GUID algorithm. From 8.4, the GUIDs are derived from the users' SIDs and will be consistent across databases. The solution to this problem is to physically delete the affected users from one of the databases using SQL DELETE on the dbo.[User].table.

Prerequisites

- The user running the scripts has sysadmin access to both databases via Windows Integrated Authentication.

- The scripts are run on a machine which has the sqlcmd.exe utility in the current path. One of the database servers involved might be the most convenient but sqlcmd.exe can be installed on a different machine by downloading the appropriate MSI from Microsoft.
- The publisher and subscriber databases must be accessible to each other and the script over the network. Normal SQL server connections (usually on port 1433) are used by both sqlcmd and the GeoSync software itself.

Initial Setup

The script is applied to a single personalization group at a time. The personalization group (identified by name) must appear on both publisher and subscriber before starting. It is assumed that GeoSync is not yet set up, and the terms 'publisher' and 'subscriber' refer to their intended use.

Normally it is assumed that a personalization group is exported from the publisher and imported into the subscriber using the import/export functionality. But if a new personalization group is created on the subscriber using application groups and windows settings groups imported from the publisher, it is possible to sync it by exporting the group from the subscriber and importing it back into the publisher.

In either case the script assumes that the personalization group to be synchronized initially exists on both databases.

Running the Script

The PowerShell script and the two SQL scripts must be in the same directory. Run the PowerShell script from a PowerShell command prompt - elevation is not required. It prompts for the details of both databases and the name of the personalization group to be synchronized. Checks are made that the specified databases exist, then the two SQL scripts are run. These scripts run on the subscriber but contact the publisher by creating a linked server entry, which is deleted afterwards.

The two scripts do the following:

- **CheckMapping.sql** - Compares all the details of the group to identify possible problems. These problems come in three categories:
  - **Warnings** - This is where the personalization group on the publisher contains extra entities, such as application groups, that are not present on the subscriber. After syncing the subscriber may therefore receive additional entities.
  - **Errors** - The personalization group on the subscriber has extra entities not present on the publisher. These may result in data disappearing from the subscriber and should be investigated.
  - **Fatals** - Windows settings groups 'originalname' fields don't match on the publisher and subscriber, usually due to similar data already present on the subscriber. Mapping cannot be performed.
- **MapUGs.sql** - Performs the mapping. This cannot be run if 'Fatals' have been discovered. The user is prompted first before this is run so he can make the required changes and restart.

Setting up GeoSync

After syncing the personalization group, GeoSync can be enabled between the two databases as described here. After setup, the synchronized personalization group must be set as synchronized on its GeoSync tab in the Environment Manager console. If this group has existing data on the publisher, setup of the GeoSync conditions might be required to ensure that not all of the publisher's data is transmitted to the subscriber.

CheckMapping Actions

CheckMapping.sql checks the following on the publisher and subscriber databases:

Checks	Problem category
The personalization group does not exist in both databases.	**Fatal**
Checkbox items on the Settings tab are not the same between the personalization groups.	**Warning**
Affected users exist on both databases, with the same SID but different GUIDs.	**Fatal**
The setting of the Advanced Property UpgradeFbrToHive differs between databases.	**Fatal**
Applications group assignments differ.	Publisher has more Application Groups - **Warning** Subscriber has more Application Groups - **Error**
Applications assigned to Application Groups differ.	Publisher has more - **Warning** Subscriber has more - **Error**
Application definitions differ - EXE, OS version, file version.	Publisher has more - **Warning**

Checks	Problem category
	Subscriber has more - **Error**
Registry, file, and folder paths assigned to application groups differ.	Publisher has more - **Warning** Subscriber has more - **Error**
Application group managed folders differ.	Publisher has more - **Warning** Subscriber has more - **Error**
Windows Settings Groups assignments differ between databases.	Publisher has more - **Warning** Subscriber has more - **Error**
Windows Settings Groups components, settings, custom settings, conditions, differ.	Publisher has more - **Warning** Subscriber has more - **Error**
OriginalName columns of WSGs to be synced differ. This can occur during import if existing WSGs on the subscriber had matching original names. It cannot be easily resolved as the 'original name' is used in the data and the archives and is not fixed by the MapUGs.sql script.	**Fatal**

Personalization Analysis

Personalization Analysis allows you to view data collected on a Personalization Server about users, applications and Windows Personalization. Reports can be run for Personalization Groups to display current and historical personalization data.

Once a report has been generated, the information can be used to directly manipulate data on the Personalization Server. This functionality has a real-time effect on application and user settings on the live database allowing administrators to:

- Manually create and delete archives for application settings
- Restore application settings from a previous, archived state
- Delete a user's application settings, reverting to the application's default settings
- View and edit an application's stored registry and file data
- Convert discovered applications to managed applications
- Move application settings between personalization groups

Multiple Personalization Analysis report windows can be opened at the same time allowing data to be easily compared between different users, applications and Windows Settings.

The Environment Manager Support Console allows users to use Personalization Analysis functionality without full configuration access to the database.

Generate a Personalization Analysis Report

1. Select the **User Personalization** navigation button.
2. Select **Personalization Groups** and select a personalization group to analyze.
3. Click **Personalization Analysis** from the Tools & Wizards ribbon. The Personalization Analysis report window displays for the selected personalization group.
4. Use the tabs to select the required report type:
    - Size
    - Application Usage
    - Discovered Application Usage
    - Archive Reports
5. Select the required criteria for the report. Each report has different criteria which can be set to manipulate the results:
    - **Size** and **Usage** reports can be generated for applications or users.
    - **Archive** reports can only be generated a specified user.
    - **Usage** reports can produce results for a specified time period. The default period is the week prior to and including the current date.

6. Click **Display**. A report based on the criteria entered is generated and displayed.

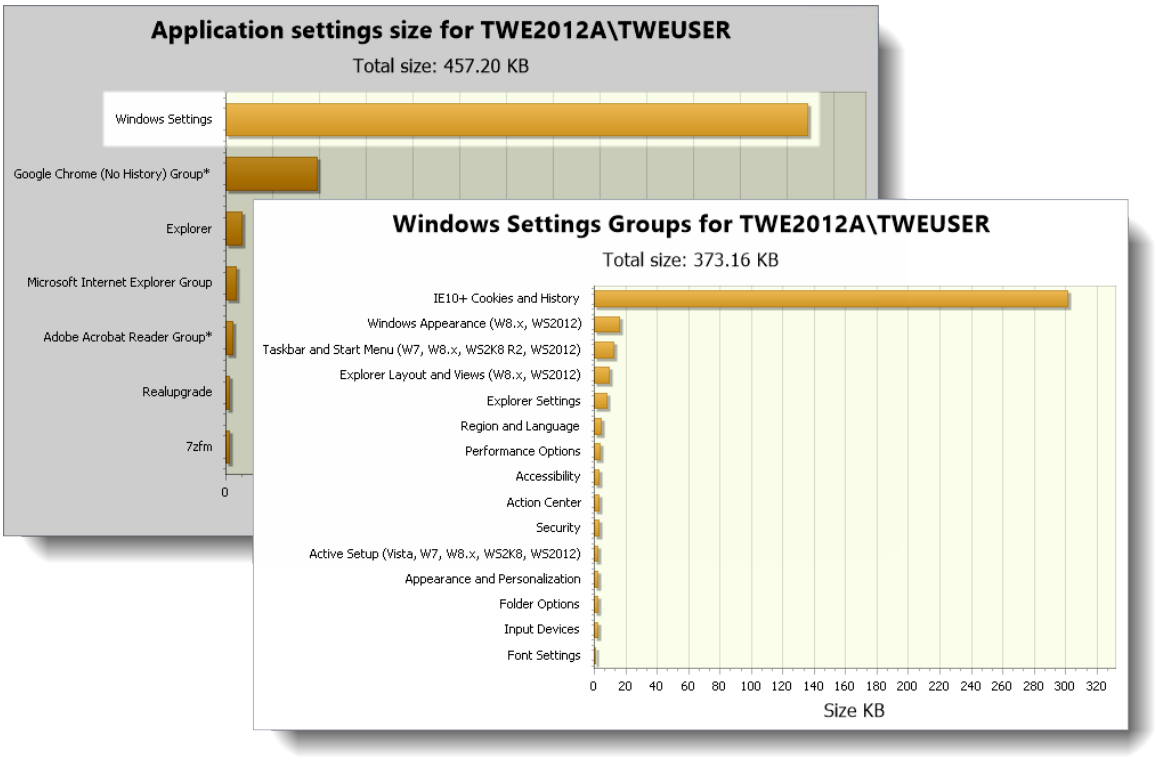
   Using the **Sort by** drop-down, **Size** reports can be ordered by **Size** or **User** and **Usage** reports by **Accesses** or **User**.

7. Click **Print** to generate a printable copy of the report. Page Settings and other print options can be used as required prior to printing.

Personalization Analysis and Windows Settings

Within Personalization Analysis, Windows Settings are listed as an application in Size, Application Usage and Archive reports.

Data for each Windows Settings Group can be accessed by clicking the Windows Settings bar. This allows the registry and file list to be edited and settings deleted for each group.



Size and Usage Reports

These reports show the amount of application and user personalization data used together with the applications that managed users are accessing. Three separate reports are available:

- **Size** - Generates a report to show how much personalization data is stored on the database per application and user. This information can identify bottlenecks and resource problems for applications and used to eliminate unnecessary registry keys and folders from personalization to reduce the amount of data being transferred between endpoints and the server.

- **Usage** - Generates a report which displays the number of times a managed application has been accessed by users over a specified time period.

Each report has a combination of functions, accessible from generated analysis reports. Right-click on a bar in one of the graphs to access the shortcut menu.

Size and Usage Report Criteria

The size and usage reports can be generated using the following criteria:

- **Report by User and <All Users>** - Reports are generated per user for all users in the database, in size or usage order. Double-click on a user to see data on their individual applications. For the application size report, each bar represents the total amount of personalization data for the user. For usage reports, each bar represents the total usage count for applications run by users.
- **Report by User for a specific user** - Reports show all applications for that user, with the data displayed per application.
- **Report by Application and <All Applications>** - Reports are displayed per application showing the data for all users in the Personalization Group. The size graph for this report shows the total size of settings stored for all users in the group for each application. Double-click on an application to show data for each user.
- **Report by Application for a specific application** - Shows the report data for each user's usage of that application. For example, the application size graph shows the amount of personalization data for each user for that application only.

To report on all users or all applications, delete any existing contents of the Report By field.

Move a User's Personalization Settings to Another Group

When a user is added to a specific personalization group, their personalization settings are only relevant for that group. Personalization Analysis enables the administrator to move the settings to another group.

This option is only available for User data and can only be performed if more than one personalization group exists.

This task only moves the user data from one personalization group to another. An administrator must move the actual user from one group to another using group membership rules. See Personalization Group Membership Rules.

1. Select the **User Personalization** navigation button.
2. Select **Personalization Groups** and select a personalization group.
3. Click **Personalization Analysis** from the Tools & Wizards ribbon. The Personalization Analysis report window displays for the selected personalization group.

4. Select a compatible report; **Size** or **Application Usage**.
5. Ensure the Report By settings are configured to **User** and **<All Users>**.
6. Click **Display**. The report for all users displays.
7. Right-click the user you wish to move and select **Move the settings for** [user] **to another group...** This prompts you to choose an available group to move the chosen user's personalization settings to.
8. Select the Personalization group to receive the user settings.
9. Click **Continue** to proceed and **OK** to confirm. The graph is refreshed with the user removed from the report.

Delete All User Data For a Selected User

In a size or usage report, select this option from a user bar shortcut menu to delete all personalization data and archives for that user. The next time the user starts any application, the default settings will be reinstated.

Delete Application Settings for a User

In a size or usage report, select this option from an application bar shortcut menu to delete the cache of an application for the selected user. Next time the user starts the application, it will revert to the default settings.

If you delete the application cache for a user who is logged on, the deletion may take longer to delete on the client as it is linked to the configuration poll, which runs every 10 minutes by default.

Clear All Usage Counts for a User

This action can be performed for usage reports on both application and user bars. Select this option from the shortcut menu to reset the application accesses count to zero for all of the user's managed applications.

Delete All User Data for a User

In a size or usage report, select this option from the shortcut menu of a user or application bar to delete all settings and archives for all applications for the specified user.

Edit Virtual Registry for an Application

Once generated the size and usage reports allow administrator's access to a registry editor which enables stored registry data for an application to be examined and edited. Files can be imported and exported and registry keys can be added, deleted, edited and excluded.

Caution: Editing registry settings can cause application failure and serious system problems which may require re-installation of your operating system. Before making any changes, create an archive for this application. See Archive Reports.

1. Create a size or usage report for a user.
2. Locate the application you want to view, right-click on the bar for that application and select **Edit application registry...**
3. A warning dialog displays. Disable the dialog for the session if required using the checkbox and click **OK**.

   The Edit Registry Settings dialog box displays showing the virtual registry structure for the application.
4. Select the required option:
   - **Import** - Click Import from the File menu to import a registry key from the local disk for the selected application. Imported files have the REG extension, as used by the Windows Regedit utility.
   - **Export** - Highlight a registry key and click Export from the File menu to export and save it to the local disk. The key can then be imported into other application's registries as required. Exported files have the REG extension, as used by the Windows Regedit utility.
   - **Print** - Click from the File menu to generate a printable Registry Settings Report for the application.
   - **New** - Click **New** from the Edit menu to create a new key and set the required values.
   - **Rename Key** - Highlight a registry key and select **Rename Key** from the Edit menu.
   - **Delete Key** - Highlight a registry key and select **Delete Key** from the Edit menu.
   - **Exclude** - Highlight a registry key and select **Exclude** from the Edit menu. The selected key is added to the Exclude list for the application. For further information, see Inclusions and Exclusions.
   - **Hide R.I.P. Entries** - Keys with an RIP extension represent residual keys, for example, keys that have been renamed or deleted. These keys are still virtualized to ensure correct behavior. However, when examining the registry, it may give a clearer view if these keys are hidden.
5. Select this checkbox to hide these entries from the registry editor.
6. When all required actions have been made, click **OK** to commit them to the database.

Edit the Application File List

Once generated the Size and Usage reports enable administrators to view the folder structure for an application or application group. This structure allows files and folders to be imported, excluded and deleted directly from Personalization Analysis reports.

1. Create a Size or Usage report for a user.
2. Locate the application you want to view, right-click on the bar for that application and select **Edit application file list...**
3. From the Folder Display drop-down, select the file structure you want to view:
    - **Vista and Windows 7 and above**
    - **XP**
    - **Raw**
4. Select a View Type; **Tree File View** or **Flat File View**.
5. Navigate to the required folder.
6. The following options are available:
    - **Import** - Right-click in the details pane and select **Import** to add files from the local disk to the selected folder.
    - **Export** - Right-click on a file and select **Export** to save the selected file to the local disk.
    - **Open** - Right-click on a file and select **Open**. This extracts the file to a temporary location and attempts to open the associated application. If the application modifies the file the modifications are written back to the profile in the database.
    - **Delete** - Right-click on a file and select **Delete** to remove the selected file from the database. Multiple files can be selected using CTRL and shift when selecting files. You can also select a file and delete its contents.
    - **Print** - Click Print to generate a printable Application File Report for the selected file.
7. Click **OK** to save any changes or to quit the file list.

Archive Reports

All managed application's stored user personalization settings are archived daily, recording the user's settings for each application and creating a restore point per application. The default daily archive is set at 1.00 am. This can be amended to any convenient time using the DailyArchiveStartTime Global Setting.

For details of how to change the DailyArchiveStartTime setting, see Advanced Settings.

Manual archives can also be created when required. Each archive can be used to return an application's settings to the position they were in at the time of the archive.

Environment Manager detects duplicate files within new application, Application Group and Windows Settings Group archives. Within the database, only one copy is stored regardless of how many archives the file exists in. This provides a large reduction in database size compared to previous versions of Environment Manager.

Archive reports list all archive points created for the managed applications of a selected user.

Manually Archive Application Data

1. Generate an Archive report for the required user.
2. Click **Display**.

   The report is created and a list of managed applications displays for the selected user. Each application entry in the report shows the EXE name, application version and operating system. The existing archive(s) for each application are listed beneath the application, accessed by expanding the tree.
3. Select the application for which you want to create an archive.
4. Right-click and select **Archive** [application] **now...**

An archive is created which stores the personalization settings defined by the user for that application, at the time the archive is created. The date and time at which the archive was created is used as the archive name.

If the user has the application open at the time the archive is created, these settings are not taken into account. The settings as they were the last time the application was closed and synchronized with the database are archived.

Roll Back an Application

This option returns a user's application settings to a previous state as recorded at an archive point. If a user's settings for a particular application become corrupted or are not as expected by that user, they may want to return them to a state when the application was successfully operating.

Select the required application in the **Archive** report and expand the tree beneath to display the related archives. Select the required archive, right-click and select **Roll back to this archive**.

The rollback replaces the current settings in the database for that application with the settings at the time of the archive. The next time the user accesses that application, their settings are reset.

Modify Archives

This option allows you to change the protection settings for an archive - protection can be added or removed for an archive.

1. Select the required application in the Archive report and expand the tree beneath to display the related archives.
2. Highlight the required archive, right-click and select **Modify archive**.

   The Modify Archive dialog displays.
3. Select the **Protect archive** checkbox as required. Only one archive can be protected per application.

4. Add or update the archive description if required.
5. Click **OK** to commit the changes.

Delete Archives

Unprotected archives can be deleted as required using one of the options from the shortcut menu:

- Delete an archive - Select the required archive, right-click and select **Delete this archive**.
- Delete all archives for an application - Select an application, right-click and select **Delete all archives for** [application]

Protected archives cannot be deleted. Use the Modify Archive option to remove protection from an archive before deleting.

Environment Manager Support Console

The Support Console offers read-only access to Environment Manager Personalization configurations and allows users to view Personalization Analysis reports. Support Console users can also use the associated analysis functionality, such as roll back application settings and convert discovered applications. Using this role, support teams can safely carry out routine maintenance for end users in a focused environment, without full configuration access to the database to perform these tasks.

When a user with a Support Console role connects, functionality to change the personalization configuration is automatically disabled and the console changes to a blue color scheme.

Support Console Functionality

The table below lists the functionality available to users with a Support Console role.

Function	Availability	Link
Connect/Disconnect	Support Console users can configure the list of Personalization Servers and connect and disconnect to/from them as required.	Connection
Advanced Settings	Read only access to view the list of database and communications settings.	Advanced Settings
Application Exclusions	Read-only access to the list of applications which are globally excluded from personalization.	Application Exclusions
Options Ribbon	Includes the following display options: • Show AND and OR labels • Disable Splash Screen • Reset View Customizations	Options Ribbon
Help Ribbon	Access to the online help, the Ivanti website, information about the console and a means of contacting Support.	Help Ribbon
Personalization Analysis	Full access to Personalization Analysis functionality to enable reports to be run and archives to be managed. Application data can be managed for users and discovered applications can be converted to managed applications.	Personalization Analysis

Streamed Applications

Once an application is under the control of User Personalization users receive their managed personalization data regardless of how they access the application. This includes virtualized applications which are streamed from a server rather than run locally. Commonly, streaming involves packaging an application in such a way that it is self-contained. For User Personalization streamed applications are managed in the same way as local applications.

To see which streamed applications are supported, access the Maintained Platforms Matrix.

Citrix XenApp

To set up Citrix XenApp streaming applications to work with certain elements of Environment Manager, such as Lockdown, Process Started and Stopped triggers and User Personalization, you need to specify certain exclusions, as follows:

1. Navigate to Citrix Streaming Profiler for Windows.
2. Open the Application Profile.
3. Highlight the relevant Target and select the **Edit** menu.
4. Select **Target Properties**.

   The Target Properties screen displays.
5. Select **Rules**.

   The Rules work area displays on the right hand side.
6. Click **Add** in the Rules work area.

   The New Rule Select Action and Objects dialog box displays.
7. In the Action section leave the default setting as **Ignore**.
8. In the Object section select **Named Objects** and click **Next**.

   The New Rule Select Objects dialog box displays.
9. Select **Some Named Objects** and click **Add**.

   The Choose Named Object dialog box displays.
10. Add the following entries and click **OK**:
    - **Appsense***
    - **\??\pipe\Appsense***

    These display in Named Objects on the New Rule Select Objects dialog box.
11. Click **Next** to display the New Rule Name Rule dialog box.
12. Enter a name for the rule or accept the default and click **Finish**.

13. Click **OK**.

    The Target Properties screen re-displays and the Ignore all named objects rule is now listed in the work area on the right hand side.

14. Save the profile.
15. Repeat for each **Application Profile** as required.

User Personalization

If using Environment Manager User Personalization you need to complete the following task in addition:

1. Navigate to Citrix Streaming Profiler for Windows.
2. Open the Application Profile.
3. Highlight the relevant Target and select the **Edit** menu.
4. Select **Target Properties**.

   The Target Properties screen displays.

5. Select **Rules**.

   The Rules work area displays on the right hand side.

6. Click **Add** in the Rules work area.

   The New Rule Select Action and Objects dialog box displays.

7. In the Action section leave the default setting as **Ignore**.
8. In the Object section select **Files and Folders** and click **Next**.

   The Select Objects dialog box displays.

9. Click **Add**.

   The Choose Path dialog box displays.

10. In Path enter **C:\AppSenseVirtual** and click **OK**.

    The New Rule Name Rule dialog box re-displays.

11. Click **Next**.
12. Enter a name for the rule or accept the default and click **Finish**.
13. Click **OK** to apply the rule.
14. Save the Profile.
15. Repeat for each Application Profile as required.

Symantec Virtualization

This section provides steps for setting up exclusions when using Environment Manager and Symantec Workspace Virtualization (6.1) and Symantec Software Virtualization Solution (2.1)

Symantec

It is recommended that you exclude the folder C:\AppSenseVirtual from the Symantec solution. Do this either as a global exclusion on the Symantec solution client or, alternatively, as an exclusion within each Symantec solution layer that is to be personalized by Environment Manager.

To add a global exclusion for the Symantec solution client:

1. Open the Symantec solution console.
2. Select **File**>**Global Excludes**.
3. Right-click within the console and select **New Exclude Entry**.
4. Select **Directory** and enter *C:\AppSenseVirtual*.
5. Select **Exclude Subdirectories** and click **OK**.
6. In the Symantec solution, exclude anything where user data is written (AppData and subdirectories, LocalAppData and subdirectories). Ensure there is no user data captured in the layer.

Environment Manager

It is recommended that you exclude the folder *C:\Fslrdr* from Environment Manager. Do this either as a global exclusion at the Personalization Group level, or for a particular application.

To add a global exclusion for Environment Manager:

1. Open Environment Manager.
2. Select the **User Personalization** bar in the left navigation pane.
3. Select **Personalization Applications** and globally exclude *%SYSTEMDRIVE%\fslrdr*.
4. Expand **Application Categories** and ensure that applications are matched by file name only and not the full path.

Support for Citrix Offline Plug-in 6.0

In order to provide support for Citrix Offline Plug-in 6.0, a driver is included in the EM User Virtualization Service software. The driver, called **AsVfxLdr.sys**, replaces the existing Windows AppInit_DLLs registry value for loading the personalization modules into managed processes. The driver enables better control over what is hooked and when.

For Citrix Offline Plug-in 6.0t all hooking is performed via a kernel based API and the driver enables Environment Manager's hook DLLs to be loaded after the Citrix hooks, as part of the process initialization.

With the driver it is possible to exclude certain processes from having the personalization modules loaded by setting the following registry value on the client:

- **Key** - HKLM\Software\AppSense Technologies\AsVfxLdr\
- **Name** - Exceptions
- **Type** - REG_MULTI_SZ
- **Data** - List of processes that should be ignored by the driver. The list should only contain the filename of the process including the file extension, e.g. calc.exe; full paths are ignored and will not be matched. The list is stored in multi-string format with each filename as a separate string. The driver will not attempt to load any DLLs into these processes.

It is also possible to disable the driver and revert to the existing AppInit_DLLs mechanism by setting the following registry value on the client:

- **Key** - HKLM\Software\AppSense Technologies\Environment Manager\
- **Name** - LegacyAppInit
- **Type** - REG_DWORD
- **Data** - Controls whether the EMLoader.dll should be loaded using the legacy AppInit_DLLs value instead of the driver. If this value is set to a non-zero value, the Environment Manager service will modify the AppInit_DLLs entry on start-up to include AsVfxLdrAppInit.dll; on stop it will also remove the entry. The AsVfxLdrAppInit.dll uses the same registry keys as the driver and loads the EMLoader.dll in a similar way to the driver.

This means that AsVfxLdrAppInit.dll appears in the AppInit_DLLs entry rather than EMLoader.dll as in previous releases.

The AppInit_DLLs must not be manually edited.