



VMware View™ Persona Management

DEPLOYMENT GUIDE

Table of Contents

Introduction to View Persona Management	3
User Profiles	3
Advantages of View Persona Management	3
System Requirements and Recommended Hardware	5
Installation and Configuration	6
1. Setting Up the Remote Repository for User Profiles	6
2. Installing View Agent with the View Persona Management Setup Option	6
3. Adding the Persona Management Administrative Template	7
4. Configuring Group Policy Settings for Persona Management	8
5. Creating and Deploying Desktop Pools from the Master Virtual Machines	25
Special Situations for Deploying View Persona Management	26
Deployments with Both View Persona Management and Windows Roaming Profiles	26
Scanning User Profiles with Antivirus Checkers	26
Backing up User Profiles	27
Enhancing ThinApp Application Startup Time	27
Use Persistent Disks If Users Have Large User Profile Files	27
Migrating Folder Redirection to Persona Management	27
Use of View 5 Persona Management with Other Profile Management Tools	27
References for Further Information	28
About the Author and Contributors	28

Introduction to View Persona Management

With VMware View™ 5, VMware introduces View Persona Management™. View Persona Management preserves user profiles and dynamically synchronizes them with a remote profile repository. View Persona Management does not require the configuration of Windows roaming profiles, and you can bypass Windows Active Directory in the management of View user profiles. If you already use roaming profiles, Persona Management enhances their functionality.

Persona Management downloads only the files that Windows requires at login, such as user registry files. When the user or application opens other files from the desktop profile folder, these files are copied from the stored user persona to the View desktop. This algorithm provides performance beyond that achieved with Windows roaming profiles.

In addition, View copies recent user profile changes to the desktop profile up to the remote repository every few minutes. The default is every ten minutes, and this time period is configurable.

For information on the benefits of View Persona Management and how it works, refer to *Providing User Personas in View* in the chapter *Configuring User Profiles with View Persona Management* in the [VMware View Administration guide](#).

User Profiles

User profiles hold personal data and settings that users can access from wherever they open their desktops. A user profile contains:

- User data, such as My Documents files
- User desktop settings, such as for desktop appearance
- Application-specific data and settings, such as customized application toolbars, or Windows registry entries generated by applications
- Other user-generated information

Advantages of View Persona Management

Before the advent of View Persona Management, View administrators handled user profiles by:

- Implementing Windows roaming profiles
- Using third-party virtual profile managers
- Keeping the user profile local by using a dedicated pool of persistent desktops, or persistent disks attached to nonpersistent desktops

Traditional roaming profiles have serious performance issues when a large number of users log in or log out simultaneously. In addition, managing user profiles through Windows Active Directory may have repercussions for more users than intended.

Choosing to implement a dedicated pool of persistent desktops, or persistent attached disks, is not optimal because of the storage space required for individual desktops or disks.

VMware includes in View 5 an integrated virtual profile management system that is easy to set up, minimizes login and logout time, and allows for flexibility in choosing desktop pool types.

View Persona Management minimizes the amount of time necessary for login and logout by:

- Downloading at login time only the files that Windows requires for login, such as user registry files.
- Downloading other user profile data only as needed, when the user or application opens a profile folder on the View desktop. The profile folders appear to contain up-to-date files, but the data is not downloaded until it is accessed.
- Periodically uploading to the remote repository any changes made to the user profile. The default time between automatic periodic uploads is ten minutes, and this time can be configured.
- Uploading at logout only the user profile changes since the last periodic upload. Because of the frequent automatic upload of changed user data during the user session, this final upload does not take a long time.

By minimizing the amount of data uploaded or downloaded at any one time, Persona Management provides a performance improvement over Windows roaming profiles. A roaming profile system managed by Windows copies the entire user profile to the local desktop at login and copies all user profile changes up to the remote repository at logout.

View Persona Management is an alternative to Windows roaming profiles and allows you to manage user profiles without relying on Active Directory for configuration. Instead, you configure and manage user profiles entirely within the View environment. Any changes you make to test View Persona Management have an effect only on View desktops and do not have a global effect on other desktops, such as physical desktops. You can easily reconfigure View to refine your implementation.

System Requirements and Recommended Hardware

Persona Management has no system requirements beyond those for VMware View itself. However, VMware recommends particular configurations for servers, network speed, and file server memory to provide you with the best performance for Persona Management of user profiles.

VMware recommends the following infrastructure for a View implementation with Persona Management enabled:

- **Servers:** One or more file servers, each one storing profiles for approximately 1000 users. If a virtual machine is used as a file server, the volume storing the profiles works optimally if striped across four virtual disks, each with its own SCSI controller. A file server on a physical system works best in a similar configuration. Consult your SCSI controller documentation regarding the supported maximum number of concurrent commands.
- **Network speed:** At least 1Gbps between the desktops and the file servers.
- **RAM on each file server:** 8GB

Your own results may vary, depending upon:

- Your storage capability
- Your network speed and latency
- Number of users
- Frequency that users access data in the user profiles
- Storage
- IOPS

Installation and Configuration

Persona Management is an optional feature, and you must purchase View Premier™ to implement View Persona Management.

After you install your vSphere™ virtual infrastructure and your View virtual desktop infrastructure, you are ready to install and configure Persona Management. Following are the major steps for a Persona Management implementation. You can reverse some of the steps, such as configuring Persona Management group policy settings in Active Directory and deploying desktop pools.

1. Set up the remote repository for user profiles.
2. Install View Agent with the View Persona Management setup option.
3. Add the Persona Management Administrative Template.
4. Configure group policy settings for Persona Management.
5. Create and deploy desktop pools from the master virtual machines.

1. Setting Up the Remote Repository for User Profiles

The remote repository for View Persona Management user profiles can be either:

- Your current Windows roaming profile repository if you already configured roaming profiles
- A newly configured network share

To set up the repository, refer to *Configure a User Profile Repository* in the *Configuring User Profiles with View Persona Management* chapter of the [VMware View Administration guide](#).

Interaction of View Persona Management with Microsoft Roaming Profiles

Persona Management can work with or without your current Windows roaming profiles setup. You can use the View Persona Management algorithms with your legacy roaming profiles repository. It makes no difference whether you create a new user profile repository for your View implementation or use a previous roaming profile repository. No conversion of the user profile data is necessary; the format is identical.

For a deployment combining View Persona Management for View desktops and Windows roaming profiles for standard desktops, see [Deployments with Both View Persona Management and Windows Roaming Profiles](#) in this document.

2. Installing View Agent with the View Persona Management Setup Option

To implement View Persona Management on your desktop pools, you must install View Agent and select the Persona Management setup option for each parent or template virtual machine used to create a desktop pool.

View Persona Management is currently supported only on virtual machines. In this release of View, VMware does not support Persona Management on:

- Physical computers or desktops
- Microsoft Terminal Servers
- View desktops that you will run in Local Mode

In addition, View Persona Management is not supported on virtual desktops from another vendor.

Note: If you implement View Persona Management on a Windows XP desktop, you must install and run the Microsoft User Profile Hive Cleanup (UPHClean) service in the XP operating system.

For instructions on installing the View Agent on virtual machines, selecting the View Persona Management setup option, and installing the UPHClean service for Windows XP, see *Install View Agent with the View Persona Management Option* in the *Configuring User Profiles with View Persona Management* chapter in the [VMware View Administration guide](#).

3. Adding the Persona Management Administrative Template

You must add the Persona Management administrative template to your View deployment to be able to configure the user profile settings. You can add the administrative template to one of the following:

- Active Directory server
- Local Computer Policy configuration on each parent or template machine for a desktop pool

If you want your entire View deployment to use View Persona Management, install the Persona Management template on the Active Directory server.

If you want to implement Persona Management for only one desktop pool, you can either:

- Add the administrative template to the parent or template virtual machine that you will use to create the desktop pool
- Add the administrative template to the Active Directory server and apply the group policy settings to the organizational unit (OU) that contains the desktops in the pool

Adding the Administrative Template to the Active Directory Server

Add the Persona Management administrative template to the Active Directory server if you want to implement Persona Management either:

- For your entire View deployment
- For an organizational unit (OU) that contains a specific desktop pool

When you install a View Connection Server, a copy of the Persona Management administrative template is automatically installed on the View Connection Server. (For information about creating a View Connection Server, see the *Installing View Connection Server* chapter in the [VMware View Installation guide](#).) You copy this administrative template from the View Connection Server to the Active Directory server.

The location of the administrative template for Persona Management on the View Connection Server is:

```
<install_directory>\VMware\VMwareView\Server\extras\GroupPolicyFiles\ViewPM.adm
```

To copy the Persona Management administrative template file from the View Connection Server to the Active Directory server and add it to a Group Policy Object (GPO) on your Active Directory server, see *Add the Persona Management ADM Template to Active Directory* in the *Configuring User Profiles with View Persona Management* chapter in the [VMware View Administration guide](#).

Adding the Administrative Template to a Parent or Template Virtual Machine for a Desktop Pool

Add the Persona Management administrative template to one parent or template virtual machine if you want to implement Persona Management for the single desktop pool you will create from that virtual machine.

When you install the View Agent on a View virtual machine desktop, the administrative template is copied to that virtual machine in:

`C:\Program Files\VMware\VMware View\Agent\bin\ViewPM.adm`

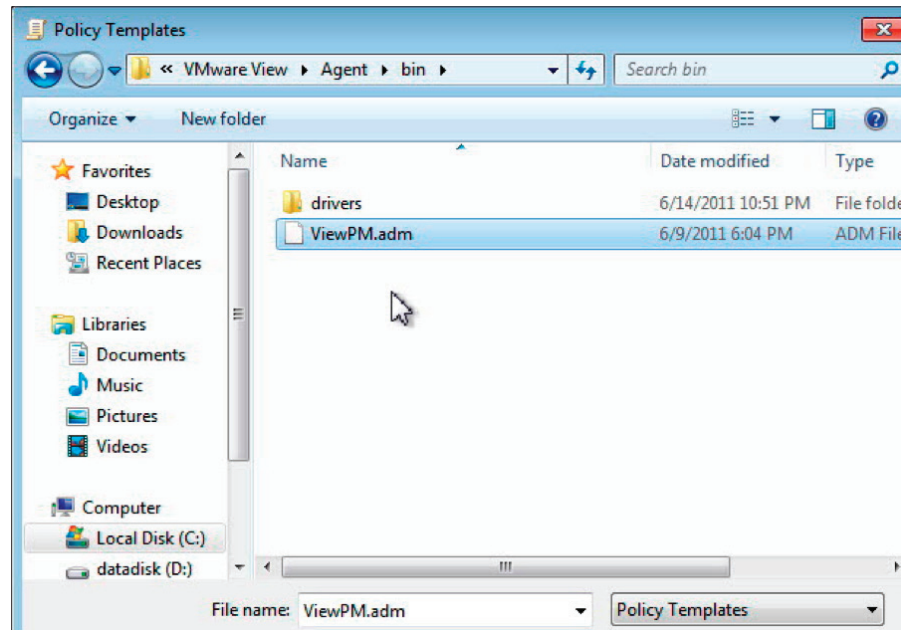


Figure 1: Location of Persona Management Administrative Template After View Agent Installation

To add this administrative template to the Local Computer Policy environment of the virtual machine desktop, see *Add the Persona Management ADM Template to a Single System* in the *Configuring User Profiles with View Persona Management* chapter in the [VMware View Administration guide](#).

4. Configuring Group Policy Settings for Persona Management

After you add the Persona Management administrative template to the virtual machine desktop or to Active Directory, you configure the settings in the group policy editor.

Configuring Group Policies on a Virtual Machine Desktop

If you added the Persona Management administrative template to the virtual machine desktop that will be the parent or template for a desktop pool, use `gpedit.msc` to edit settings in the Local Group Policy Editor console. Following are detailed steps:

1. If you are not already in the Local Computer Policy window, select **Start > Run** and type `gpedit.msc`.
The Local Group Policy Editor window opens. >
2. Under **Local Computer Policy**, navigate to **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > VMware View Agent Configuration > Persona Management**.

- Expand **Persona Management** and select the **Roaming & Synchronization** group policy settings folder.
The configurable policies appear in the right pane.

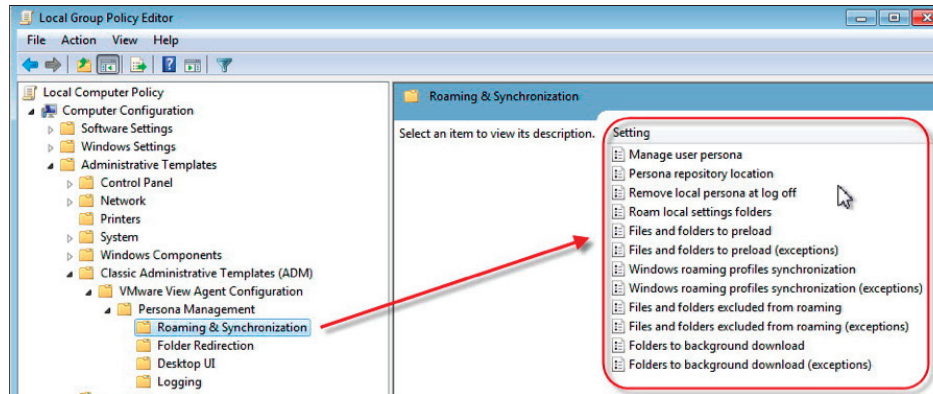


Figure 2: Local Group Policy Editor > Roaming & Synchronization

- Select the **Manage user persona** group policy setting, click **Edit policy setting**, and click **Enabled**. This activates View Persona Management to manage the user profiles.

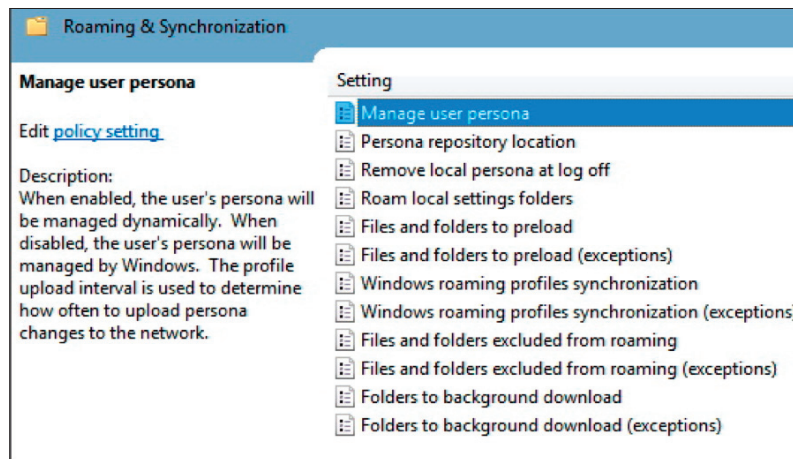


Figure 3: Roaming & Synchronization Settings

- Select each group policy setting and configure for your View deployment.
- After you complete the Roaming & Synchronization settings, proceed to the Folder Redirection, Desktop UI, and Logging folders to fully configure Persona Management. Refer to the following tables under [Group Policy Settings Descriptions](#) for details on the settings.

Configuring Group Policies on the Active Directory Server

If you copied the Persona Management administrative template to the Active Directory server, configure the settings with Group Policy Management in Administrative Tools. Following are detailed instructions.

1. Navigate to **Start > Administrative Tools > Group Policy Management**.

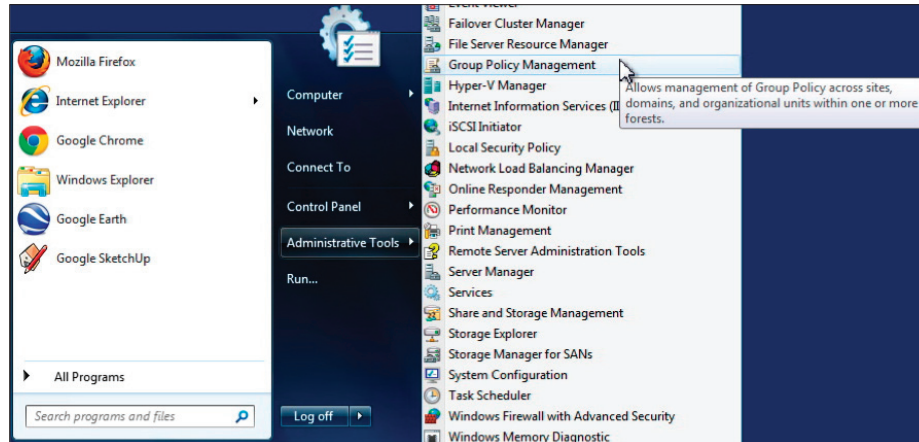


Figure 4: Administrative Tools > Group Policy Management

2. In the left pane, navigate to **Group Policy Management > <your_forest> > Domains > <your_cloud> > View Environments > View Desktops**.
3. Right-click on **View Desktops** and select **Edit**.

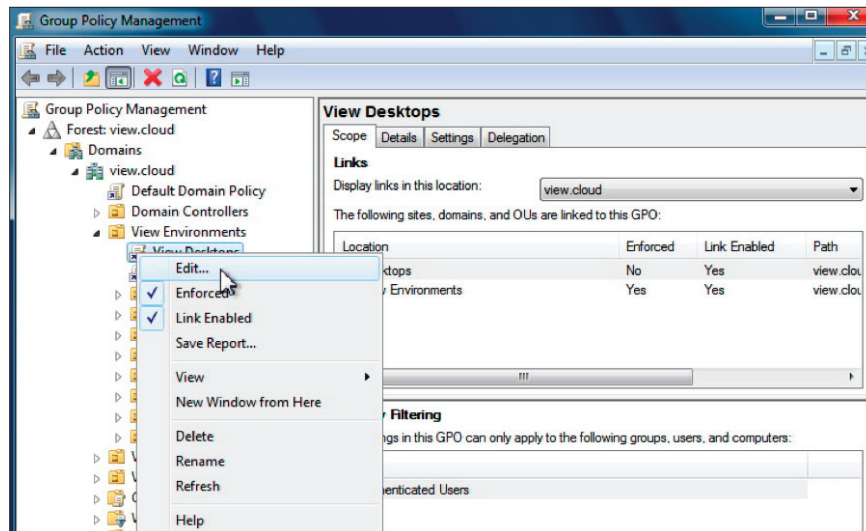


Figure 5: Group Policy Management > Edit

4. The Group Policy Management Editor opens with View Desktops in detail.
5. Navigate to **Computer Configuration > Policies > Administrative Templates... > Classic Administrative Templates (ADM) > VMware View Agent Configuration > Persona Management**
6. Configure settings in the same way as on an individual desktop. Refer to the following tables under [Group Policy Settings Descriptions](#) for details on the settings.

Group Policy Settings Descriptions

This section discusses for each Persona Management group policy setting:

- The brief definition
- The default value
- The possible values
- Use cases for when you might want to change the default

For full definitions of these group policy settings, see the *Configuring User Profiles with View Persona Management* chapter in the [VMware View Administration guide](#).

Note: With View Persona Management, you can manage user profiles set up and stored in the Windows roaming profile repository. Or you can manage user profiles set up and stored in a View user profile repository.

Domain-level GPOs always override local group policy.

You can configure GPOs at the domain level (applied on a per-organizational unit basis) or at the machine level (local group policy). The configuration at the lowest-level organizational unit (OU) takes precedence over a setting in a higher-level parent OU. The default domain policy is the last to take effect for domain-level GPOs. If nothing is set at the domain level, then the local group policy takes effect. View looks for the first instance of a particular setting at the lowest-level OU and continues up through the hierarchy until it finds a setting. Once found, View Persona Management uses that value and proceeds no further.

Roaming and Synchronization Group Policy Settings

MANAGE USER PERSONA	
Brief definition	Manage user profiles with View Persona Management, instead of with Windows roaming profiles.
Default value	Disabled (user profiles are managed by Windows, not by View Persona Management).
Possible values	Enabled, disabled
Use cases and details	If you want to use View Persona Management, you must enable this setting.

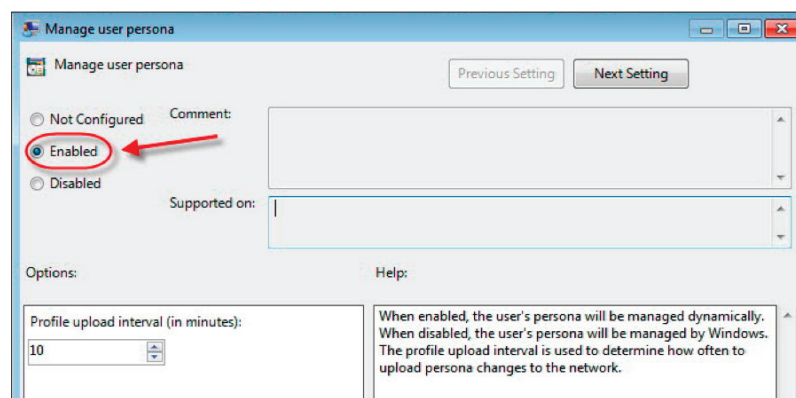


Figure 6: Manage User Persona

PROFILE UPLOAD INTERVAL	
Brief definition	Frequency of uploading to the remote repository any changes to the user profile.
Default value	10 minutes
Possible values	1-9999 (in minutes)
Use cases and details	Only available if Manage user persona is enabled.

PERSONA REPOSITORY LOCATION	
Brief definition	Toggle for enabling a Persona Management repository that is different from the Windows roaming profile location. If you wish to bypass the Windows roaming profile location, you must set up a View user profile repository, enable Persona repository location , and specify its path in Share path .
Default value	Disabled (View Persona Management uses the Windows roaming profile path).
Possible values	Enabled, disabled
Use cases and details	<p>Enable if you wish to avoid using the Windows roaming profile path. Disable if you wish to automatically use the Windows roaming profile path already set for the user object in Active Directory or with a Windows GPO. *</p> <p>This repository must be a network file share that supports certain features of NTFS, such as alternate data streams and extended attributes to ensure consistency. For details on setting up the View Persona Management repository, see <i>Configure a User Profile Repository</i> in the <i>Configuring User Profiles with View Persona Management</i> chapter of the VMware View Administration guide.</p>

* Some Windows GPOs can override the Active Directory profile path:

- **Set path for TS roaming profiles** under **Administrative Templates > Windows Components > Terminal Services**, which only applies to RDP connections to XP desktops
- **Set roaming profile path** under **Administrative Templates > System > User Profiles**, which only applies to Vista and Windows 7

SHARE PATH	
Brief definition	Location of the user profile repository. You must enable Persona repository location, and then specify the path in Share path .
Default value	Blank (uses Windows roaming profile path).
Possible values	UNC path to a network share that is available to View Persona Management-enabled desktops.
Use cases and details	Only available if Persona repository location is enabled. If you wish to bypass Windows Active Directory management of roaming profiles, specify a network share location in Share path . If blank, View uses the Windows roaming profile path.

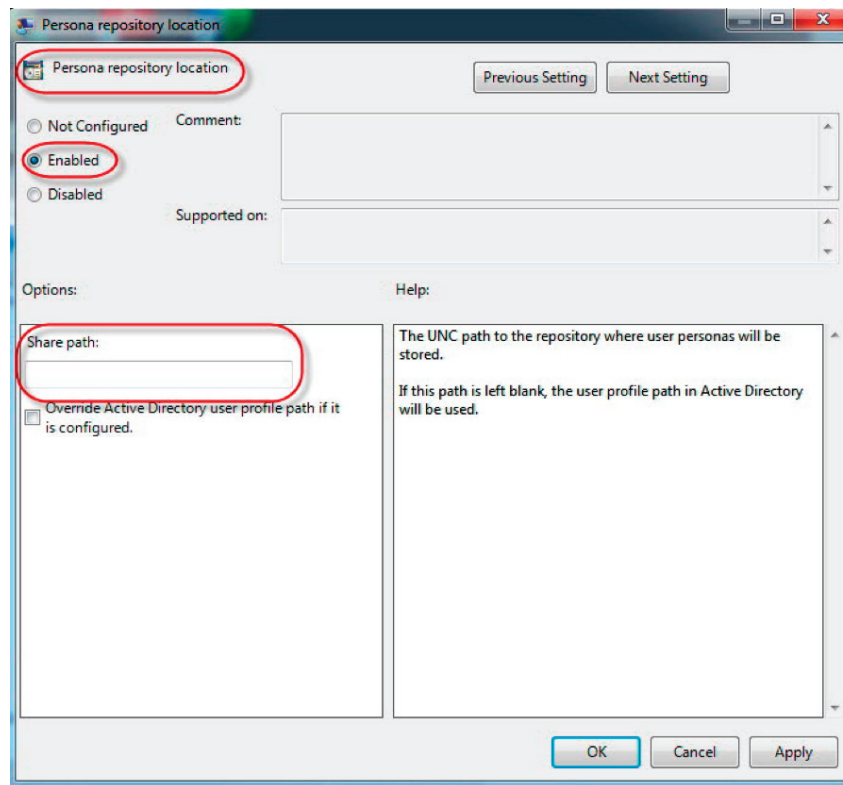


Figure 7: Persona Repository Location Configuration

OVERRIDE ACTIVE DIRECTORY USER PROFILE PATH IF IT IS CONFIGURED	
Brief definition	(Override Windows roaming profile path if it is configured.) If both a Windows roaming profile path and a View Persona Management user profile Share path are specified, overrides the Windows roaming profile path for View.
Default value	Disabled (No override. View Persona Management uses the Windows roaming profile path if both a View Share path and a Windows path are specified).
Possible values	Enabled, disabled
Use cases and details	<p>Available only if Persona repository location is enabled. If Windows roaming profiles are set up, and you wish to bypass the Windows roaming profile location for View Persona Management, enable this setting. Simply entering a Share path location does not override the Windows roaming profile location if you have both Share path and the Windows profile location configured.</p> <p>Use case for enabling Override Active Directory user profile path if it is configured:</p> <p>If a user is logged in on a physical or virtual Windows machine where roaming profiles are implemented and then opens a View Client from that same machine and logs in as the same user in the same domain, the correct profile is loaded on each desktop (the Windows desktop and the View desktop). If Persona Management is implemented on the View desktop, then Persona Management manages the profile on the View desktop, and Windows manages the roaming profile on the Windows desktop. Conflicts can occur if changes are made from both the Windows desktop and the View desktop to the same files or registry entries in the profiles, even though they are different profiles. This is particularly true for the registry, which is stored in a single file. The order of precedence of saving changes to profiles causes both View and Windows to use the Windows profile. The rule is that changes made during the last session to log out are uploaded to the network user profile. Because Windows roaming profiles are saved to the network at log out, and not continuously as in Persona Management, changes to the Windows user profile always override changes to the View user profile, and the Windows changes are uploaded to the repository. To avoid this conflict, configure different paths for the View user profile and the Windows roaming profile, and enable Override AD user profile path if it is configured. Two profiles—one for the View desktop, and one for the Windows desktop—are then maintained.</p>

REMOVE LOCAL PERSONA AT LOG OFF	
Brief definition	Deletes the user's locally stored user profile upon logout.
Default value	Disabled (user profiles stored on the local desktop, including local settings folders, are not deleted when the user logs out).
Possible values	Enabled, disabled
Use cases and details	<p>Generally do not enable this. Logout is generally faster if you keep this disabled. Processing time would be increased with enablement because View would delete the user's profile on the local device after synchronizing with the user profile location upon user logout.</p> <p>Use cases to keep the setting disabled:</p> <ul style="list-style-type: none"> • In a floating pool of nonpersistent desktops, the local user profile is deleted at logout automatically, anyway. • In a dedicated pool, you do not need to delete the local profile because there is no sharing of desktops. Leaving the copy on the desktop does not cause issues and would only take extra time to delete. • Do not enable this setting if you configure persistent disks, which store enduring local profiles on disks attached to nonpersistent virtual desktops. This would delete the user data from the persistent disks at logout. <p>Use cases to enable this setting:</p> <ul style="list-style-type: none"> • Enabling this setting would be useful for removing user profiles in a physical desktop pool. If a user logged into the physical desktop, someone else's user profile would not remain on the desktop. • If a virtual desktop is shared between users (such as a floating pool without regular refreshes), enabling this setting to remove the local persona would reduce storage requirements on the desktop. • Enable this setting for persistent desktops or desktops with persistent disks where user profiles have a large number of files (tens of thousands). Login times will be significantly faster if you enable this setting. This is because the local profile on the desktop must be synchronized upon login, and if the local profile is large, the synchronization with the network version will delay login time. Without a local profile, no synchronization will be necessary.

DELETE 'LOCAL SETTINGS' OR 'APPDATA\LOCAL' WHEN PERSONA IS REMOVED	
Brief definition	Deletes a user's local settings folders when the user persona is removed at logout.
Default value	<p>Disabled by default when Remove local persona at log off is disabled (local settings folders are not deleted when users log off, and the local persona is not removed).</p> <p>If Remove local persona at log off is enabled, this setting defaults to enabled, and everything in the local profile, including the <code>Local Settings</code> folders, is deleted.</p> <p>If this setting is disabled, then everything in the local profile will be deleted on logout except for the <code>Local Settings</code> folders.*</p>
Possible values	Enabled, disabled
Use cases and details	<p>Available when Remove local persona at log off is enabled.</p> <p>Use cases for disabling this setting:</p> <ul style="list-style-type: none"> If you are using persistent desktops or disks and have enabled Remove local persona at log off, but Roam local settings folders is not enabled, then disable Delete 'Local Settings'.... In this case, it is better to leave the local settings folders on the desktop, or you may lose data. For example, Outlook stores information in <code>Local Settings</code> that would be lost if you do not roam the local settings folders, and you also delete the local settings folders at logoff. With applications that store data or settings in local settings folders, you can have some choices. You can enable Roam local settings folders, or you can keep the local persona and the local settings on the desktop by disabling Remove local persona at log off and Delete 'Local Settings'.... The latter choice is not possible for floating desktops, so you must enable Roam local settings.

* The following table explains the interaction between **Delete 'Local Settings' or 'AppData\Local' when persona is removed** and **Remove local persona at log off**.

	Remove local persona at log off enabled	Remove local persona at log off disabled
Delete 'Local Settings' or 'AppData\Local' when persona is removed enabled	<p>Both local persona and local settings are removed at logout.</p> <p>If you enable Remove local persona..., Delete 'Local Settings'... is enabled by default.</p>	<p>Local persona is kept at logout, local settings are removed.</p> <p>Not available.</p> <p>If Remove local persona... is disabled, Delete 'Local Settings'... is not activated.</p>
Delete 'Local Settings' or 'AppData\Local' when persona is removed disabled	<p>Local persona is removed at logout, local settings are kept.</p> <p>If you enable Remove local persona..., you must disable Delete 'Local Settings'... to achieve this.</p>	<p>Local persona and local settings are kept at logout.</p> <p>Default for Remove local persona... is disabled. Delete 'Local Settings'... defaults to disabled and is unchangeable when Remove local persona... is disabled.</p>

ROAM LOCAL SETTINGS FOLDERS	
Brief definition	Include the Local Settings or AppData\Local folders in synchronization with the remote repository, along with the rest of the user persona.
Default value	Disabled (local settings folders are not roamed or synchronized when the rest of the user profile is roamed).
Possible values	Enabled, disabled
Use cases and details	<p>Use cases for enabling this setting:</p> <ul style="list-style-type: none"> • In the physical world, where a user may roam between physical computers (for example, home and office), the local settings directory is a repository to store settings for each individual physical machine. In the virtual world, those same local settings are needed at each login. Enabling this setting allows View Persona to retain local settings between sessions. • A use case for enabling Roam local settings folders is with applications like Outlook or Zimbra, which store data (such as email messages) or settings in local settings folders. However, performance and scalability can be negatively impacted if data is stored in one large file (such as Outlook email messages) that must be periodically uploaded to the network repository. • With applications that store data or settings in local settings folders, you can have some choices. You can enable Roam local settings folders, or you can keep the local persona and the local settings on the desktop by disabling Remove local persona at log off and Delete 'Local Settings'.... The latter choice is not possible for floating desktops, so you must enable Roam local settings.

FILES AND FOLDERS TO PRELOAD	
Brief definition	Files and folders to be fully downloaded at login. Changes are uploaded periodically to the repository, as configured in View Persona Management. Persona Management manages these files and folders after the preload.
Default value	One folder (<Start Menu>\Programs\Startup) is preloaded by default, and you cannot delete this. You can add to this default.
Possible values	Paths relative to the root of the local profile. Do not use drives in pathnames.
Use cases and details	If you know that the user is going to need a particular file or folder available at login, specify the folder here.

FILES AND FOLDERS TO PRELOAD (EXCEPTIONS)	
Brief definition	Files and folders within the Files and folders to preload paths that are not to be preloaded.
Default value	Blank
Possible values	Paths relative to the root of the local profile. Do not use drives in pathnames.
Use cases and details	Within the folders that the user needs preloaded at login, you can exclude some files or folders that do not need to be downloaded before login.

WINDOWS ROAMING PROFILES SYNCHRONIZATION	
Brief definition	Files and folders to be managed by standard Windows roaming profiles, with full download at login and no upload until the full upload at logout.
Default value	Two folders are in this list by default, and you cannot delete these. These folders are <Roamed Application Data>\Microsoft\Windows\Themes\Custom.theme and <Roamed Application Data>\Microsoft\SystemCertificates. You can add to the default list.
Possible values	Paths relative to the root of the local profile. Do not use drives in pathnames.
Use cases and details	You might want particular profile files and folders to behave like standard Windows roaming profiles, with download at login and upload only at logout, and not downloaded as needed or uploaded periodically, as in Persona Management.

WINDOWS ROAMING PROFILES SYNCHRONIZATION (EXCEPTIONS)	
Brief definition	Files and folders within the Windows roaming profiles synchronization paths that are to be managed by View Persona Management, instead of by Windows roaming profiles.
Default value	Blank
Possible values	Paths relative to the root of the local profile. Do not use drives in pathnames.
Use cases and details	Within the folders that you want downloaded at login and uploaded only at logout, you can exclude some files or folders.

FILES AND FOLDERS EXCLUDED FROM ROAMING	
Brief definition	Files and folders in the user profile that exist only on the local system and do not roam with the user.
Default value	Several folders are excluded from roaming by default, and you cannot delete these. You can add to the default list. The default list includes the user profile's temp folder, the ThinApp cache folder, and the cache folders for Internet Explorer, Firefox, Chrome, and Opera.
Possible values	Paths relative to the root of the local profile. Do not use drives in pathnames.
Use cases and details	You might use this setting for an application subfolder that holds temporary or cache files that do not need to be synchronized with the user profile on the repository.

FILES AND FOLDERS EXCLUDED FROM ROAMING (EXCEPTIONS)	
Brief definition	Exceptions within the folders specified in Files and folders excluded from roaming , which must roam (synchronize with the repository).
Default value	Blank
Possible values	Paths relative to the root of the local profile. Do not use drives in pathnames.
Use cases and details	Within the profile folders that you want to exclude from roaming, you can specify some files or folders that must roam.

FOLDERS TO BACKGROUND DOWNLOAD	
Brief definition	Folders to download in the background immediately after login. User can work while files download.
Default value	Disabled
Possible values	Paths relative to the root of the local profile. Do not use drives in pathnames.
Use cases and details	If you know of large application files that the user will need soon after login, you can maintain the quick Persona Management login and allow the user to do work in another application. The next application's files will be available sooner than if they were downloaded when the application opens. A typical folder to background download would be the sandbox for a ThinApp application. By the time the user starts up the ThinApp application, the needed files may already have downloaded. This improves the ThinApp application startup time.

FOLDERS TO BACKGROUND DOWNLOAD (EXCEPTIONS)	
Brief definition	Subfolders within the folders specified in Folders to background download that are not to background download.
Default value	Disabled
Possible values	Paths relative to the root of the local profile. Do not use drives in pathnames.
Use cases and details	For example, subfolders in the ThinApp application's sandbox that do not need to be downloaded for imminent use. They might be small subfolders that would download quickly when needed.

The order of preloading and loading files and folders with these settings is:

1. User logs in, and View Persona Management downloads only the files and folders that Windows requires. Persona Management also preloads any specified user profile files and folders at the time of login.
2. Persona Management background-downloads any specified files and folders from the user profile.
3. The remaining user profile settings and data are downloaded as the user or application opens a user profile file and needs to use the data.

Logging Group Policy Settings

The **Logging flags** group policy setting must be enabled to turn on Persona Management logging. Logging is enabled by default. Error messages and information messages are displayed in the log.

You can extend the logging level by activating **Log debug messages** within **Logging flags**. Then you specify which debug messages you want in the log in the **Debug flags** setting.

LOGGING FILENAME	
Brief definition	Full pathname where you would like the Persona Management log file.
Default value	<Common Application Data>\VMware\VDM\logs\VMWVvp.txt
Possible values	Cannot be a UNC path. Includes the log file name. You can change the log file name.
Use cases and details	Generally do not change this from the default. If you have multiple disks configured, and you want the log on a different disk with more space, you might set a new path value. Consult with VMware Technical Support.

LOGGING DESTINATION	
Brief definition	Where log messages will be sent.
Default value	Send log messages to the log file.
Possible values	Choose from: <ul style="list-style-type: none"> • Send log messages to the log file • Send log messages to the debug port • Both
Use cases and details	Generally keep this setting at the default, unless VMware Technical Support recommends otherwise.

LOGGING FLAGS	
Brief definition	Enabling Logging flags activates logging. You also specify the types of messages to be generated in the log.
Default value	Enabled, with Log error messages and Log information messages selected.
Possible values	You can specify any or all log message types: <ul style="list-style-type: none"> • Log error messages • Log information messages • Log debug messages
Use cases and details	You may wish to disable this setting to turn off logging. Consult with VMware Technical Support for when to select Log debug messages for troubleshooting.

DEBUG FLAGS	
Brief definition	Generates a number of types of debug messages that are placed in the log. Provides more detail than Logging flags alone.
Default value	Disabled (debug messages are turned off).
Possible values	Once enabled, you can choose any or all of: <ul style="list-style-type: none"> • Debug error messages • Debug information messages • Debug registry messages • Debug IRQL messages • Debug port messages • Debug process messages
Use cases and details	Consult with VMware Technical Support for recommendations about when to enable Debug flags . When you do enable Debug flags , it is recommended that you select all options except for Debug IRQL messages and Debug port messages .

Desktop UI Group Policy Settings

HIDE LOCAL OFFLINE FILE ICON	
Brief definition	An offline icon on a file in the user profile indicates that it has not been updated from the user profile repository yet. With this setting, you can hide the offline icon when the user views locally stored user profile files, in Windows File Explorer and most Windows dialog boxes.
Default value	Enabled (the local offline icon is hidden, and the icons in a user's profile appear as normal icons).
Possible values	Enabled, disabled (icons that have not been downloaded from the Persona Management repository appear with the offline symbol).
Use cases and details	Disable Hide local offline file icon when troubleshooting or evaluating Persona Management.

SHOW PROGRESS WHEN DOWNLOADING LARGE FILES	
Brief definition	Display a progress window on the desktop when View is downloading large files from the remote persona repository.
Default value	Disabled (no progress window is displayed).
Possible values	Enabled, disabled
Use cases and details	If your user population would benefit from receiving a status message when a large file download causes a delay, enable this setting.

MINIMUM FILE SIZE TO SHOW PROGRESS WINDOW (MB)	
Brief definition	Works in conjunction with enablement of Show progress when downloading large files . Minimum file size in MB that must be in the process of downloading for a progress dialog to appear. This minimum file size is an aggregate size of all files downloading at one time.
Default value	50MB when Show progress when downloading large files is enabled.
Possible values	0-4294967295, in MB
Use cases and details	When Show progress when downloading large files is enabled, this setting is also enabled.

SHOW CRITICAL ERRORS TO USERS VIA TRAY ICON ALERTS	
Brief definition	Indicates critical errors with alert icons in the user's desktop tray.
Default value	Disabled (alerts are hidden).
Possible values	Disabled, enabled
Use cases and details	Errors such as loss of network connectivity to the Persona Repository location or replication problems will appear in the tray icon when this setting is enabled.

Folder Redirection Group Policy Settings

View Persona Management downloads the user profile from the repository to the local machine for editing. With Windows folder redirection, the user profile remains on the network share and is edited on the network share. In general, Persona Management as-needed user profile retrieval is preferable. However, in some use cases, Windows folder redirection for the user profile is a better choice.

FOLDER REDIRECTION GROUP POLICY SETTINGS IN GENERAL	
Brief definition	Folder redirection allows the administrator to redirect the path of any local profile folder to a new location on a network file share. Users access the files in the redirected folder during the user session as if the documents were based on a local drive.
Default value	No redirection
Possible values	Enabled, disabled. The redirected location specified for each folder must be a UNC path. It is a best practice to use different subdirectories for the persona repository location and each redirected folder location. For example, if the persona repository location is \\UNCpath\share\%username%.%userdomain%\profile, you can use \\UNCpath\share\%sename%.%userdomain%\My Documents. You can specify a different redirection location for each user profile folder, or no redirection folder for any of the user profile folders.
Use cases and details	<p>In most cases, do not use folder redirection, and use the Persona Management as-needed file downloads and periodic file uploads of user profile data.</p> <p>Use cases for Persona Management user profile management and not folder redirection:</p> <ul style="list-style-type: none"> • User profile is large, or there is latency to the network share: If the user profile is large, or there is latency on the network share, editing a file on the network share may proceed slowly. Persona Management is the better choice. • User profile repository accessed over WAN: If the user profile is accessed over a WAN, then Persona Management is preferable. <p>Use cases for redirection, not Persona Management:</p> <ul style="list-style-type: none"> • Local system is unstable: If the redirected folder is accessed over the WAN, user experience can suffer when editing a document. However, sometimes the local system is unstable and has network outages or failures, and upload to the remote repository is at risk. Redirecting the synchronization to another folder eliminates the need to rely on the unstable local environment. • User profile repository is in the same data center or on the same SAN: If the user profile repository is close by, then folder redirection may be preferable to Persona Management. The user profile will take a short enough time to download and upload. • Both physical and virtual desktops: If the user must access both a physical desktop and a virtual desktop, you can use redirected folders to allow the user to share data between the desktops. Windows folder redirection is required because Persona Management is not currently supported on physical desktops. <p>The alternative is to install View Agent with the Persona Management setup choice on the non-View physical machine. (Note: you cannot install View Agent on the same machine with View Client.) The View Agent with the Persona Management setup choice on the physical machine can copy the user profile from the physical machine to the central profile repository. You are then able to migrate data from the physical machine to the virtual desktop.*</p>

FOLDER REDIRECTION GROUP POLICY SETTINGS IN GENERAL (CONTINUED)	
Use cases and details (continued)	<ul style="list-style-type: none"> • Both Windows XP and Windows 7 desktops: If the user must access both a Windows XP View desktop and a Windows 7 View desktop, redirected folders provide a way to share files between these operating systems. Normally, roaming profiles cannot be shared between Type 1 Windows operating systems (XP) and Type 2 operating systems (Vista or Windows 7).*

* For which folders to redirect for the last two use cases, see the following table.

	Redirect This Folder If Users Must Share Files Between Physical and Virtual Desktops	Redirect This Folder If Users Must Share Files Between Their Windows XP and Windows 7 Desktops
Application Data (Roaming)	Yes	No
Contacts	Yes	No
Cookies	Yes	No
Desktop	Yes	Yes
Downloads	Yes	No
Favorites	Yes	No
History	Yes	No
Links	Yes	No
My Documents	Yes	Yes
My Music	Yes	No
My Pictures	Yes	Yes
My Videos	Yes	No
Network Neighborhood (My Network Places)	Yes	No
Printer Neighborhood	Yes	No
Recent Items	Yes	No
Saved Games	Yes	No
Searches	Yes	No
Send To	Yes	No
Start Menu	Yes	No

	Redirect This Folder If Users Must Share Files Between Physical and Virtual Desktops (Continued)	Redirect This Folder If Users Must Share Files Between Their Windows XP and Windows 7 Desktops (Continued)
Startup Items	Yes	No
Templates	Yes	No
Temporary Internet Files (Internet Cache)	Never	Never

For information about folder redirection as a special situation for deploying Persona Management, see [Deployments with Both View Persona Management and Windows Roaming Profiles](#).

5. Creating and Deploying Desktop Pools from the Master Virtual Machines

After configuring the parent or template desktops with the View Agent and the Persona Management setup option, and the group policy configurations, you create and deploy your desktop pools. For details, see *Create View Desktops That Use Persona Management* in the *Configuring User Profiles with View Persona Management* chapter in the [VMware View Administration guide](#).

Special Situations for Deploying View Persona Management

Some situations demand special considerations when deploying Persona Management. Following are brief notes regarding these special situations.

Deployments with Both View Persona Management and Windows Roaming Profiles

Deployments where users access both View desktops managed by Persona Management and standard Windows desktops managed by roaming profiles can cause problems. The best solution if the desktops are in the same domain is to use different profiles for the two desktop environments. To accomplish this:

- Configure Windows roaming profiles (either with Windows GPO settings or on the user object in Active Directory)
- Configure View Persona Management
 - Enable **Persona repository location**
 - Enable **Override Active Directory user profile path if it is configured**

This prevents Windows roaming profiles from overwriting a View Persona Management profile when the user logs out of the desktop.

For more information, see [Override Active Directory user profile path if it is configured](#).

If users will share data between Windows roaming profiles and View Persona Management profiles, configure Windows folder redirection. For more information about folder redirection for sharing information between physical and virtual desktops, see [Both physical and virtual desktops](#).

Paths for Redirected Folders

In folder redirection group policy settings for user profile folders, be sure to:

- Include %username% in the folder path, but do not place it last in the path. If you forget to include %username%, Persona Management appends it to your path.
- Use the name of the redirected folder as the last subfolder in the path; for example, My Documents. The last folder in the path is displayed as the folder name on the user's desktop.

Scanning User Profiles with Antivirus Checkers

If you have an antivirus checker installed in each desktop, exclude the user profiles from the scans. Instead, scan the profiles stored on the remote repository. This saves IOPS.

VMware View offers vShield Endpoint, which scans user profile files as they open, from outside the desktop. You do not need an antivirus checker within each desktop.

Backing up User Profiles

Do not back up View user profiles with software that requires the Windows Volume Shadow Service. View already backs up the user profile during user sessions. Another piece of software backing up with the Volume Shadow Service could cause corruption of files.

For recommendations on settings for the Volume Shadow Service with Persona Management, see the [VMware View Optimization Guide for Windows 7](#).

Enhancing ThinApp Application Startup Time

If you provision your desktops with ThinApp applications, the ThinApp sandboxes of user data can also be stored in the View user profile and roam with the user.

You can configure View Persona Management to enhance ThinApp application startup time. Configure **Folders to background download** to include the ThinApp sandbox for any ThinApp application that has large files. This reduces the time to start up the ThinApp package because the sandbox is already loaded.

Use Persistent Disks If Users Have Large User Profile Files

If your users create large files as part of their user profiles, configuring View Composer persistent disks can enhance performance of Persona Management. Persistent disks act as a cache for the user profiles. Persistent disks can be configured only with dedicated-assignment, linked-clone desktops.

For more information, see *Configuring View Composer Persistent Disks with View Persona Management* in the *Configuring User Profiles with View Persona Management* chapter in the [VMware View Administration guide](#).

Migrating Folder Redirection to Persona Management

If you have a system with folder redirection already in place, but no roaming profiles, and you want to migrate to a View deployment, you can easily migrate the data. For example, if you are migrating from Windows XP physical desktops with folder redirection to Windows 7 in View, preserve your folder redirection settings. When users log in to their new Windows 7 View desktops, the data in their redirected folders will be available to them.

The data migration is automatic through redirected folders, but View does not force you to migrate the registry settings from the physical desktops to View desktops.

Use of View 5 Persona Management with Other Profile Management Tools

If you have another profile management tool besides Windows roaming profiles installed for your View desktops, and you want to try implementing Persona Management, VMware does not have best practice advice. VMware ships View 5 with Persona Management disabled so that you can test the new version of View with your current profile management tool.

References for Further Information

For more information on VMware View:

- Visit the [VMware Community Forum](#) for View
- Query the [VMware Knowledge Base](#)
- Contact your local authorized [VMware partner](#)
- Delve into the [View Technical Resources](#) (technical whitepapers), including the [Windows 7 Optimization Guide for VMware View](#)
- Refer to the [VMware View documentation](#):
 - [VMware View Architecture Planning](#)
 - [VMware View Administration guide](#)
 - [VMware View Installation guide](#)
 - [VMware View Upgrades guide](#)
 - [VMware View Clients documentation](#)
 - [VMware View Integration guide](#)

About the Author and Contributors

Tina de Benedictis is a Technical Marketing Manager for Enterprise Desktop at VMware, focused on VMware View and ThinApp. Tina's background at VMware includes writing Knowledge Base articles and developing Technical Support training on ThinApp, Fusion, and Capacity Planner. Her previous background is in customer training, technical support, and technical publications at companies including Mobileum (Roamware), Scopus (Siebel), and ASK/Ingres (Computer Associates).

Special thanks to Kevin Goodman and Steve McAllister for their dedicated contributions to the content in this guide.

