

## ENVIRONMENT MANAGER – PERSONALIZATION SERVER Best Practice Guide (version 8.0.x.0)

AppSense Environment Manager Personalization (version 8.0.x.0) best practice include:

- [Introduction](#)
- [Supported Operating Systems](#)
- [Personalization Architecture Best Practice](#)
- [Enabling Personalization Server](#)
- [Personalization Group Usage](#)
- [Personalization Sites Configuration](#)
- [Personalization Implementation](#)
- [Personalization Hints and Tips](#)

### Introduction

#### **Purpose of this Document**

This document is designed to help an engineer implement AppSense Environment Manager Personalization (EMP) to the “best of its ability”. Ensuring the customer experiences the benefits of the AppSense’ User Environment Management (UEM) solution.

#### **Assumptions**

This guide assumes that there are already existing user profiles being used, in the form of roaming profiles. And, that all applications within the environment are known.

### Supported Operating Systems

#### **AppSense Personalization Client (Environment Manager Agent)**

- Microsoft Windows XP Professional with Service Pack 3 (32-bit and 64-editions)
- Microsoft Windows Vista Business, Enterprise, or Ultimate with or without Service Pack 2

(32-bit and 64-bit editions)

- Microsoft Windows Server 2003 with Service Pack 1 or 2 (32-bit and 64-bit editions)
- Microsoft Windows Server 2003 R2 with Service Pack 1 or 2 (32-bit and 64-bit editions)
- Microsoft Windows Server 2008 with or without Service Pack 2 (32-bit and 64-bit editions)

#### **AppSense Personalization Server**

- Microsoft Windows Server 2003 with Service Pack 1 or 2 (32-bit and 64-bit editions)
- Microsoft Windows Server 2003 R2 with Service Pack 1 or 2 (32-bit and 64-bit editions)
- Microsoft Windows Server 2008 with or without Service Pack 2 (32-bit and 64-bit editions)

#### **AppSense Personalization Database Server**

- Microsoft SQL Server 2000 – all editions (32-bit and 64-bit editions)
- Microsoft SQL Server 2005 – all editions (32-bit and 64-bit editions)
- Microsoft SQL Server 2008 – all editions (32-bit and 64-bit editions)

## Personalization Architecture Design Best Practice

### **Standard Architecture**

AppSense Environment Manager Personalization has a standard architecture of:

- **Personalization Database**

This is where all the user profiles managed by the EMP are stored. Communications to or from this location to the client are via the Personalization Server over port 1433 TCP.
- **Personalization Server**

The Personalization Server sits in between the Personalization Client and the Personalization Database. It is responsible for delivering the Personalization configuration to client upon request from the client and also managing the personalization synchronizations. Communication is via port 80 or 443 TCP (HTTP / HTTPS).
- **Personalization Client**

The Personalization Client is responsible for communicating with the Personalization Server, retrieving the Personalization configuration, and applying the configuration to the user. The Personalization Client is actually the AppSense Environment Manager Agent.



Environment Manager Personalization Architecture with Management Centre

**Best Practice**

The following points should be adhered to as AppSense best practice when designing and implementing Environment Manager Personalization (EMP).

- The Personalization Database and Personalization Server should be installed on separate devices (physical or virtual).
- Where possible the Personalization Database should be installed with High Availability in mind, typically for this Clustering of the Microsoft SQL Server is recommended.
- Currently one Personalization Server (Quad Core & 4Gb of Physical Memory), will support 20,000 concurrent users. AppSense always recommends having multiple Personalization Servers for high availability. These servers should always be listed when Personalization is enabled within the Environment Manager Policy configuration.
- If required Personalization Servers will support Network Load Balancing being placed in front of the servers. Please refer to the **AppSense Network Load Balancing Guide** for more information.
- If a customer has multiple sites or data centers, be it for disaster recovery etc. AppSense recommends that Personalization Servers and Database are installed at these sites and local clients are pointed to their local Personalization Server and Databases.
- If multiple sites are being used, AppSense also strongly recommends the use of Microsoft SQL Replication. Please refer to the **AppSense Environment Manager Administration Guide** for information on configuring Microsoft SQL replication for EMP.

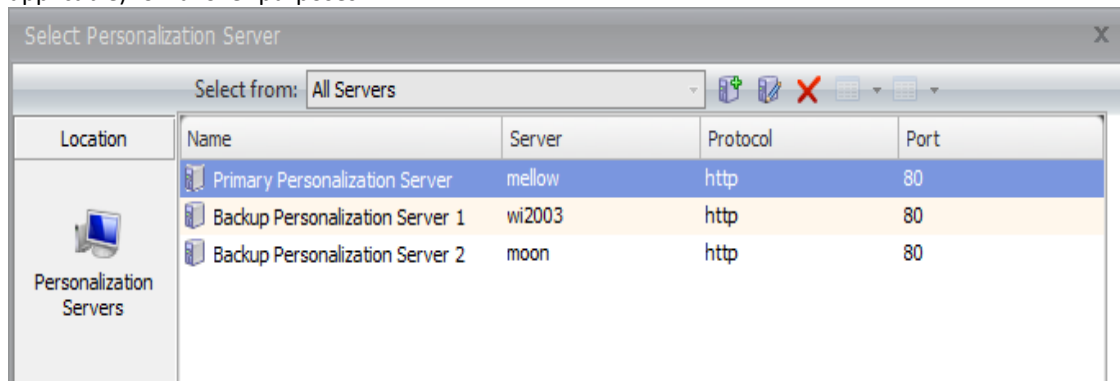
## Enabling Personalization Server

### How to Enable Personalization

Personalization is enabled from within the Policy Configuration side of the console. This is achieved by selecting the Enable User Personalization option from the General Properties section of the Home ribbon:



Within the Select Personalization Server dialog, it is then possible to add a single or multiple Personalization Servers. It is recommended multiple Personalization Servers are added here (where applicable) for failover purposes:



The Policy Configuration file that contains this list of Personalization Servers is then required to be deployed out to the endpoints, which results in the **configuration.aemp** file being sent to the managed computer.

The first time a user logs on to the managed endpoint, the list of Personalization Servers as entered above is queried from the top of the list down. If the managed endpoint can communicate with the first Personalization Server in the list, then the user gets their User Personalization configuration pulled down from the backend database via this Personalization Server.

However, if the first Personalization Server in the list is unavailable for any reason, then the next Server in the list is contacted and so on until successful communication is achieved. If this list is exhausted, i.e. no Personalization Servers are contactable, then the User Personalization configuration is not downloaded and no Personalization will take place.

It is therefore recommended that event **9661 – Timeout Communicating with Personalization Server** be enabled in the Auditing section of the Policy Configuration in order to cater for such a scenario.

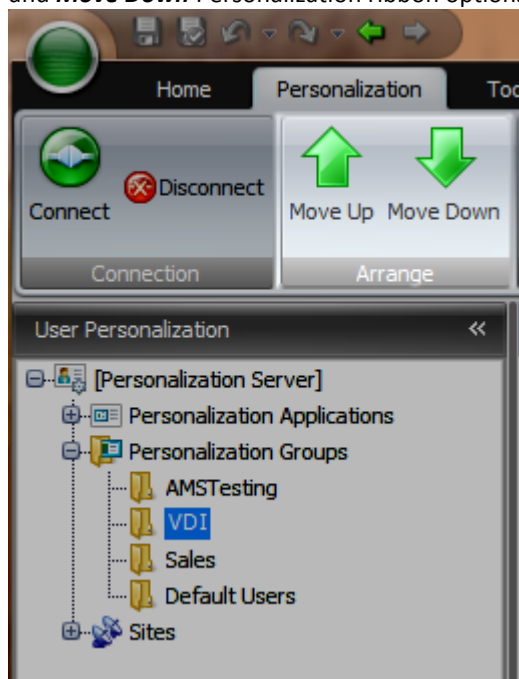
## Personalization Group Usage

### Managing Personalization Groups

Environment Manager 8.0 makes use of Personalization Groups which allows for different personalization settings to be applied to users based on different membership rules.

So for example, if a user has access to a series of Terminal Servers, then they always get the same personalization settings independent of which Terminal Server they are logging on to. However, if there is a specific server silo that contains a critical application, that does not require personalization settings to be used, then a separate Personalization Group can be created for this specific Server and the Personalization Settings can be disabled.

On occasions, a user may be a member of more than one Personalization Group. Where this is the case, the user is assigned to the first Personalization Group in the list where the membership rule is valid. With this in mind, Personalization Groups can be ordered in the list by means of the **Move Up** and **Move Down** Personalization ribbon options:



It is therefore recommended that your Personalization Groups be ordered in terms of importance to ensure that your users are assigned to the more relevant Personalization Group.

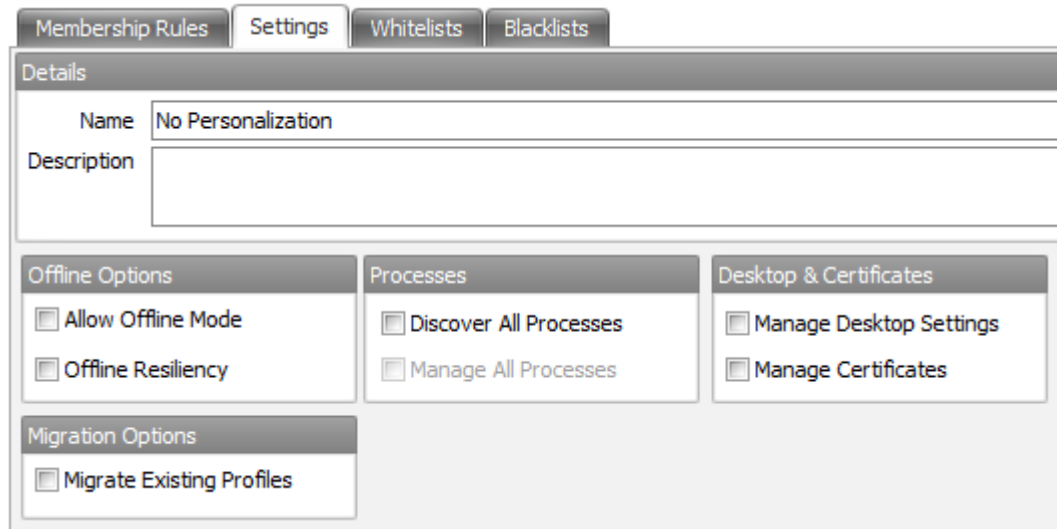
The **Default Users** Personalization Group is used as the catch-all group should none of the membership rules be passed in any of the other Personalization Groups. This is always located at the bottom of the Personalization Groups list and cannot be moved.

### Excluding Users from Personalization

Under certain circumstances, it may be viable to have users who will not be under the management of User Personalization.

By default, all users will be assigned to a Personalization Group if User Personalization is enabled. Therefore most users will fall into the Default Users Personalization Group.

In order to exclude a specific user or computer from User Personalization a new Personalization Group must be created. Once created, each option on the Settings tab will need to be disabled:



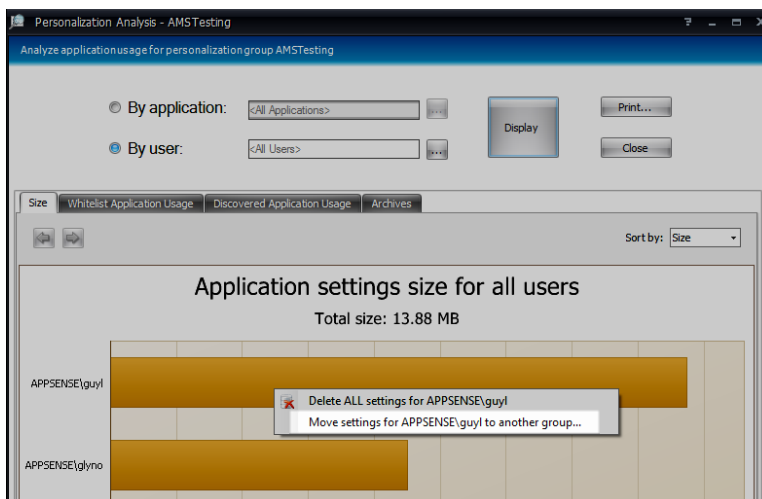
You must then add the relevant membership rules to the Personalization Group to include the users or computers you wish to exclude.

### Moving users between Personalization Groups

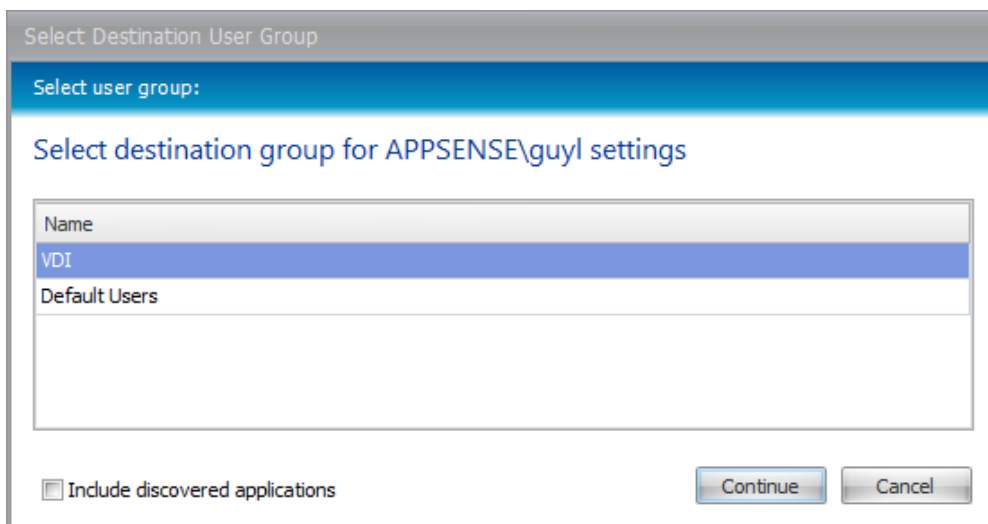
If a user is added to a specific Personalization Group, their personalization settings are only relevant for that group. If you need to move a user and their settings to another Personalization Group, this can now be done via Personalization Analysis.

This is achieved by running up a Personalization Analysis report, By user, from either the Size, Whitelist Application Usage or Discovered Application Usage reports.

It is then possible to select the user you wish to move, right click and choose 'Move settings for <user> to another group...':



This will prompt the administrator to choose another available group to move the chosen user’s personalization settings to:



There is also an option ***'Include discovered applications'*** which is off by default, which will allow you to move any discovered applications (rather than white listed applications) to the new group too. It is recommended this also be checked.

### Personalization Group Settings

Each Personalization Group has a number of options available on the Settings tab for that specific Personalization Group. These include:

- Offline Options
- Processes

- Desktop & Certificates
- Migration Options

### Offline Options

#### Allow Offline Mode

By default Allow Offline Mode is off by default. This enables mobile users to still have access to their personalization settings whilst off the corporate network.

By enabling this option, a local copy of the virtual personalization cache is retained on the managed endpoint device when the user logs off.

It is therefore recommended this option only be switched on for managed endpoints that are mobile, i.e. laptops devices, otherwise valuable disk space could be unnecessarily utilized on both static desktops and servers.

#### Offline Resiliency

By default Offline Resiliency is on by default. It is recommended this setting remains enabled.

Offline Resiliency ensures that if a user is online, but for some reason, such as network outage, Personalization Server outage or SQL Server outage, communication between the managed endpoint and the database is lost, the synchronization of personalization data from the managed endpoint to the database is re-attempted until communication is re-established.

### Processes

There are effectively three modes in which you can configure User Personalization to work:

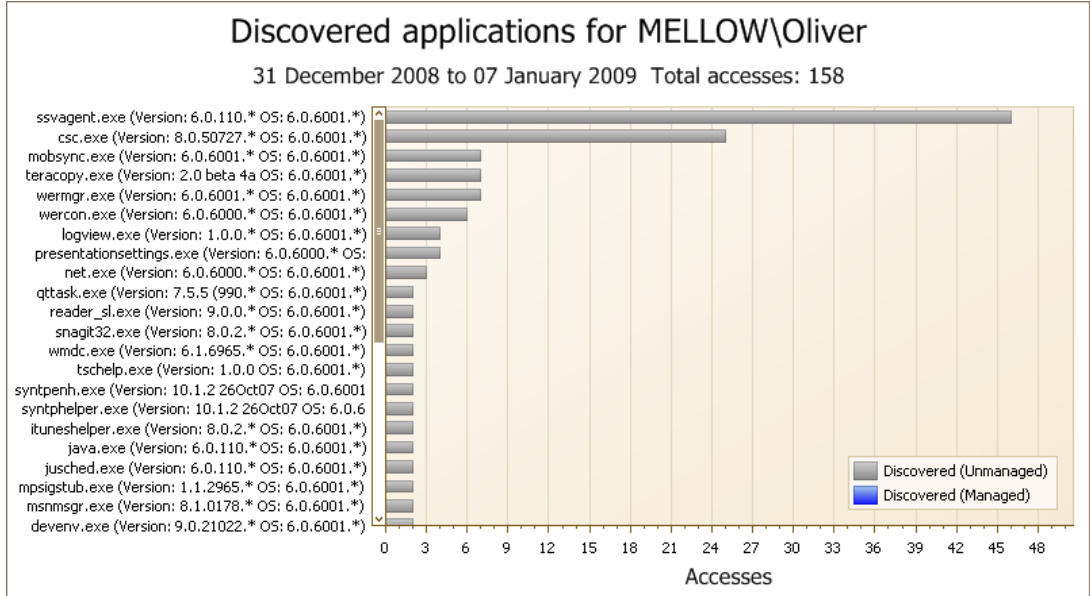
- Discover All Processes
- Manage All Processes
- Whitelists & Blacklists (these work in conjunction with Discover / Manage All Processes)

#### Discover All Processes

By default **Discover All Processes** is **off** by default.

This option is a 'passive monitoring' mode which allows managed endpoints to be monitored for launched applications. Each application a user launches is 'discovered' and recorded so that, at a later date, it can either be added to a whitelist, blacklist or deleted. It is recommended that 'Discover All Processes' is switched on by default so that applications being used by users can be identified. Personalization Analysis reports can be run that show applications discovered by the 'Discover All Processes' option:





As you can see above, Discovered (Unmanaged) applications are shown in grey in the graph above.

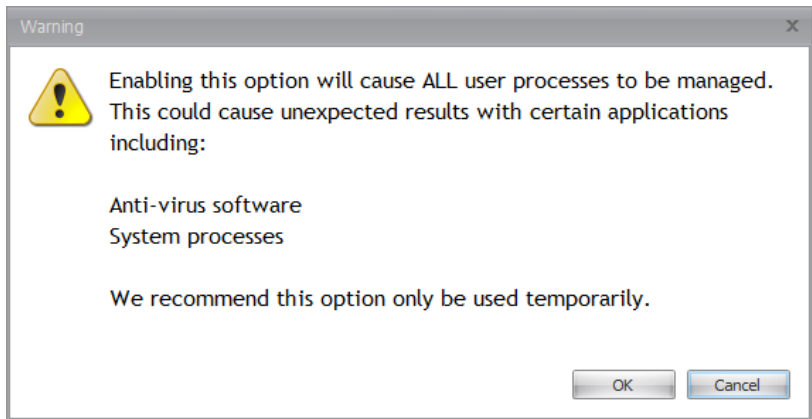
It is recommended that discovered applications are then converted to Whitelisted applications where required.

### Manage All Processes

By default **Manage All Processes** is **off** by default.

The **'Manage All Processes'** option is a sub option of the **'Discover All Processes'** option and can only be enabled if **'Discover All Processes'** is also enabled.

It is not recommended that this option be used in a live environment, but instead used in a pilot environment to identify applications and also prove that they can be personalized without issue. Enabling this option results in the following warning message being displayed:



**Discovered (Managed)** applications are shown in the Personalization Analysis graphs in blue to distinguish them from **Discovered (Unmanaged)** applications.

### Whitelists & Blacklists

It is recommended that Whitelists be utilized along with **'Discover All Processes'**. This allows the administrator to specify only a specific set of applications that a user executes to be personalized. Anything not in the Whitelist will not be managed.

For example, you may want to add applications to the whitelist such as MS Office Applications, Web Browsers, instant messaging applications etc. but exclude utility applications such as compression software, anti-virus and system tools from being personalized.

If the **'Manage All Processes'** option has been enabled, then it is recommended that a Blacklist of applications be utilized also. A Default Blacklist application group exists that contains a recommended list of Blacklisted applications. This should be assigned to any Personalization Group created that has the **'Manage All Processes'** option enabled. It should also be updated with other applications that may cause issues when the **'Manage All Processes'** option is enabled, such as anti-virus software and system processes.

### Desktop & Certificates

#### Manage Desktop Settings

By default **Manage Desktop Settings** is **on** by default.

Desktop settings are configured globally from the Desktop Settings option on the Tools Ribbon. However, the application of the settings can now be configured on a per Personalization Group basis. It is therefore recommended that **'Manage Desktop Settings'** only be enabled for Personalization Groups where you would like the desktop settings to be personalized and become mobile with the user.

So, for example, where you may want to log an administrator on to a user's machine to fix an issue, you would not want the administrator's desktop to roam with them. Therefore you could create a Personalization Group that has a membership rule for administrators only that has the **'Manage Desktop Settings'** option disabled.

#### Manage Certificates

By default **Manage Certificates** is **on** by default.

Even though this option is enabled by default, it should only be used where users are making use of mandatory profiles.

Enabling this option instigates **'profile state emulation'** whereby the operating system is fooled into thinking the user is logged in with a roaming profile. This is so that certificates can be added to the certificate store and restored the next time the user logs on. At logoff, the profile is set back to a mandatory profile.

It is therefore recommended that this option be disabled on Personalization Groups where the members of that group are not utilizing a mandatory profile.

## Migration Options

### Migrate Existing Profiles

By default ***Migrate Existing Profiles*** is **off** by default.

Environment Manager 8.0 utilizes a technique called ‘Virtualize-on-Write’ so that when an application attempts to write to the physical registry or file system, it is instead virtualized and redirected to the Environment Manager virtual cache instead.

By enabling the ‘Migrate Existing Profiles’ option an additional technique called ‘Virtualize-on-Read’ is implemented which virtualizes an application’s settings as soon as it is launched and attempts to read from the physical registry or file system.

It is recommended this option be used when migrating users from a local or roaming profile to a mandatory profile with the Environment Manager User Personalization solution. It is also recommended this be used when migrating users from one operating system to another, or from one version of an application to another.

This option should be disabled once the user has launched each application desired to be personalized. This can be ascertained from both the Discovered and / or Whitelisted application reports in Personalization Analysis.

## Personalization Sites Configuration

### Sites

Additional sites should only be configured when organizations have a requirement for more than one geographically dispersed Personalization Server (and/or SQL database).

It is recommended the primary site be installed at the organizations HQ (or IT Datacenter) as this, by default, becomes the Default Site listed under the Sites list.

Additional branch sites can then be added by installing the Personalization Server at the required branch site location and configuring it using the Server Configuration Utility.

A new Site can then be created in the Environment Manager Console and membership rules applied to it. The new Personalization Server can then be added beneath the new site.

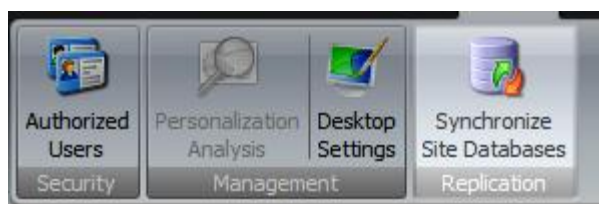
Users who log on will be provided with their User Personalization configuration from the first Personalization Server contactable as detailed in the **configuration.aemp** file. Subsequent personalization synchronizations will then occur via the designated Site based on the membership rules assigned to the individual Sites.

### Database Replication & Synchronization

Where multiple databases are required (for failover support or to support geographically dispersed locations) replication can be configured as per the **AppSense Environment Manager Administration Guide – Appendixes – Personalization Database Replication** section.

When configured, this replication will occur, by default, once per day.

However, it is recommended that the ‘Synchronize Site Databases’ option, available from the Tools ribbon, be utilized if replication between databases is required immediately:



## Personalization Implementation

### Installation

Make sure you have installed and deployed the following components:

- Installed AppSense Management Centre
- Installed and configured Environment Manager Personalization Database
- Installed and configured Environment Manager Personalization Server
- Installed the AppSense Environment Manager Agent to clients
- Configured and deploy an AppSense Environment Manager Policy configuration with Personalization enabled.
- Consider the environment you are installing into to evaluate the best configuration for High Availability such as:
  - Number and Location of Personalization Servers required.
  - What is the customer's requires with regards to High Availability and Disaster Recovery – how does the Personalization Server fit with this?
  - Are all potential client devices distributed or centralized? This will affect the location of your Personalization sites.
  - Also take into account the bandwidth and what other traffic to going to the sites. (Avg. Desktop settings are 1Mb at Logon / Log off, application settings are on Avg. 200Kb if synchronization is required)

### Configuration

Once you have installed and deployed out the above components for Environment Manager Personalization you will need to consider the following steps for configuration:

- Does the customer wish to migrate existing user profiles or start with fresh new profiles?
- Identify not only the applications the customer wishes to manage with Personalization Server but also if any applications are dependent on each other and Application Grouping is required.
- If applications are going to be delivered by a virtualization method such as Microsoft App-V or Citrix Streaming Client, please refer to the AppSense Environment Manager Administrator guide for configuring the application package to work with Environment Manager Personalization.
- Setup the Personalization Groups with regards to how you wish to manage the users. If a group of users only run Published Applications, then they may not require desktop settings to be managed for that group.

- If you are performing a migration of their existing profiles, then you will need to allow a period of time that will allow all users's to login and at least run the migrated applications once so settings can be captured.
- Configure your site memberships to ensure that devices are communicating with their closest Personalization Server and also the priority of Personalization Servers for failover is correct.
- If multiple sites are being used, configure the SQL replication as per the AppSense Environment Manager Administrator Guide
- For more intelligent failover of Personalization servers, investigate the use of Network Load Balancing.
- Ensure the any support desk staff that will be performing Personalization roll backs have sufficient rights to the Personalization Console, at the least User rights.

## Personalization Hints and Tips

### Mandatory vs. Local Profiles

A regular consideration that needs to be taken into account during the design and implementation stages is what type of profile needs to be used as the base to be loaded for the user before Environment Manager Personalization overlays the user's actual settings.

Typically most customers will create and use a Mandatory profile, as this profile is very light weight and contributes to faster logon times for users. This profile is great for environments where all users are accessing devices which are permanently online.

If the user population also uses laptops to work offline, then we 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. But, you must also remember to delete the cached copy of the local profile using Group Policy or the utility from Microsoft called **DELPROF**.

It has been found that if required a middle ground solution can be found where you create the .MAN file for the mandatory, but place it within the location of %SYSTEMDRIVE%\Default Users.

This allows us two benefits in that we do not have to specify a path within the User properties of Active Directory and that because it is a Mandatory profile, the Windows Operating System will flush this automatically. Of course this will require some time to copy to each managed device.

## Mandatory Profiles

Creating a Mandatory Profile is a straight forward task, but there are a few tips which ensure that the mandatory profile you create is as clean and basic as possible.

- Create a Template User Account in an OU with no Group Policies applied whatsoever.
- Log the Template account onto a client which also has no Group Policies and ideally no applications installed.
- Ensure you set the permissions when copying the profile to Authenticated Users.
- The only part of the mandatory profile you need to keep is the .MAN (which is renamed from the .DAT) file. The folder structure for the profile can be deleted.

Microsoft have a Technet article on how to create a mandatory profile ([http://technet.microsoft.com/en-us/library/cc786301\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc786301(WS.10).aspx)). What also needs to be taken into account is if you are using multiple Windows Operating Systems which cannot all use the same mandatory profile.

Windows XP and Windows 2003 Server can share the same .MAN, while Windows Vista, Windows 7 and Windows 2008 all use a completely different .MAN file to Windows 2003 and XP.

You are still able to assign one profile path in the user's properties though to accommodate for both profiles. Do the following to achieve this:

- Create a .MAN file from either a Windows XP or Windows 2003 machine
- Create another .MAN from a Windows Vista, Windows 7 or Windows 2008 machine.
- If your profile is to be stored in the location **%LOGONSERVER%\Netlogon\Mandatory**
- Create two folders in this location Profile and Profile.v2
- Copy the .MAN for Windows XP or 2003 to the Profile folder
- Copy the .MAN for Windows Vista, 7 or 2008 to the Profile.v2 folder.
- Within the user profile path use the path **%LOGONSERVER%\Netlogon\Mandatory**, Windows Operating System will be able to automatically pickup which profile to load in.

## Microsoft Office Applications

Because Microsoft Office applications share parts of the user's registry and file system within the user's profile, AppSense recommends that Microsoft Office Applications are grouped together within an Application Group within the Environment Manager Personalization configuration.

This then allows all the nominated executables within office to access the one copy of the virtual registry and file system in the user's profile, allowing the different executables to share such things as dictionary paths and user information.

Each different version of Microsoft Office should be grouped in their own Application Group (i.e. Microsoft Office 2003 should be grouped independently of Microsoft Office 2007).

Please be aware that when you group applications together that even though one executable within the group is run, the entire settings for all applications within the group will be delivered to the client.

Likewise if rollback is used for an Application Group then all settings for all applications within the group will be rolled back.

### **Microsoft Groove and OneNote**

It has been found that Microsoft Groove and OneNote are processes which run slightly differently to the normal Microsoft Office application set.

These processes are constantly running during the user's sessions. They are initiated at logon, and closed at log off. Because of the way they run, normal application personalization will not work correctly for these executables.

Therefore AppSense suggests that these processes are ignored from the Personalization process altogether if they are not required. Or alternatively if they are required, just add in the registry keys required for each application within the desktop settings for Personalization Server, so that these settings are applied at logon and captured at log off.

The registry for each application to use in desktop settings is:

Groove

- HKCU\Software\Microsoft\Office\12.0\Groove

OneNote

- HKCU\Software\Microsoft\Office\12.0\OneNote

### **Microsoft Office Signatures**

Microsoft Office signatures can be captured and moved into the Personalization Server successfully, but, in the case where a user's profile is being migrated into the Personalization Server, then some manual intervention is required on the user's behalf.

Because migration mode works by using the method "Virtualize on Read", it does require the user to manually access the signatures within the Microsoft Office application so they are forced to be read by the application. At this point the Personalization server will then be able to capture the signatures successfully because the application has been forced to read the signature files.

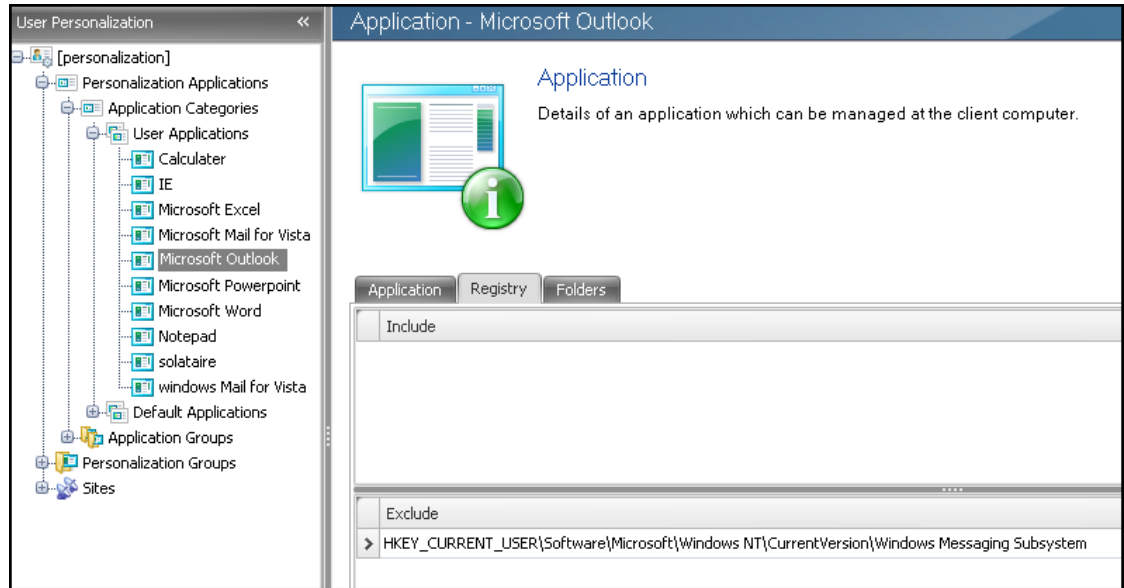
### **Microsoft Outlook**

Microsoft Outlook requires a slight configuration change to allow for the Outlook profile to work correctly in retaining the Windows Messaging Subsystem settings.



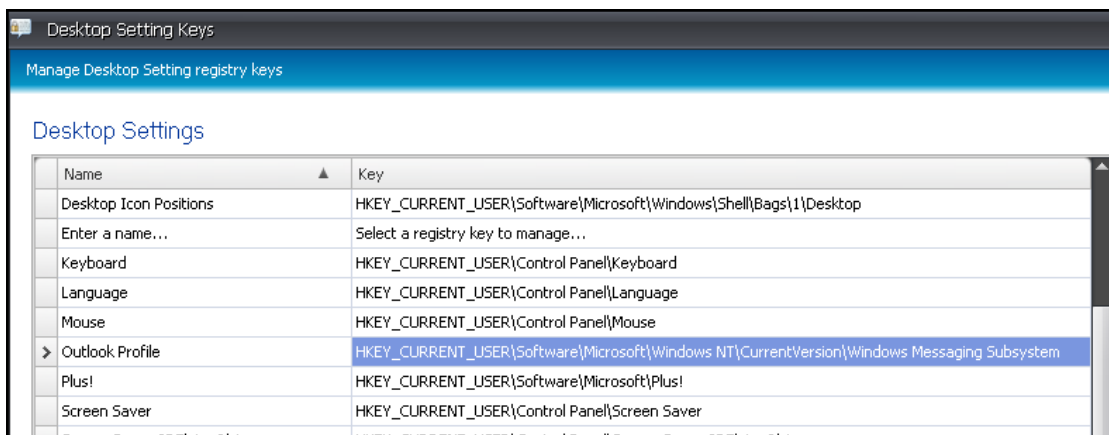
Because these settings are not only used by the **OUTLOOK.EXE** but also by the process **REG32DLL.EXE** for the Mail component within Control Panel we need to force **OUTLOOK.EXE** to use the physical registry and not the virtual registry provided by Environment Manager Personalization Server.

Firstly we need to exclude the Windows Messaging Subsystem key from the Outlook.exe application defined within the Personalization Server console.



Then Environment Manager Personalization Server needs to be configured to keep this setting managed but within the physical registry. This is done by adding this key to the Desktop Settings.





This now allows both the OUTLOOK.EXE and REG32DLL.EXE processes to access this part of the registry allowing for Microsoft Outlook work correctly with Environment Manager Personalization.

### Microsoft Outlook PST and OST Files

Because of the nature of these particular files which are used by Microsoft Outlook for user data, the AppSense Personalization server will ignore these file types and not capture them within its virtualization of the profile.

Therefore as part of best practice we recommend that PST or even OST files are made available, where possibly via network drives.

This obviously reduces the amount of the within the profile, and allows Microsoft Outlook to access these files correctly, whilst still being able to be personalized by Environment Manager Personalization Server.

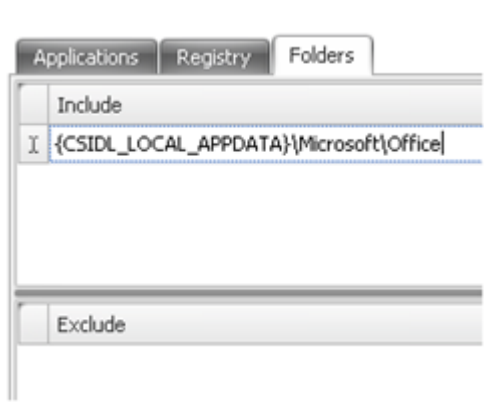
### Microsoft Office 2007 Quick Access Toolbar

The Microsoft Office 2007 Quick Access toolbars are captured by default within the Environment Manager Personalization Server. This is because Office 2007 keeps the values for this toolbar within a non-roaming location within the profile.

In order to include the Quick Access Toolbar in the user’s personalization profile, the location of the .QAT files needs to be included.

To achieve this do the following:

- Select the Application Group you have created for Microsoft Office 2007, or alternatively the Microsoft Office 2007 application if you are not using application groups.
- Select the Folders tab for the Application or Group and enter in the value **{CSIDL\_LOCAL\_APPDATA}\Microsoft\Office**



### Applications that use INI files

Some applications that are used within a customer's environment require the use of .INI files or files of these types to keep their 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.

If however, the .INI file is not kept within the user's profile, but in another location (e.g. C:\Windows etc.) Then we do not want EMP to capture information from this location, due to the nature and the amount of files in that location.

At this point, this is where we would 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 Log off or Process Stop trigger.

### Using Offline Personalization

As explained earlier in this guide, Offline mode within Environment Manager Personalization allows the Personalization Virtual Cache (PVC) to be permanently available to the user, this allows the user who is using a mobile device to work offline without their Personalization settings being lost and also allows those offline settings to be synchronized when back online.

These mobile users though may login to a VDI, Workstation or Terminal Server. With their Personalization configuration though being in offline mode, this means that when they log off from the VDI, Workstation or Terminal Server, their PVC will still exist. This of course is against all best practice as we want to remove the user's profile once the user has logged off from the device.

Therefore to accommodate for this, AppSense recommends deleting the contents of the **%SYSTEMDRIVE%\AppSenseVirtual** folder during shutdown of the device. This will ensure that disk space is not taken up and that the user's profile is never kept on a device.

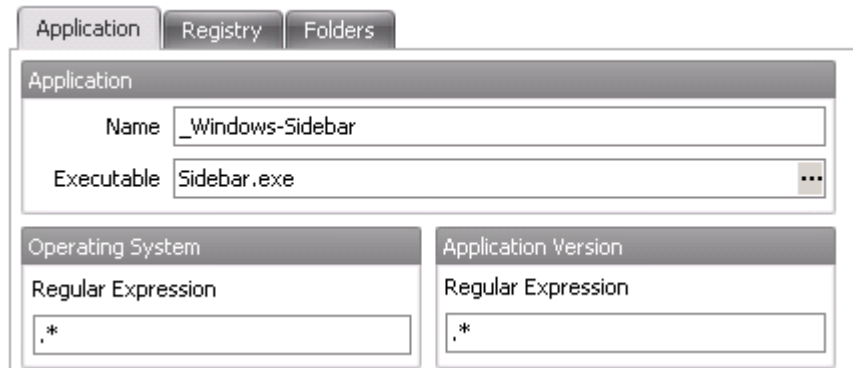
If you are using a non-persistent pooled VDI solution, this step would not be required.

### Microsoft Sidebar (Vista)

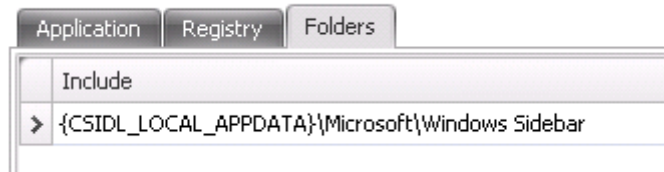
In some environments, you may wish to keep the settings of the Microsoft Sidebar, which is included with Microsoft Vista operating system.

To achieve this please perform the following steps within the Environment Manager Personalization Server.

1. Add the Sidebar.exe application to the list of known applications within Personalization Server.



2. Within the folders tab of the Sidebar.exe application add in the following inclusion



These steps will now ensure that when you add the Sidebar application to your personalization group that it will be captured correctly for the user.

### Printer Settings

If printer settings are required to be kept by the user, then the following keys need to be added to the Desktop 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

## Desktop Settings for Personalization

The below registry keys are known areas which is used by the explorer shell to keep certain settings for the users. Please add these locations where required to the desktop settings within Personalization Server.

- Explorer Settings

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Shell (Windows XP and 2003 Server)

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\ShellNoRoam (Windows XP and 2003 Server)

HKEY\_CURRENT\_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell (Microsoft Vista and 2008 Server)

- Text Auto Complete

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete

- Autoplay Settings for Removable Drivers

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers

- Recycle Bin Settings

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket

- Path Settings for Explorer

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState

- CD Burning

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning

- Explorer Dialog Open options

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDOpen

- Explorer Dialog Save options

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDSave

- Icon Picture Settings

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID

- Control Panel

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel

- Context Menu for NEW option

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable

- Extraction Settings for Windows ZIP  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ExtractionWizard
- File Extension Settings  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
- Recent Network Drives  
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
- Menu Order within Favourites in Explorer Window  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder
- Modules Settings  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Modules
- Shortcut Handlers  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\NewShortcutHand  
lers
- Vista Printing Lab  
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\PhotoPrintingWizard
- Recent Documents (requires Folder Redirection from Policy as well)  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
- Recent Run  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- IE and Windows Search options  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SearchPlatform
- User Session Information  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo
- Start Page for Internet Explorer  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage