Best Practices for Personalization

This section outlines the key points for consideration when implementing Environment Manager Personalization (EMP), and to ensure the experience of the benefits of the AppSense User Environment Management (UEM) solution.

The following sections assume that there are already existing user profiles in use, in the form of roaming profiles, and that all applications within the environment are known.

Supported Operating Systems

For all supported operating systems refer to System Requirements.

Personalization Architecture Design Best Practice

Standard Architecture

Environment Manager Personalization has a standard architecture of:

- Personalization Database

This is where all the user profiles managed by Environment Manager Personalization 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 Personalization Database. It is responsible for delivering the Personalization configuration to the 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.

Designing and Implementing Environment Manager Personalization

The following points should be adhered to as AppSense best practice when designing and implementing Environment Manager 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.
- Currently, one Personalization Server (Quad Core and 4GB of physical memory) supports 7000 concurrent users. It is recommended to have multiple Personalization Servers for High Availability. These servers should always be listed when Personalization is enabled within the Environment Manager Policy configuration.
- When required, Personalization Servers will support Network Load Balancing being placed in front of the servers. Refer to the *AppSense Network Load Balancing Guide* for more information.
- When you have multiple sites or data centers, for example, for disaster recovery, it is recommended that Personalization Servers and Databases are installed at these sites and local clients pointed to their local Personalization Server and Databases.
- When multiple sites are used, it is recommended to use Microsoft SQL replication. Refer to Personalization Database Replication for information on configuring Microsoft SQL replication for Environment Manager Personalization.

Enabling the Personalization Server

How to Enable Personalization

Personalization is enabled from within the Policy Configuration side of the console.

- Click **Enable User Personalization** on the **Home** ribbon page > **General Properties** group.
  The **Select Personalization Server** dialog box displays.

You can add a single or multiple servers to the **Select Personalization Server** dialog box. It is recommended to add multiple servers (where applicable) for failover purposes.

Deploy the Policy Configuration that contains this list of Personalization Servers out to the endpoints. This results in the configuration.aemp file being sent to the managed computer.

The first time a user logs on to the managed endpoint the User Personalization mechanism attempts to connect to the first server listed, if that attempt fails, connection is attempted on the next server in the list and so on until a connection has been successful. The user then receives their User Personalization configuration which is pulled down from the database via the Personalization Server.

If all attempts fail, then the User Personalization configuration is not downloaded and no Personalization takes place.

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

Do the following:

1. Within Policy Configuration, click **Auditing** on the **Home** ribbon page > **Common** group.
   The **Auditing** dialog box is displayed.
2. Select the **9661 - Timeout Communicating with Personalization Server** event.

Personalization Group Usage

Managing Personalization settings

Personalization Groups allow for different Personalization settings to be applied to users based on different membership rules.

For example, if a user has access to a series of Terminal Servers, they receive the same Personalization settings independent of which Terminal Server they are logging on to. However, for a specific server silo that contains a critical application, that does not require Personalization settings to be used, you can create a separate Personalization Group for the specific server and disable the Personalization settings.

Ordering Personalization Groups

A user may be a member of more than one Personalization Group. The user is assigned to the first Personalization Group in the list where the membership rule is valid.

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

To order a list of Personalization Groups:

1. Select the Personalization Group to order.
2. Click **Move Up** and **Move Down** on the **Personalization** ribbon page > **Arrange** group.

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

Excluding Users from Personalization

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

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

In order to exclude a specific user or computer from User Personalization you can create a new Personalization Group. Once created, disable each option on the **Settings** tab for the Personalization Group.

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

When a user is added to a specific Personalization Group, their Personalization settings are only relevant for that group. When you need to move a user and their settings to another Personalization Group you can do this via Personalization Analysis.

To move users between Personalization Groups:

1. Navigate to the Personalization Group in the navigation tree which the user you want to move belongs.
2. Click **Personalization Analysis** on the **Tools** ribbon page > **Management** group.
   The **Personalization Analysis** dialog box displays.
3. Leave the default settings of <All Users> in the **By user** field. Select **Display**.
   The report for all users displays.
4. Right-click the user you wish to move and choose **Move the settings for <user> to another group....** This prompts the administrator to choose another available group to move the chosen user's Personalization settings to.
5. Select the group to move the user to.
6. It is recommended to select the **Include Discovered Applications** option. Selecting this option allows you to move any discovered applications (rather than Whitelist applications) to the new group too.
7. Click **Continue** to proceed with the move.
8. If the user and the associated data is successfully moved a confirmation message displays, click **OK**.
   The graph is refreshed and the user bar disappears.

Personalization Group Settings

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

- Offline Options
- Processes
- Desktop & Certificates
- Migration Options

Offline Options

Allow Offline Mode

Disabled by default.

This option 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 recommended that this option only be enabled for managed endpoints that are mobile, such as laptop devices, otherwise valuable disk space may be unnecessarily utilized on both static desktops and servers.

Offline Resiliency

Enabled by default.

It is recommended this setting remains enabled. **Offline Resiliency** ensures that if a user is online, but for some reason, such as a 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** and **Whitelists & Blacklists**.

Discover All Processes

Disabled 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, a blacklist or deleted.

It is recommended that **Discover All Processes** is enabled so that applications being used by users can be identified. Personalization Analysis reports can be run to show applications discovered by the **Discover All Processes** option.

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

Discovered (Unmanaged) applications are shown as grey bars in the Personalization Analysis graphs.

Manage All Processes

Disabled 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 a message to warn of the consequences.

Discovered (Managed) applications are shown as blue bars in the Personalization Analysis graphs.

Whitelists & Blacklists

It is recommended that whitelists be utilized along with the **Discover All Processes** option. 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, and so on, 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, 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. Assign this 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

Enabled by default.

Desktop settings are configured globally in the **Desktop Settings Keys** dialog box available on the **Tools** ribbon page > **Management** group.

However, the application of these settings can 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.

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

Manage Certificates

Enabled by default.

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

Enabling this option triggers 'profile state emulation' in which the operating system is given false data indicating the user is logged in with a roaming profile. This allows certificates to be added to the certificate store. At log off, the profile is set back to a mandatory profile and the next time the user logs on, the certificates are restored.

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

Migration Options

Migrate Existing Profiles

Disabled 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.

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 Application Usage** and/or **Whitelist Application Usage** reports in Personalization Analysis.

Personalization Sites Configuration

Sites

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

It is recommended that the primary site be installed at your Head Quarters (or IT data center) 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 (SCU).

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 are provided with their User Personalization configuration from the first Personalization Server which can be contacted from the list of servers in the configuration.aemp file. Subsequent personalization synchronizations 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 according to the Personalization Database Replication section.

When configured, replication occurs by default once per day.

It is recommended that the **Synchronize Site Databases** option, available on the **Tools** ribbon page > **Replication** group, be utilized if replication between databases is required immediately.

Personalization Implementation

Installation

Ensure you have installed and deployed the following components:

- Installed AppSense Management Center.
- Installed and configured Environment Manager Personalization Database.
- Installed and configured Environment Manager Personalization Server.
- Installed the AppSense Environment Manager Agent to clients.
- Configured and deployed an AppSense Environment Manager Policy configuration with Personalization enabled.
- Considered the environment you are installing into to evaluate the best configuration for High Availability, such as:
  - Number and location of Personalization Servers required?
  - What are your requirements 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.
  - The bandwidth and other traffic going to the sites. (On average, desktop settings are 1MB at Logon/Logoff, application settings are, on average, 200KB if synchronization is required).

Configuration

Once you have installed and deployed the above components (within the **Installation** section) for Environment Manager Personalization you will need to consider the following steps for configuration:

- Do you want to migrate existing user profiles or start with fresh new profiles?

- Identify not only the applications you want to manage with the Personalization Server but also if any applications are dependent on each other and Application Grouping is required.
- When applications are to be delivered by a virtualization method such as Microsoft App-V or Citrix Streaming Client, refer to Streamed Applications for configuring the application package to work with Environment Manager Personalization.
- Set up the Personalization Groups with regards to how you want 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.
- When performing a migration of existing profiles, you will need to allow a period of time that will allow all user'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.
- When multiple sites are used, configure the SQL replication as per the Personalization Database Replication section.
- For more intelligent failover of Personalization Servers, investigate the use of Network Load Balancing. Refer to the *AppSense Network Load Balancing Guide* for more information.
- Ensure any support desk staff that will be performing Personalization roll backs have sufficient rights to the Personalization Console, at 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 create and use a Mandatory profile as this profile is very light weight and contributes to faster logon times for users. This profile is good for environments where all users are accessing devices which are permanently online.

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

When required, a middle ground solution can be found where you create the .man file for the Mandatory profile, but place it within the location of %SYSTEMDRIVE%\Default Users.

This allows two benefits in that you 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. Note that this will require some time to copy to each managed device.

Mandatory Profiles

Creating a Mandatory profile is a straight forward task, however, 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 Organizational Unit (OU) with no Group Policies applied whatsoever.
- Log the Template account on to 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 .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). 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 file, while Windows Vista, Windows 7 and Windows 2008 all use a completely different .man file to Windows XP and Windows 2003.

You can still assign one profile path in the user's properties to accommodate for both profiles.

Do the following to achieve this:

1. Create a .man file from either a Windows XP or Windows 2003 machine.
2. Create another .man file from a Windows Vista, Windows 7 or Windows 2008 machine.
3. 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 file for Windows XP or Windows 2003 to the **Profile** folder.
   - Copy the .man file for Windows Vista, Windows 7 or Windows 2008 to the **Profile.v2** folder.
   - Within the user profile path use the path %LOGONSERVER%\NetLogon\Mandatory. The Windows operating system will automatically pick up which profile to load in.

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, and so on, then you do 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.

Microsoft Applications

Group Microsoft Office Applications

Because Microsoft Office applications share parts of the user's registry and file system within the user's profile, it is recommended 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 Microsoft 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, for example, Microsoft Office 2008 should be grouped independently of Microsoft Office 2007.

Be aware that when you group applications together that, even though one executable within the group is run, the entire settings for all applications 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

Microsoft Groove and Microsoft OneNote are processes which run slightly differently to the normal Microsoft application set.

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

It is recommended that these processes are ignored from the Personalization process altogether if they are not required. Alternatively, if they are required, add in the registry keys required for each application within the desktop settings for the Personalization Server, so that these settings are applied at log on and captured at log off.

The registry key 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.

These settings are not only used by outlook.exe but also by the rundll32.exe for the Mail component within Control Panel. Therefore, you need to force outlook.exe to use the physical registry and not the virtual registry provided by Environment Manager Personalization Server.

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

- Select the **Personalization Applications** node in the left navigation pane and exclude the Windows Messaging Subsystem key, for example, HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem.

  

  This key can alternatively be added as an exclusion for the outlook.exe process under the **Personalized Applications** section.

The 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**.

- Select **Desktop Settings** on the **Tools** ribbon page > **Management** group and add the same key, for example, HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem.

These steps allow both the outlook.exe and rundll32.exe processes to access this part of the registry allowing Microsoft Outlook to work correctly with Environment Manager Personalization.

Microsoft Outlook PST and OST Files

By default, the Personalization Server ignores the Microsoft Outlook PST and OST files that are used by Microsoft Outlook for user data, and does not capture them within its virtualization of the profile. This is because of the nature of the PST and OST files.

It is recommended that the PST or even OST files are made available, where possible, via network drives, or in the case of mobile devices such as notebooks or laptops, stored outside of the profile on a local drive.

This reduces the amount of data stored within the profile and allows Microsoft Outlook to access these files correctly, and to be personalized by the 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 Microsoft Office 2007 keeps the values for this toolbar within a non-roaming location within the profile.

To include the Quick Access Toolbar in the user's Personalization profile, the location of the .qat files need to be included.

1. 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.
2. Select the **Folders** tab for the Application Group or application and include the value {CSIDL_LOCAL_APPDATA}\Microsoft\Office.

Microsoft Sidebar (Vista)

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

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

1. Add the sidebar.exe application to the list of known applications within the Personalization Server.
2. Within the **Folders** tab of the sidebar.exe application add in the inclusion {CSIDL_LOCAL_APPDATA} \Microsoft\Windows Sidebar.

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

Printer Settings for Personalization

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

Desktop Settings

The registry keys below are known areas which are used by the explorer shell to keep certain settings for the users. Add these locations, where required, to the **Desktop Settings** within the Personalization Server.

- Explorer Settings
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell (Windows XP and Windows Server 2003)
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam (Windows XP and Windows Server 2003)
  - HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell (Microsoft Vista and Windows Server 2008)
- 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\Explorere\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\FilesExts
- 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 Favorites 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\NewShortcutHandlers
- Vista Printing Lab
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\PhotoPrintingWizard
- Recent Documents (also requires Folder Redirection from Environment Manager Policy)
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
- Recent Run
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- Internet Explorer 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