

17

Managing the End User Environment in Horizon

One of the topics we touched on earlier in this book was the need to manage user profiles when deploying a virtual desktop environment, particularly with regard to using a floating desktop assignment, where the desktop doesn't belong to any of the users. Therefore, it contains none of their personal information or settings. There are a number of more advanced third-party tools available to manage user profiles, such as Liquidware Labs' ProfileUnity. However, in this chapter, we will discuss the two VMware options that ship as part of the Horizon View product suite. The first of these, **View Persona Management**, ships with all versions of Horizon View, but the latest solution, **VMware User Environment Manager (UEM)**, is either available as part of the Enterprise Edition or available as a standalone product.

VMware View Persona Management allows you to configure user profiles that are dynamically synchronized with a central profile repository, stored on a server in the data center. By using View Persona, you can give users access to their own personalized desktop, irrespective of which virtual desktop machine they log on to. By contrast, VMware UEM is a more scalable, enterprise-class solution, which works by installing a client on the hosting infrastructure for the hosted desktops and applications, the endpoint devices such as desktops and laptops, and also the virtual desktop machines. These clients are then configured from Active Directory using Group Policy to manage the end users.

When an end user logs on to their endpoint device or virtual desktop machine, they then have their policy settings applied, such as network and printer mappings and application shortcuts. UEM is a more advanced solution compared to Persona Management. UEM allows you to create dynamic contextual policies that are based on conditional statements that you configure using the management console, rather than the binary on or off approach that Persona Management takes.

You also have the ability to speed up apps by predefining the policies and settings ready for when an end user launches the app, the configuration settings are automatically applied. These settings can also be applied to published apps, published desktop sessions, and virtual desktop machines.

In this chapter, we are going to look at both options, but before we get into the details and the configuration steps required to get Persona Management and UEM up and running, let's briefly discuss what we mean by a user profile and the benefits of deploying a tool to manage user profiles.

We will cover the following topics in this chapter :

- Defining a user profile
- View Persona Management
- VMware UEM

Defining a user profile

A user profile is a collection of settings that makes the computer look, work, and feel the way the end user wants it to. It contains their personal settings for desktop backgrounds, screensavers, data files, configuration settings, and other features that are user-specific. User profiles ensure that the desktop that a user logs in to contains their own personal preferences. More advanced settings include adding specific registry settings and allowing users to migrate between different versions of the Windows operating system.

It is also worth remembering that there are different profile versions based on which operating system you are using. These are listed in the following table:

Windows Desktop OS Version	Windows Server OS Version	Profile Version
Windows NT 4.0 to Windows Vista	Windows NT Server 4.0 - Windows Server 2008	Version 1 Profile
Windows 7	Windows Server 2008 R2	Version 2 Profile
Windows 8 to Windows 8.1	Windows Server 2012 - 2012 R2	Version 3 Profile
Windows 8.1	Windows Server 2012 R2	Version 4 Profile
Windows 10 (1507 to 1511)	Windows Server 2016	Version 5 Profile
Windows 10 (1607 and later)		Version 6 Profile

A user profile includes the following information:

- User-generated information
- User-specific data and desktop settings
- Application data and settings
- Windows Registry entries that are configured by applications

If you are deploying ThinApp virtualized applications to the desktop, the ThinApp sandbox can also be included within the user profile and, as such, be roamed with it.

It's also worth remembering that a user profile is different from a user account. A user account is what you use to log on to a Windows desktop, whereas a user profile is where an end user's settings and data live. Each user account will have at least one user profile associated with it.

Why do you need profile management?

As we discussed back in *Chapter 2, Understanding Horizon 7 Architecture and Components*, the key reason you would want to deploy Persona Management is to move the end users away from having persistent desktops and get them to use a non-persistent desktop or floating/stateless desktop model. Moving to this type of deployment model essentially means that a user does not own their own virtual desktop, and they merely use one for the time they are logged in. It also means that all their personal data and settings cannot be applied to a virtual desktop machine that can essentially be used by anyone. Therefore, you need a mechanism for delivering this level of personalization—that is, profile management, or user environment management, as it's now more commonly referred to.

This will ultimately save management costs as well as reduce infrastructure, as you can now look at concurrent user connections rather than having to deploy a virtual desktop machine for every user in your organization.

Now that we have talked about what profile management is, and why you would need it, let's look at the two VMware solutions in a bit more detail, what each one delivers, and how to configure them.

View Persona Management

As we discussed previously, Persona Management ships with all versions of Horizon View. It delivers a solution that allows you to configure user profiles to be dynamically synchronized with a central repository, downloading the user data and information when a user logs in and requests it, from virtual desktops as well as physical desktops. However, the real use case is in allowing you to move to a non-persistent desktop model.

View Persona Management features

The following lists some of the features that View Persona Management delivers:

- It delivers access to the end users for a personalized desktop experience whenever they log in to a desktop, no matter which virtual desktop machine is assigned to them. Persona Management operates independent of the virtual desktop machine.
- It helps to expand the functionality and enhance the performance of Windows roaming profiles.
- It has centralized configuration using the View Administrator.
- It is configured via Group Policy.
- It requires fewer IOPS than a Windows roaming profiles deployment.
- It can store files on any CIFS share.
- It supports Full Clone and Linked Clone virtual desktop machines.
- It complies with security policies, as the end user still owns the files and folders.
- It integrates with existing Windows roaming profile deployments.

In the next section, we are going to take a look at how Persona Management works.

Understanding how Persona Management works

The question that typically gets asked is, "How does Persona Management differ from something like Windows roaming profiles?"

When the end user logs in to their virtual desktop machine, View will only download the files that Windows requires in order to run. One of the tricks here is that Persona Management lets Windows think that it has downloaded the user's profile, and so, Windows continues with the login process, thus speeding up login times.

What actually happens is that the profile folder on the virtual desktop machine appears to the end user as if all of their files and data have been downloaded and are present. In reality, the files and data only get downloaded when the user requests them or when they launch an application that requires additional files and data.

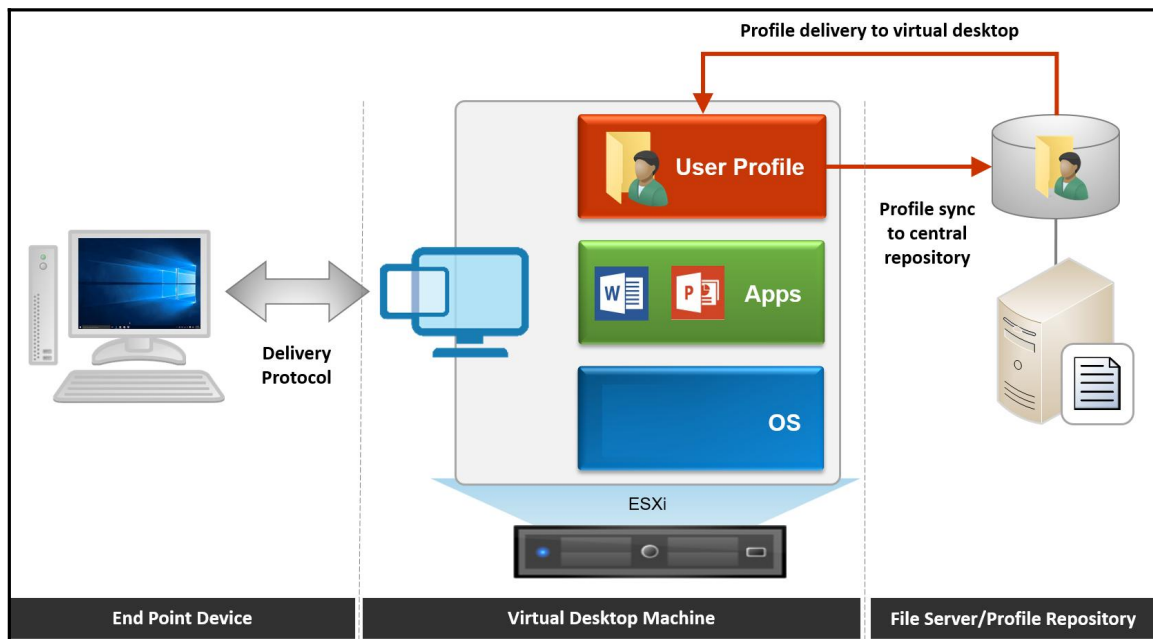
If some of these files are larger than normal files, then there is the option to preload certain types of files to help improve performance.

When the user is using their desktop normally, Persona Management periodically copies any recently changed files or data that have been changed on their virtual desktop machine. It then copies those files and data to the central repository. By default, this replication interval is set to happen every 10 minutes, but you can configure it to a time interval that is more suited to your environment.

This is a key feature, as you reduce data loss inside the **virtual desktop infrastructure (VDI)** environment when compared to physical desktops, or when using roaming profiles.

Once the end user has completed their work and they log out of their virtual desktop machine, Persona Management will only copy files and data that have been updated since the last replication occurred. These file and data changes are then uploaded to the central repository.

This is illustrated in the following diagram:



In the next section, we will take a brief look at how Microsoft roaming profiles fit in with View Persona Management.

Persona Management and roaming profiles

If View Persona Management is enabled, you cannot manage a Horizon View user's profile by using Windows roaming profiles at the same time. You can, however, choose other files and folders that could be managed using Windows roaming profiles. For example, you might want to do this if you are already using Folder Redirection.

To do this, you need to specify a list of files and folders that you want Windows roaming profiles to manage. When the end user logs in to their virtual desktop machine, these files and folders are retrieved from the central repository and then copied back to the central repository when they log out. The point to note here is that all the files and folders are copied, whereas while using Persona Management, they are only copied on demand and, therefore, there is no replication interval.

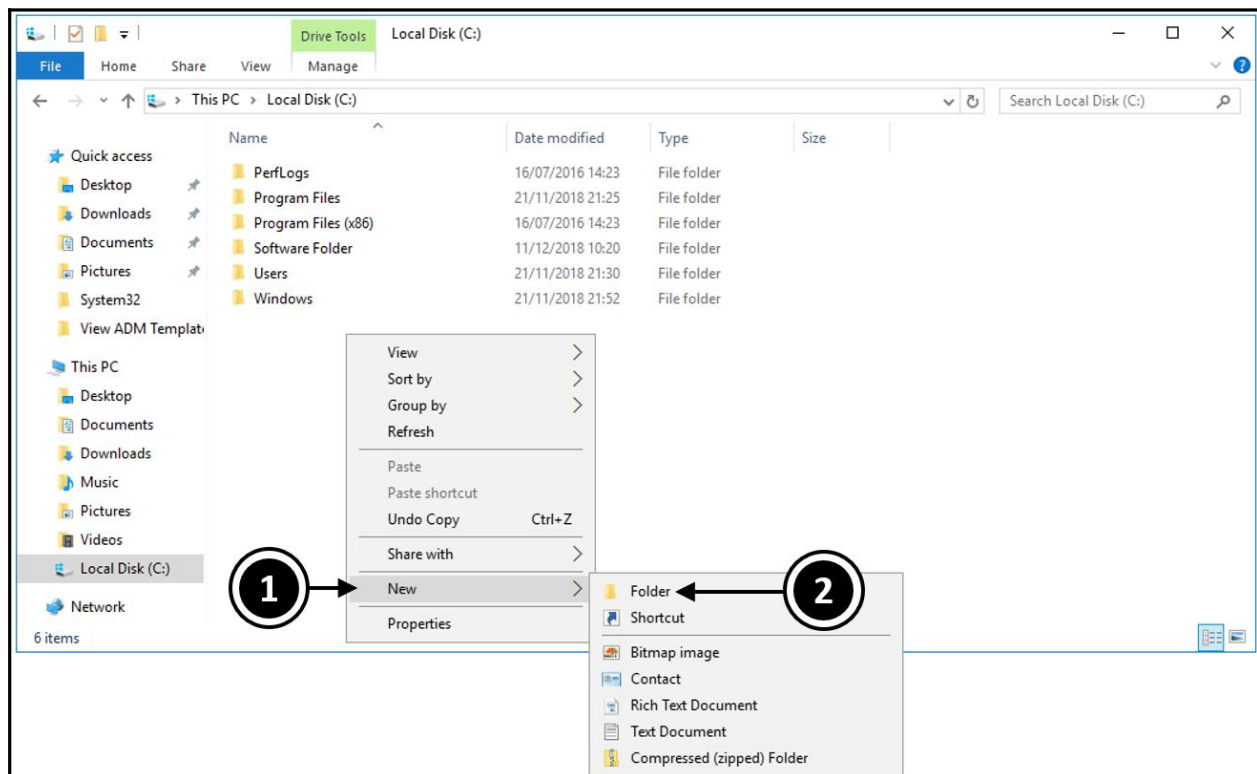
Installing and configuring View Persona Management

Now that we have explained what View Persona Management is and how it works, we are going to configure it in the example lab to demonstrate how it works.

Configuring a user profile repository

First, we need to create a shared folder that will be used to store the user profiles. This folder will be located on a file server that has enough storage capacity to store the profiles. In the example lab, we are going to use the domain controller for this task. To do this, undertake the following steps:

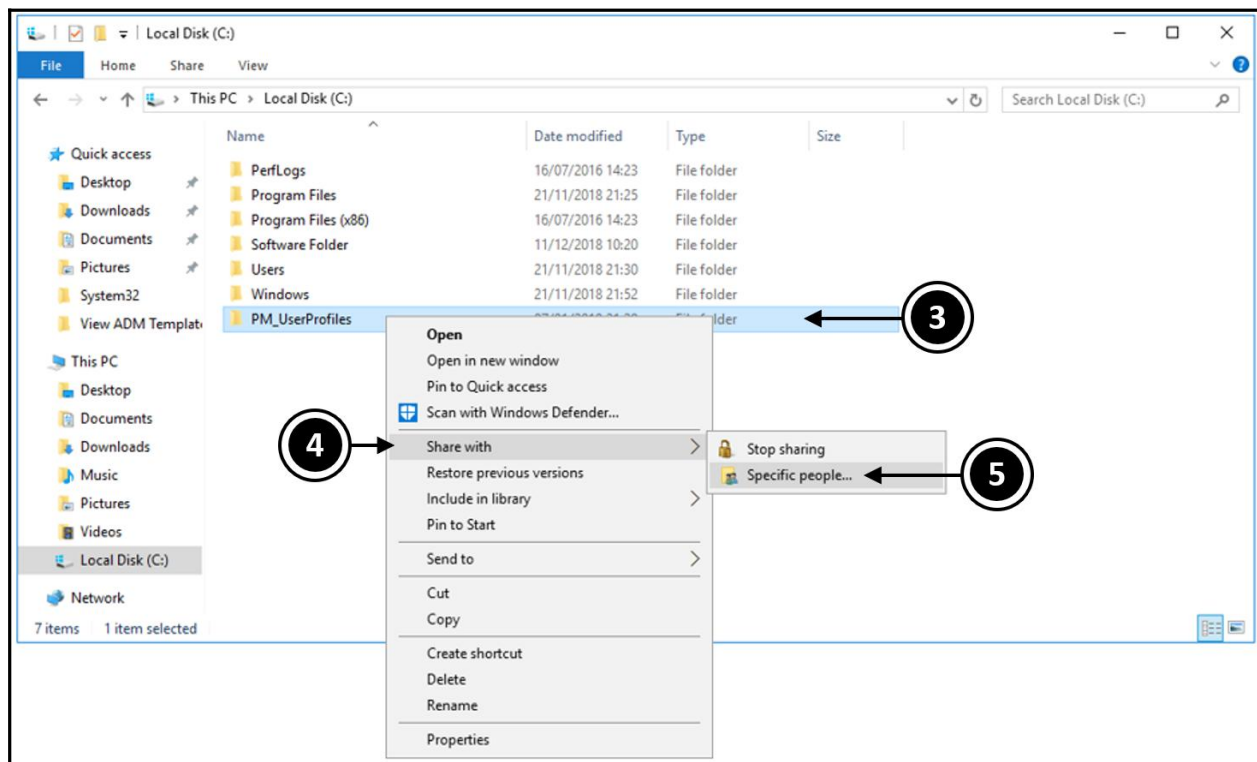
1. Open a console to the server you want to create the folder on and launch Windows Explorer. Navigate to the Local Disk (C:) drive, right-click, and then move your mouse to hover over **New** (1). In the menu that pops up, select **Folder** (2), as shown in the following screenshot:



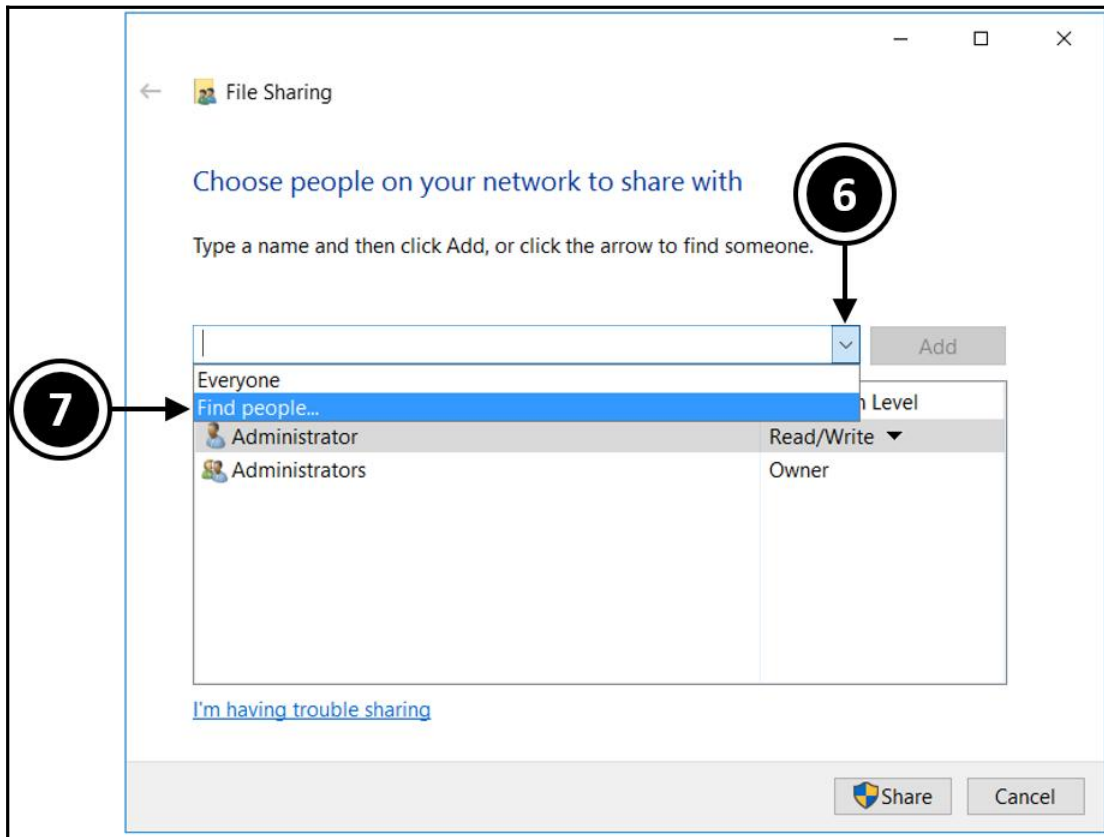
- In the example lab, we've called this this folder `PM_UserProfiles`, as shown in the following screenshot:

Name	Date modified	Type
PerfLogs	16/07/2016 14:23	File folder
Program Files	21/11/2018 21:25	File folder
Program Files (x86)	16/07/2016 14:23	File folder
Software Folder	11/12/2018 10:20	File folder
Users	21/11/2018 21:30	File folder
Windows	21/11/2018 21:52	File folder
PM_UserProfiles	07/01/2019 21:29	File folder

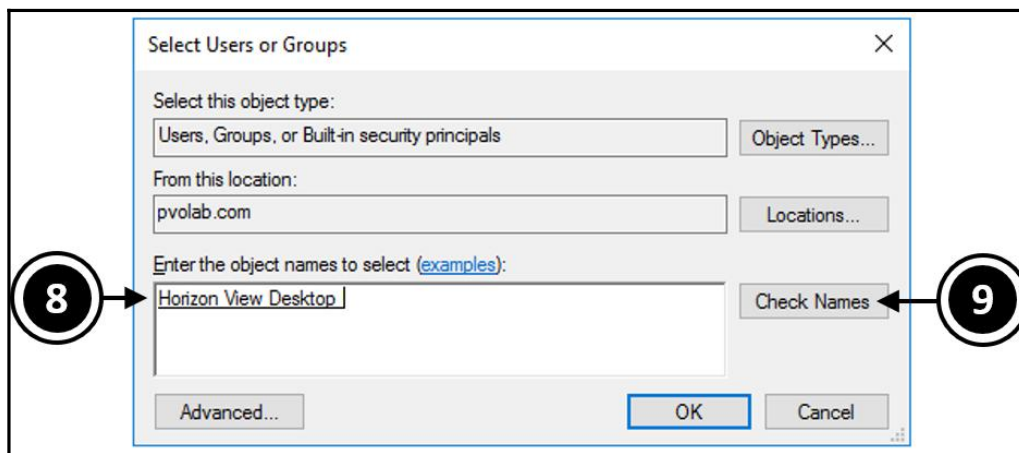
- The next step is to share the newly created folder so that all the users have access to it, as this is where their profiles will be stored. To do this, highlight the `PM_UserProfiles` folder (3) and then right-click. In the contextual menu, move the mouse to **Share with** (4) and then from the new menu, select **Specific people...** (5), as shown in the following screenshot:



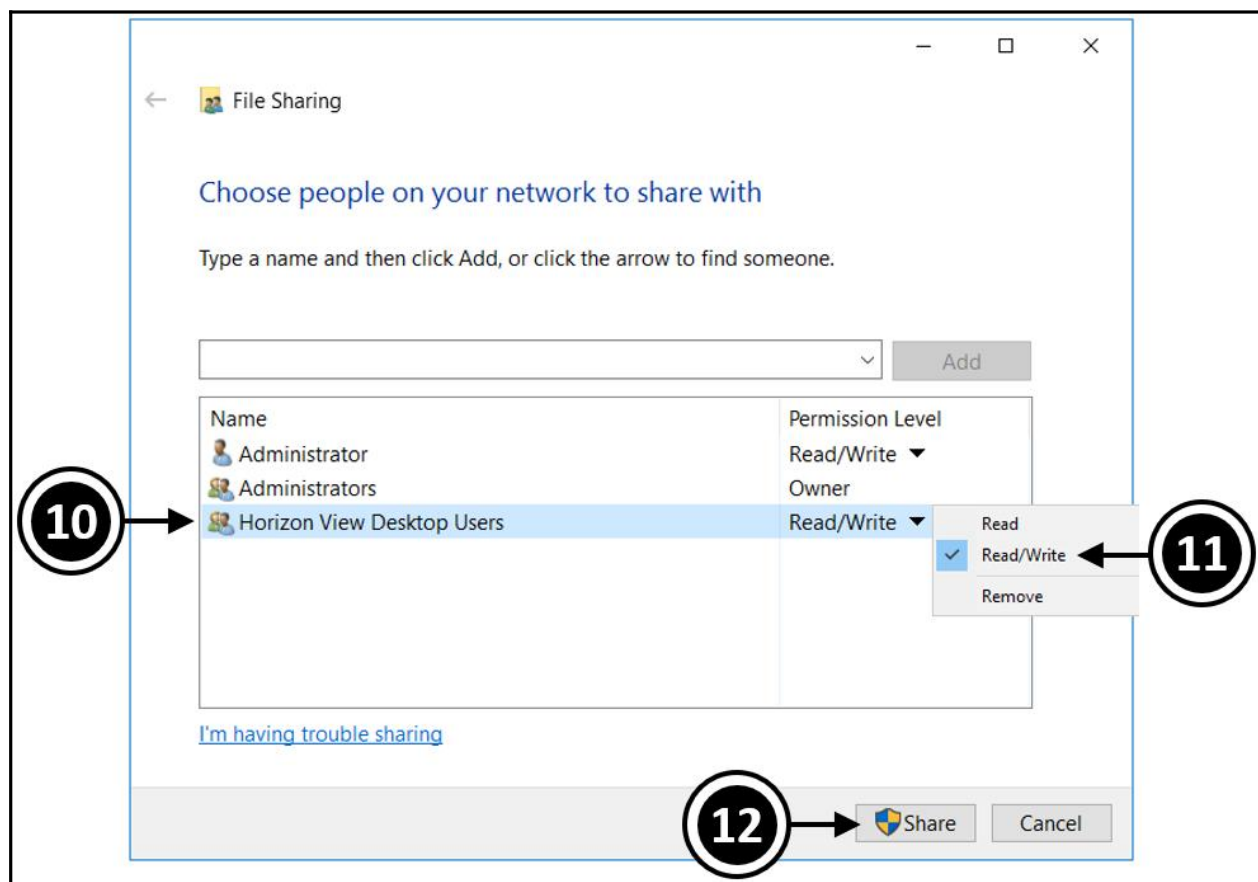
- You will then see the **File Sharing** dialog box, as shown in the following screenshot:



- Click the down arrow (6) and then from the menu options, click **Find people...** (7). You will now see the **Select Users or Groups** dialog box, as shown in the following screenshot:

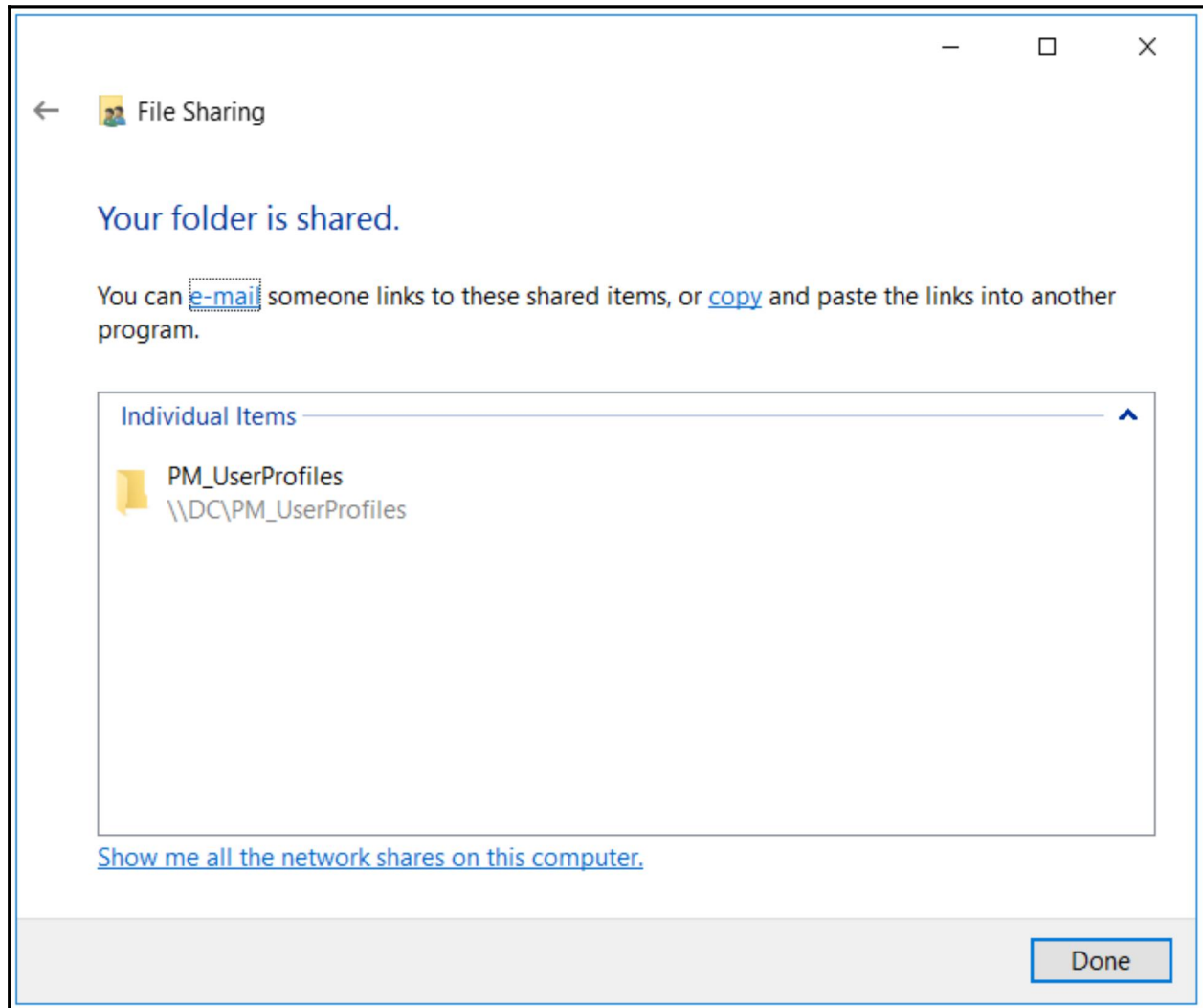


6. In the **Enter the object names to select** box (8), type in the name of the group you want to add to the share. In the example lab, we already have a folder on the file server called `Horizon View Desktop`, so you can just start to type in the first few characters of the name and then click the **Check Names** box (9).
7. Once the group name has been verified, the entire name will be displayed and underlined.
8. Click **OK** to continue.
9. You will now return to the **File Sharing** dialog box.
10. The final step is to set the **Permission Level** for the group you just added to the share. In the example lab, click on the **Horizon View Desktop Users** group (10), and then click on the down arrow (11).
11. From the menu options, select **Read/Write** (11), as shown in the following screenshot:



12. Once you have set the permission level, click the **Share** button (12).

13. You will now see the details for the new shared folder and the path to that folder. In the example lab, the path is `\\DC\PM_UserProfiles`, as shown in the following screenshot:



14. Click the **Done** button when you have finished setting up the shared folder.



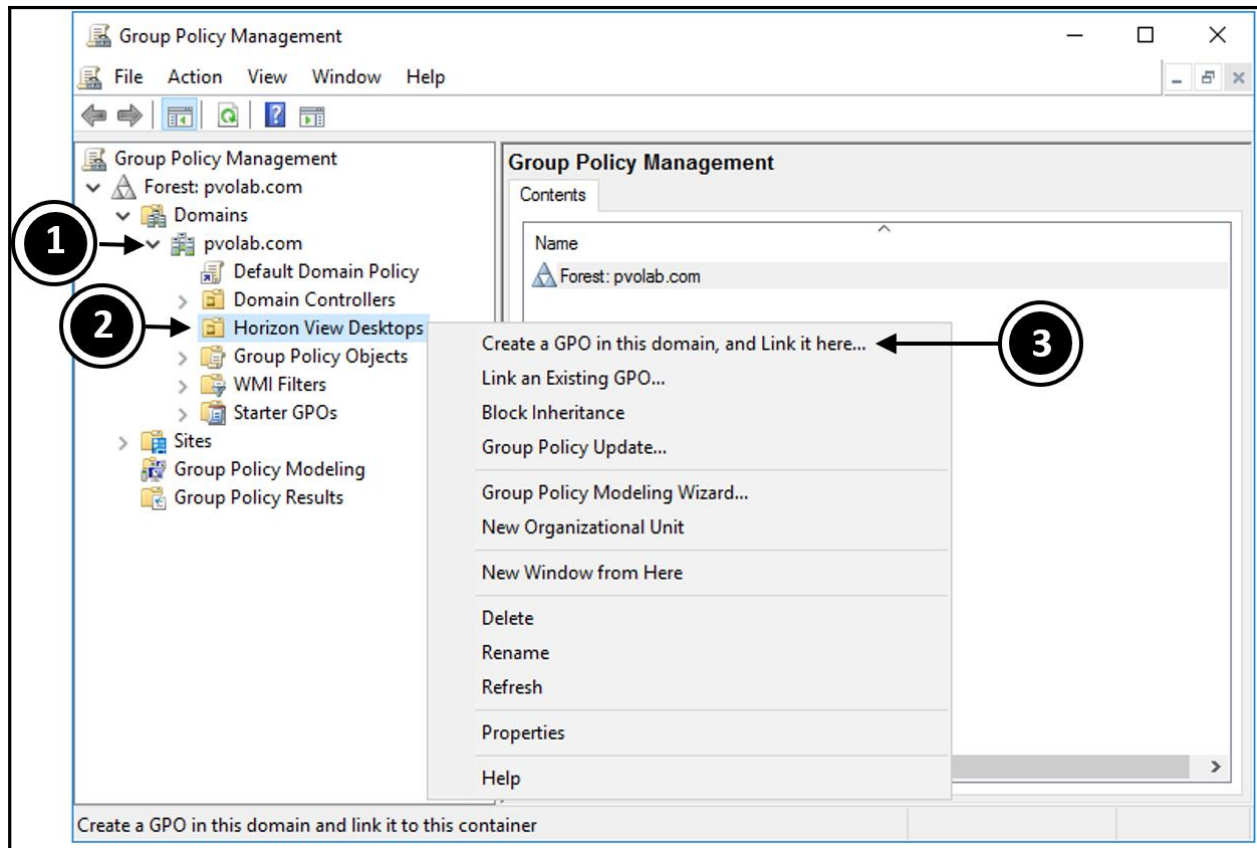
If you are using Windows Server 2008, there is another step in the folder-sharing process, as Windows Server 2008 does not add the permissions for all the users in this group. You need to go into the properties of the shared folder and click on the **Sharing** tab and then on the **Advanced Sharing** button. Tick on the box for **Share this folder** and then click on the **Permissions** button. Then, you need to add the group you want to share the folder with, and then tick the box to give the group permissions for **Full Control**.

You should now have a shared folder set up ready to store the user profiles. The next step is to configure the Persona Management Group Policy templates on the domain controller.

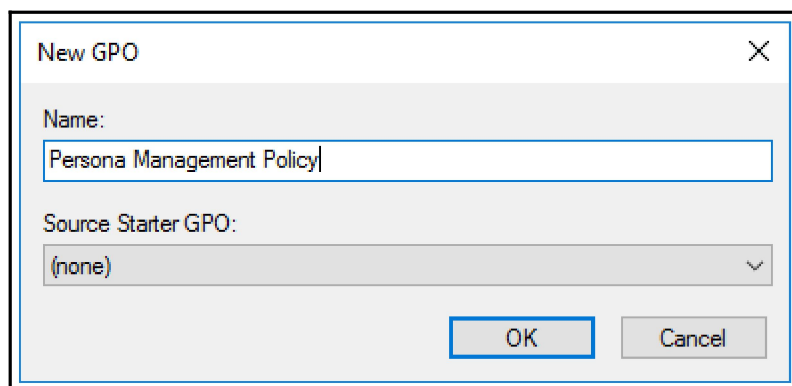
Creating a Group Policy for Persona Management

In Chapter 8, *Configuring and Managing Desktop Pools – Part 1*, we created an **Organizational Unit (OU)** for your virtual desktop machines called `Horizon View Desktops`, Group Policy objects to link to that OU. We also created a policy called **Horizon View Virtual Desktop Policy**, but in this section, we are going to create a second policy for Persona Management by following the steps described here:

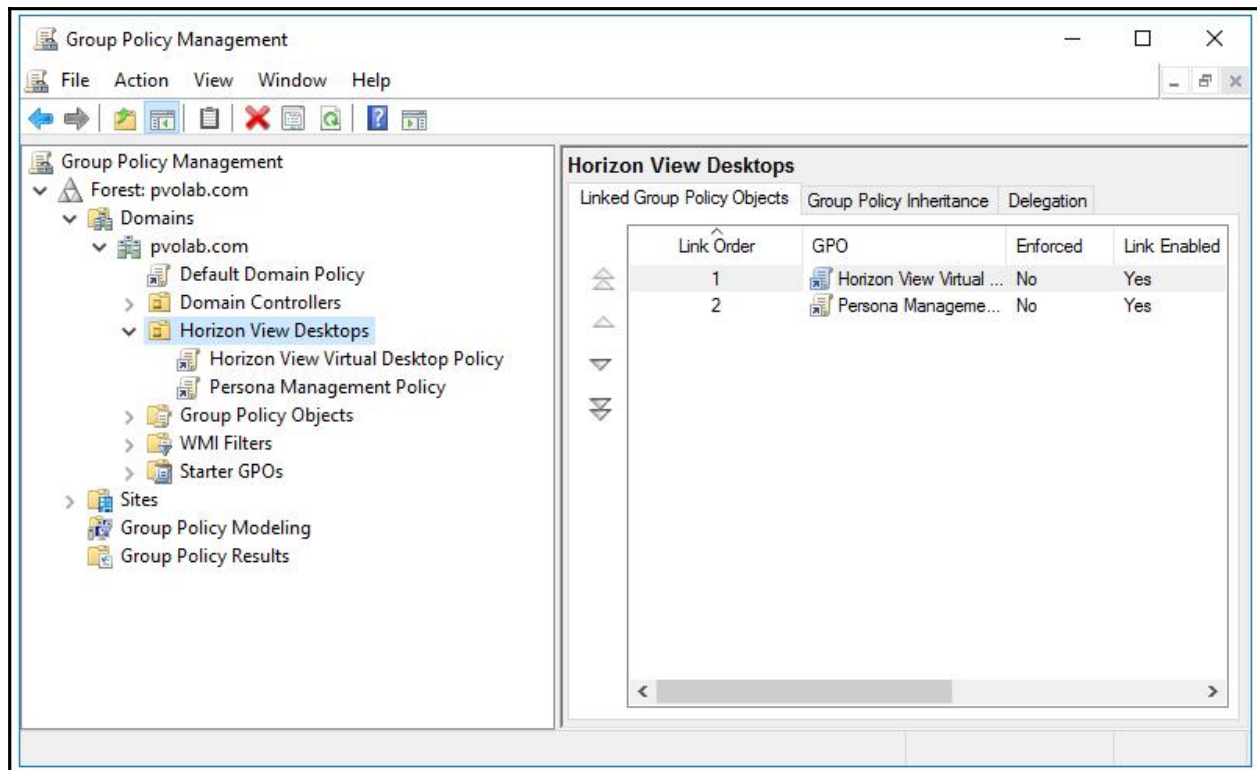
1. To start the configuration, double-click on the Windows Administrative Tools icon to launch the admin tools. You will now see the **Windows Administrative Tools** screen displayed.
2. From this screen, scroll down and then double-click on the option for **Group Policy Management**. You will now see the **Group Policy Management** screen, as shown in the following screenshot:



3. Expand out the folders for Forest : pvolab . com (1), Domains, and then pvolab . com. Click and highlight the Horizon View Desktops OU (2), and then right-click on it.
4. From the contextual menu that appears, click the option for **Create a GPO in this domain, and Link it here...** (3).
5. You will now see the **New GPO** dialog box, as shown in the following screenshot:

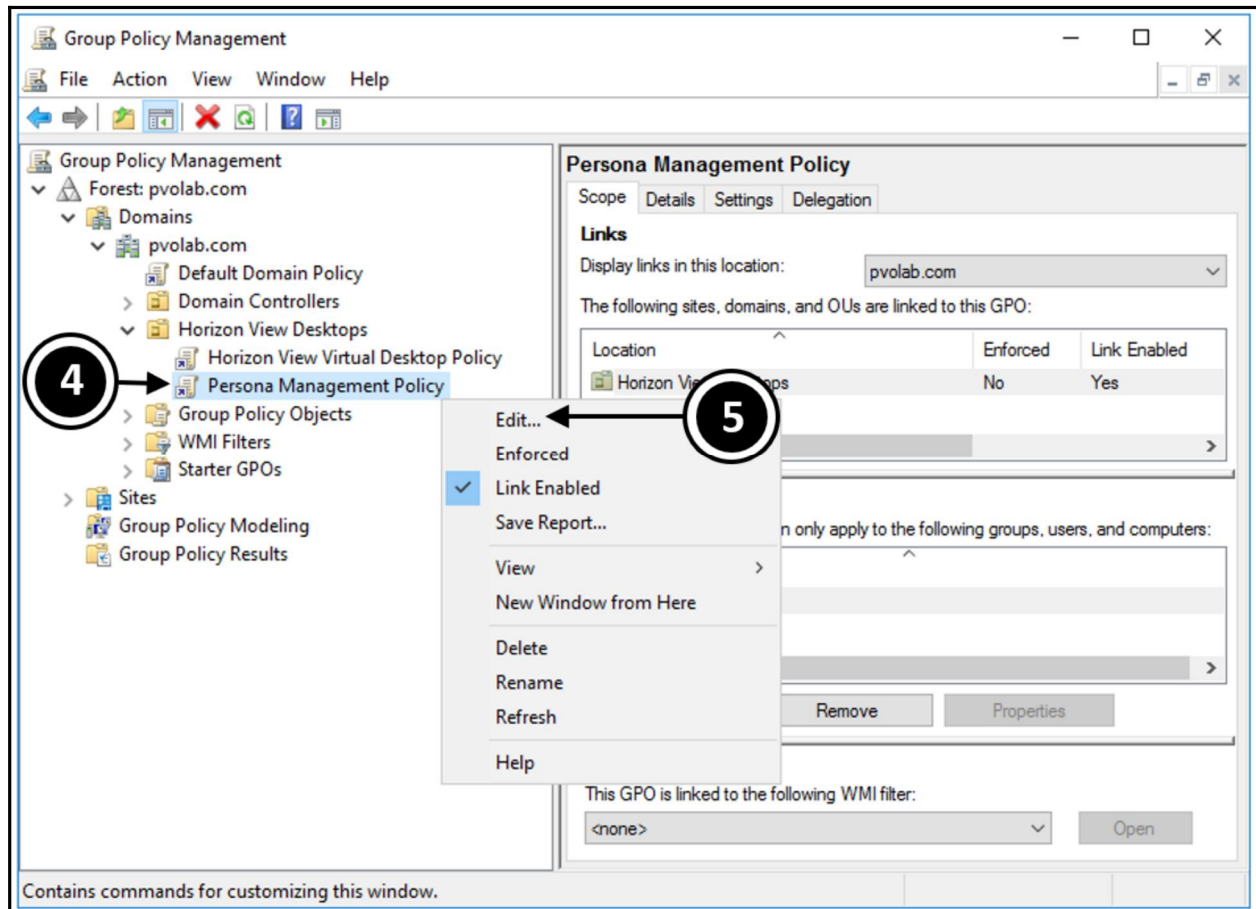


6. In the **Name** box, type in the name for this policy. In the example lab, we have called this Persona Management Policy.
7. Click **OK**.
8. You will now return to the **Group Policy Management** screen, which will show the newly created policy, as shown in the following screenshot:

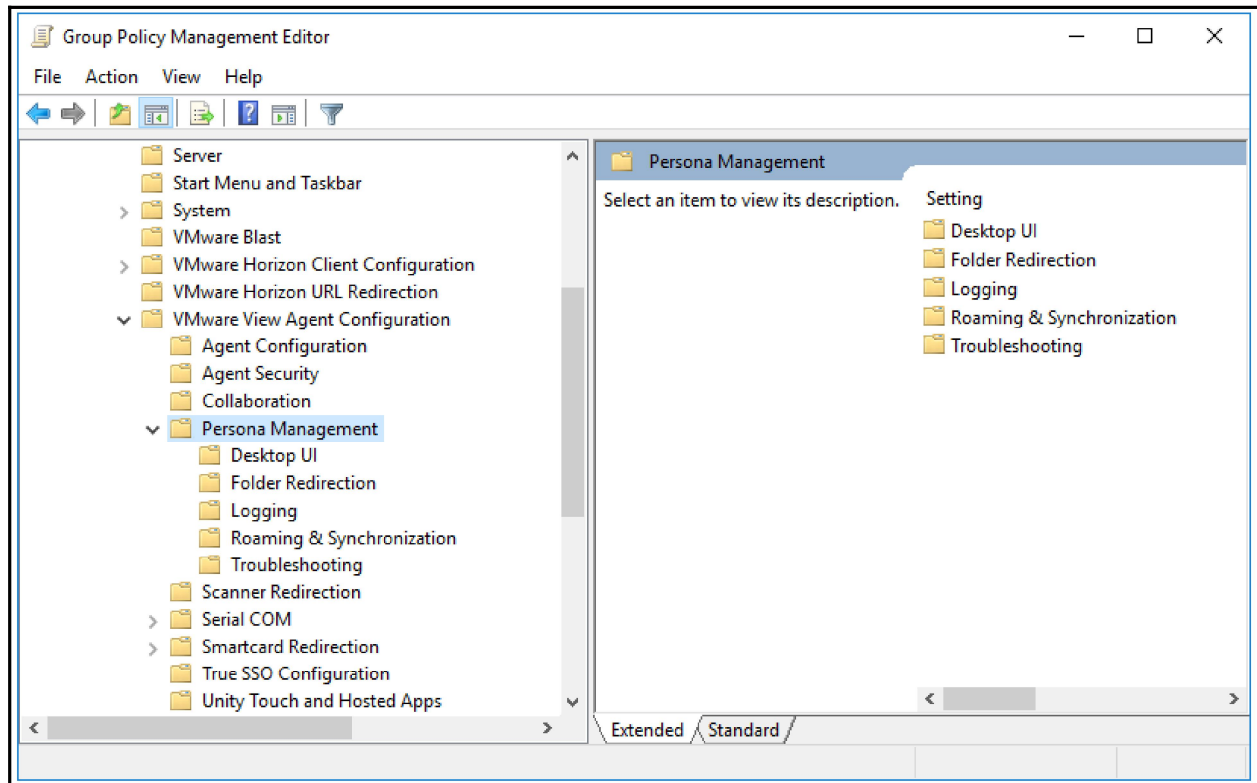


Next, we need to edit the newly created Persona Management policy so that we can configure the specific policy options:

1. To edit the policy, from the **Group Policy Management** screen, click and highlight the **Persona Management Policy** (4).
 1. Right-click and from the contextual menu that appears, click **Edit...** (5), as shown in the following screenshot:



You will now see the **Group Policy Management Editor** screen. If you expand out the Computer Configuration section, and then Policies, Administrative Templates Policy definitions, and then VMware View Agent Configuration, you will see the folder that contains the Persona Management policy settings, as shown in the following screenshot:



You will see the five sections for the different configuration options for Persona Management, which are as follows:

- Desktop UI
- Folder Redirection
- Logging
- Roaming & Synchronization
- Troubleshooting

In the next section, we will walk through configuring these options to set up Persona Management.

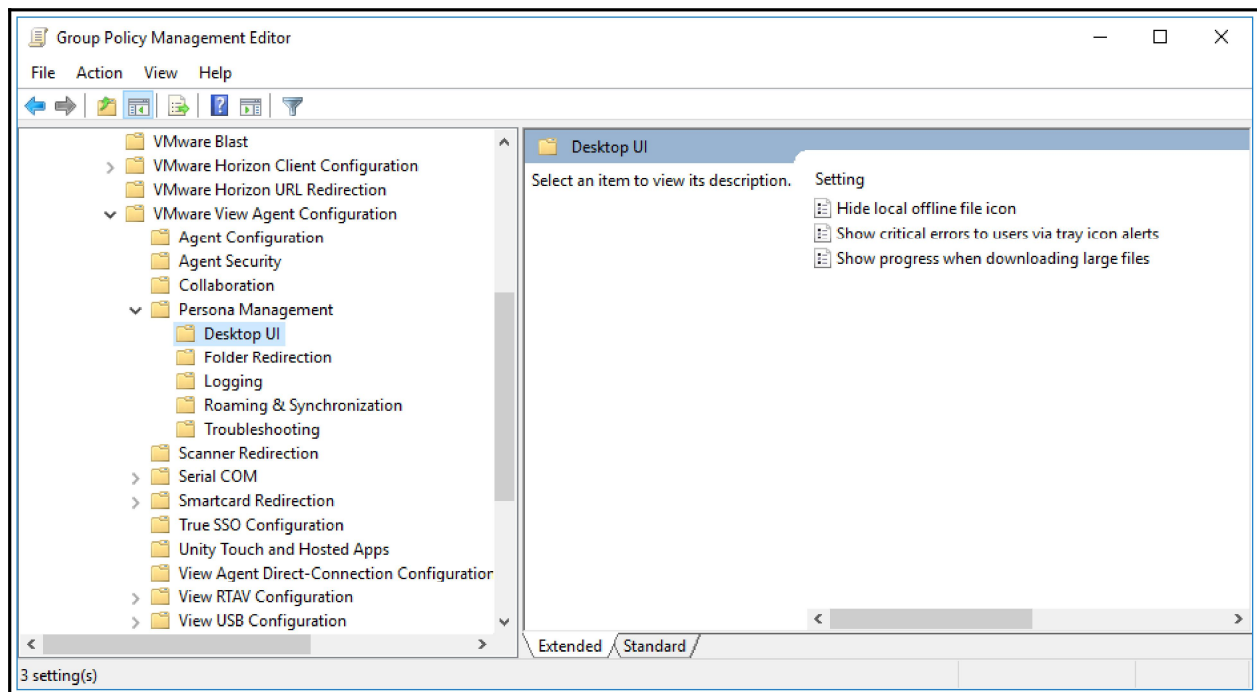
Configuring Persona Management policy options

In this section, we will cover the five Persona Management configuration options in more detail and show how to configure some of the policies, starting with the Desktop UI policy settings.

Desktop UI policy configuration options

In the Desktop UI category of our Persona Management policy settings, you can configure Desktop UI options such as hiding icons or progress bars. It's all about the desktop interface:

1. To configure the Desktop UI policy settings, expand out the Computer Configuration section, and then Policies, Administrative Templates Policy definitions, VMware View Agent Configuration, and then finally the Persona Management folder.
2. Now click on the Desktop UI folder, as shown in the following screenshot:

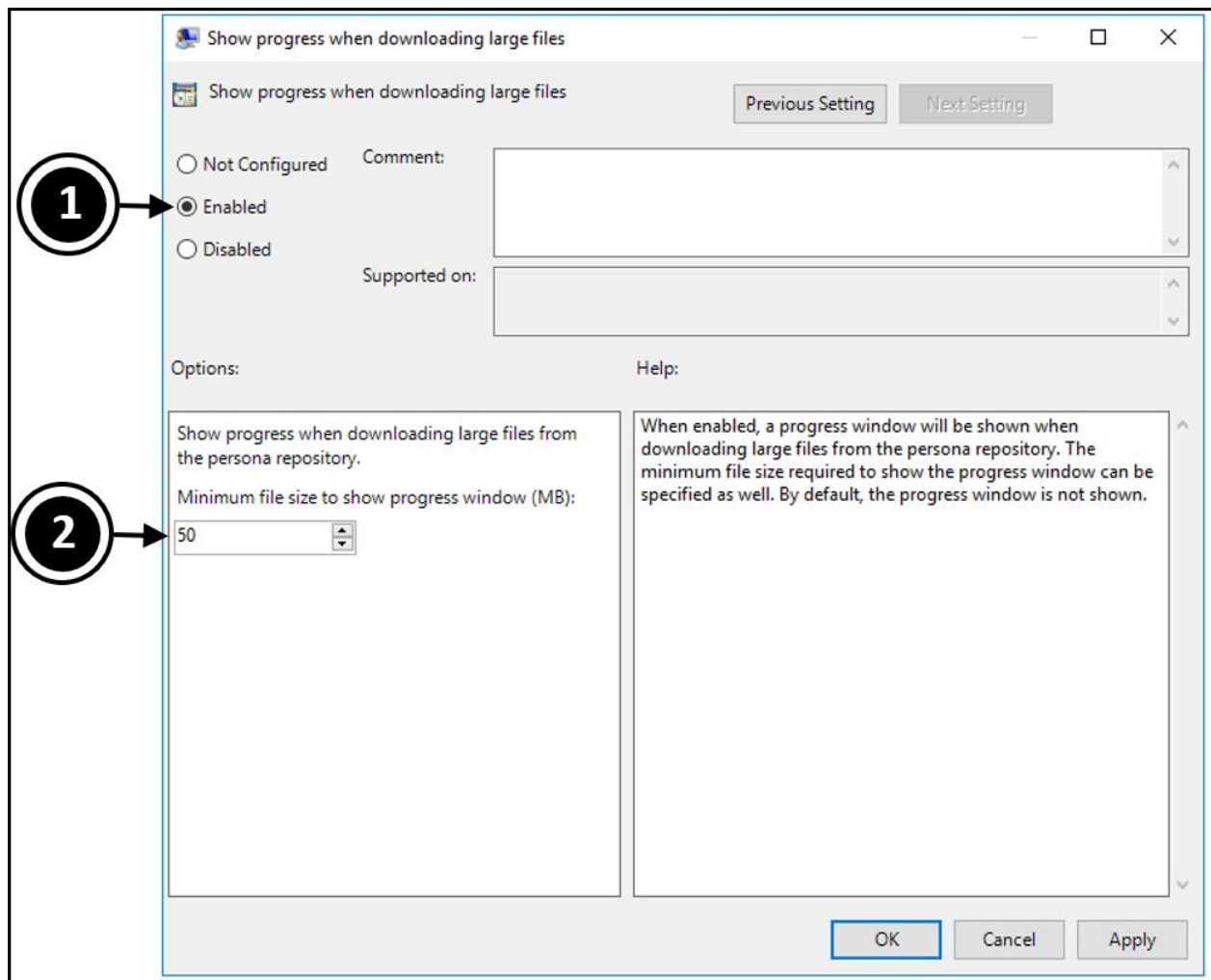


3. You will see the policy options in the right-hand window pane. There are three options that you can configure:
 - **Hide local offline file icon:** This simply hides the tray icon from the user.
 - **Show critical errors to users via tray icon alerts:** This will pop up an alert if the synchronization process fails.
 - **Show progress when downloading large files:** This displays a progress bar when a large file is downloaded.

The configuration options for the first two of these policies is simply to enable or disable it by clicking the appropriate radio button for **Enable** or **Disable**. There are no other configuration settings.

However, in addition to enabling or disabling the **Show progress when downloading large files** policy, there are some additional configuration options, which we will take a closer look at by following the steps described:

4. Double-click the policy to launch the configuration screen, as shown in the following screenshot:



First, click the **Enabled** radio button (1) to turn the policy on. This option allows you to configure a minimum file size (2) for when the progress bar should be displayed. For example, if you set this option to 100 MB and then download an 80 MB file, then the progress bar will not be displayed. However, if you download a 120 MB file, then you will see the progress bar.

In another example, if you download a 50 MB file and a 60 MB file at the same time, individually, they would not be displayed on the progress bar. However, the sum of both files would mean that you have exceeded the set limit of 100 MB that was set, and so, you would see the progress bar.

The next policy settings we are going to look at are for configuring Folder Redirection.

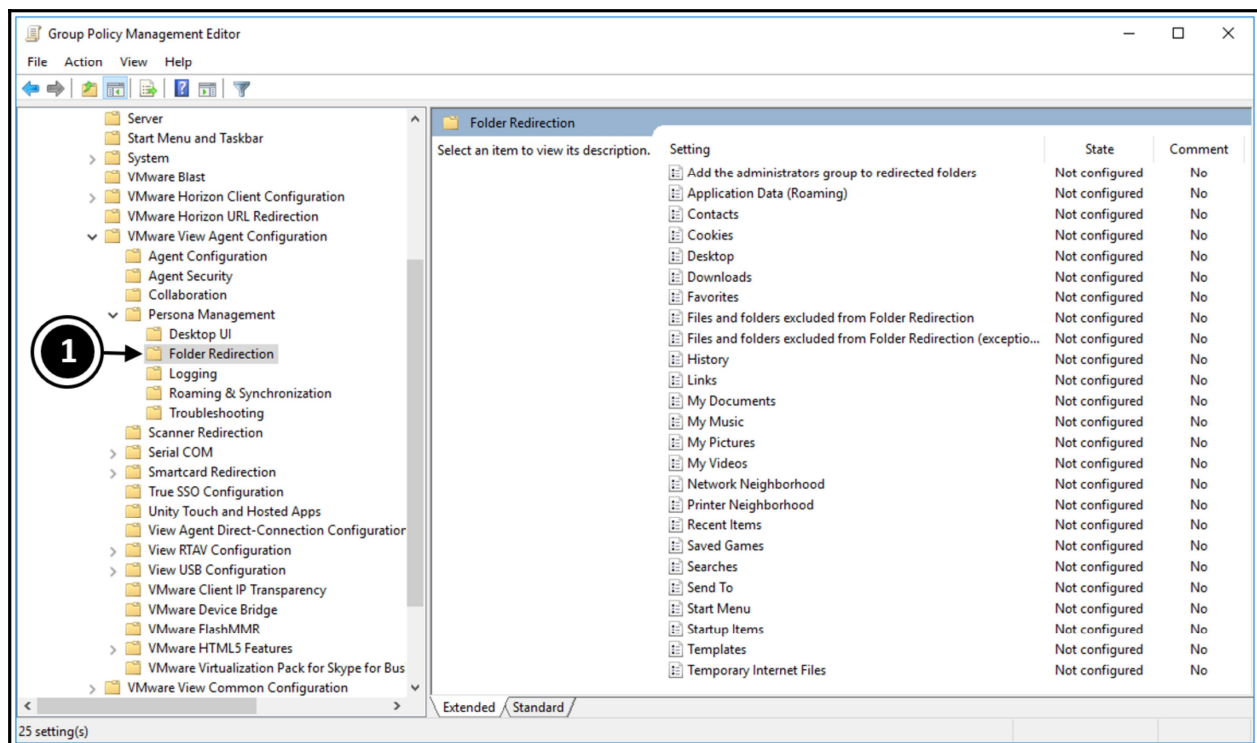
Folder Redirection policy configuration options

With Folder Redirection, you can specify which folders get synchronized to the central repository on the file server. This data is stored directly on the network share during the user session.

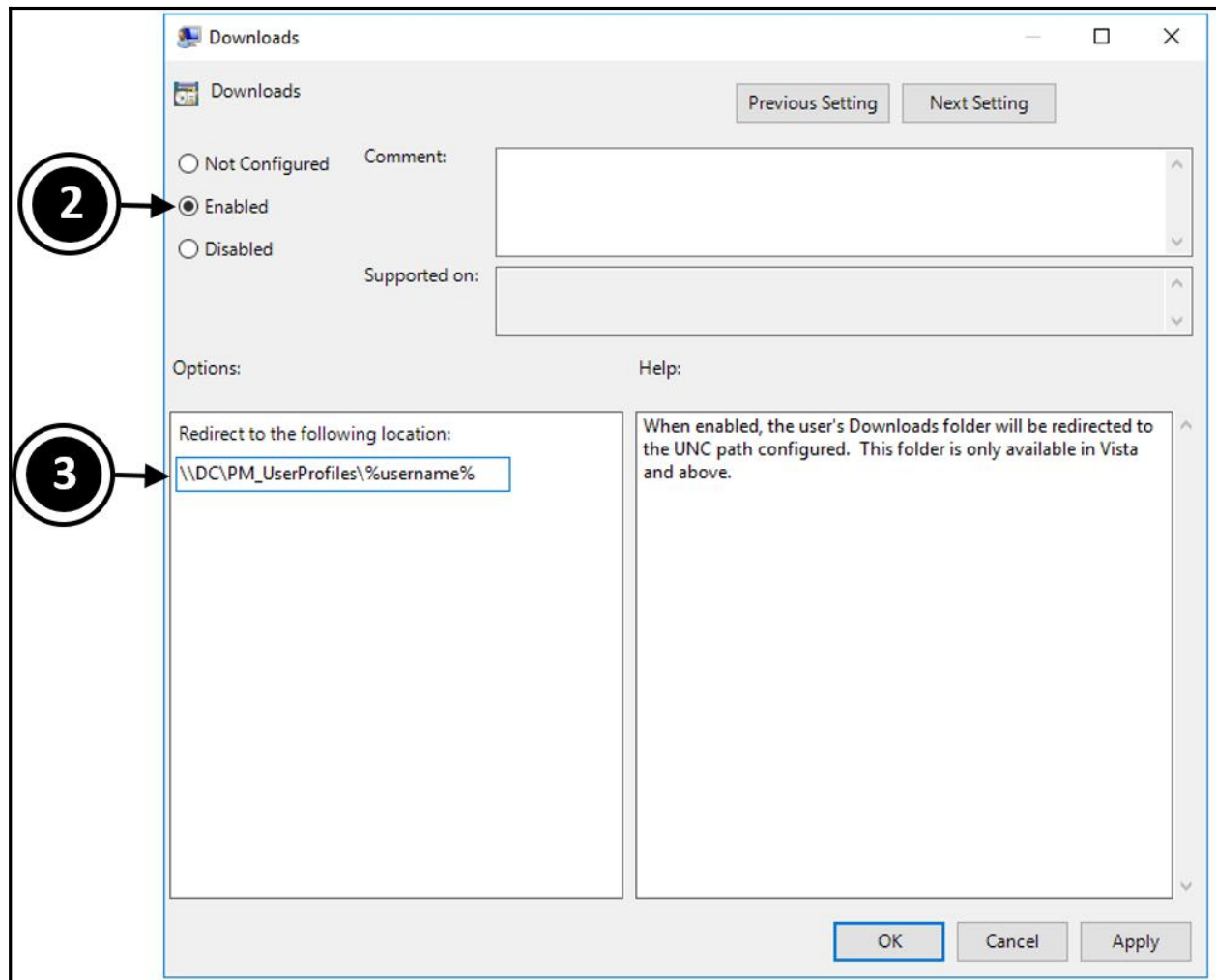
One of the use cases for Folder Redirection is for high availability and backup functions. In this example, we are going to configure the folders that contain critical data so that they are regularly synchronized with the central repository. When you configure which of the folders to redirect, you can also decide which ones remain local to the virtual desktop machine.

You can also choose to redirect different folders to different shared folders:

1. Expand out the Computer Configuration section, and then Policies, Administrative Templates Policy definitions, VMware View Agent Configuration, and then finally the Persona Management folder.
2. Now click on the Folder Redirection folder (1), as shown in the following screenshot:



3. You will see the policy options displayed in the right-hand pane.
As you can see, there are a number of folder redirection policy options you can configure. We are not going to go through all of them in detail and show the configuration for each one; however, we will describe what each one does. As an example, we are going to configure the policy for **Downloads** just to demonstrate the process, as each one is pretty much identical in the way you configure it. To configure this policy, follow the steps as described:
4. Double-click on the **Downloads** option from the right-hand pane. You will now see the **Downloads** configuration box, as shown in the following screenshot:



5. Click the radio button for **Enabled (2)** to switch this policy on and apply it. Now you need to enter the path to which we want to redirect the Downloads folder.
6. In the **Redirect to the following location** box (3), enter the path to the shared folder that we configured earlier, but this time, we will add to the end of the path so that we create and redirect folders to a unique folder for each user. To do this, we will use the %username% variable.
7. So, for the example lab, you would enter \\DC\PM_UserProfiles\%username% to create a unique folder for each user within the profile folder itself.
8. You will then need to repeat this process for any other folders that you want to redirect. As mentioned in the previous section, you could actually set up multiple shared folders and configure different folders to be redirected to different repositories on the server or even different servers.

As you can see from the `Folder Redirection` policy settings, there are a number of configurable policy settings. These are described as follows:

- **Add the administration group to redirected folders:** When enabled, the administrator's group will be added to each redirected folder. The default setting is for end users to have exclusive rights.
- **Application Data (Roaming):** Redirects the user's roaming `Application Data` folder to the path location that you configure.
- **Contacts:** Redirects the user's `Contacts` folder to the path location that you configure.
- **Cookies:** Redirects the user's `Cookies` folder to the path location that you configure.
- **Desktop:** Redirects the user's `Desktop` folder to the path location that you configure.
- **Downloads:** Redirects the user's `Downloads` folder to the path location that you configure.
- **Favorites:** Redirects the user's `Favorites` folder to the path location that you configure.
- **Files and folders excluded from Folder Redirection:** The selected file and folder paths will not be redirected. You have the ability to enter the files and folders you want to exclude. For example, you might want to exclude a PST file due to its size.

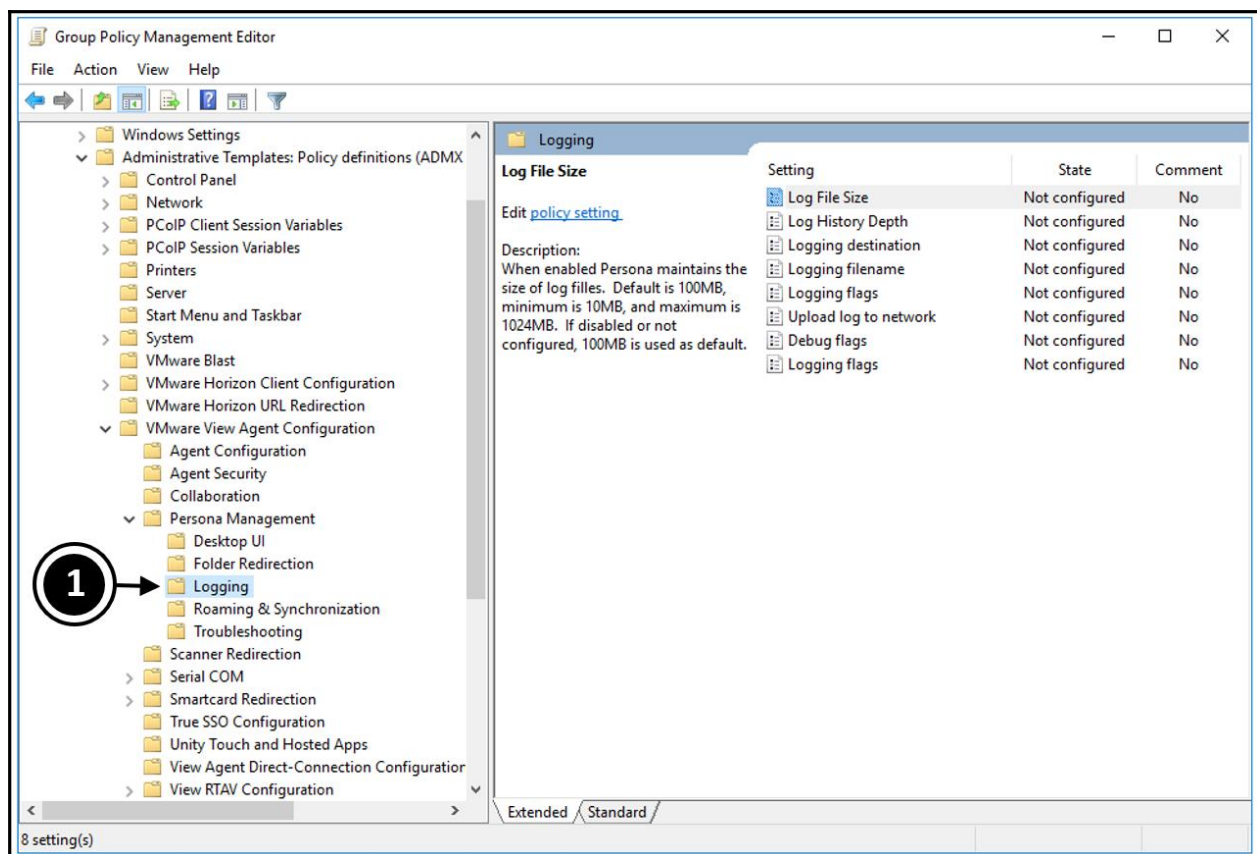
- **Files and folders excluded from Folder Redirection (exceptions):** The file and folder paths that are selected are exceptions to the paths listed in the **Files and folders excluded from Folder Redirection** policy described previously. You can specify a folder in the previous policy and then specify a file within that folder so that it is not redirected.
- **History:** Redirects the user's `History` folder to the path location that you configure.
- **Links:** Redirects the user's `Links` folder to the path location that you configure.
- **My Documents:** Redirects the user's `My Documents` folder to the path location that you configure.
- **My Music:** Redirects the user's `My Music` folder to the path location that you configure.
- **My Pictures:** Redirects the user's `My Pictures` folder to the path location that you configure.
- **My Videos:** Redirects the user's `My Videos` folder to the path location that you configure.
- **Network Neighborhood:** Redirects the user's `Network Neighborhood` folder to the path location that you configure.
- **Printer Neighborhood:** Redirects the user's `Printer Neighborhood` folder to the path location that you configure.
- **Recent Items:** Redirects the user's `Recent Items` folder to the path location that you configure.
- **Saved Games:** Redirects the user's `Saved Games` folder to the path location that you configure.
- **Searches:** Redirects the user's `Searches` folder to the path location that you configure.
- **Send To:** Redirects the user's `Send To` folder to the path location that you configure.
- **Start Menu:** Redirects the user's `Start Menu` folder to the path location that you configure.
- **Startup Items:** Redirects the user's `Startup Items` folder to the path location that you configure.
- **Templates Folder:** Redirects the user's `Templates` folder to the path location that you configure.
- **Temporary Internet Files:** Redirects the user's `Temporary Internet Files` or `cache` folder to the path location that you configure.

We have now covered all the folder redirection policy settings. In the next section, we are going to discuss the policy configuration options for logging.

Logging policy configuration options

The logging policy allows you to configure how the log files are managed. These options include settings such as the size of the log file and where to upload it to. To configure these policy options, follow the steps as described:

1. Expand out the Computer Configuration section, and then Policies, Administrative Templates Policy definitions, VMware View Agent Configuration, and then finally the Persona Management folder.
2. Now click on the Logging folder (1), as shown in the following screenshot:



You then have the different policy configuration options shown in the right-hand pane, which are described as follows:

- **Log File Size:** This setting manages the size of the Persona Management log files. The default setting is 100 MB, with a minimum setting of 10 MB, and a maximum setting of 1024 MB. If the policy is disabled or you don't configure it, then the default setting is used as the configured size.
- **Log History Depth:** This setting manages the Persona Management archive of historical log files. The default setting is 1. The minimum setting is 1, and the maximum setting is 10. If the policy is disabled or you don't configure it, then Persona Management only keeps 1 historical log file.
- **Logging destination:** This setting helps us to understand where the log messages will be sent to. Log messages can be sent to a local log file or the debug port. The default setting is to ensure that the log messages are sent to the log file.
- **Logging filename:** This is the full pathname of the local View Persona Management log file. The path should also include the filename.



If you enable the logging filename policy and leave the pathname field blank, then the log file will be saved to `ProgramData\VMware\VDM\logs\VMWVvp.txt`. Also, don't use a UNC path for the pathname.

- **Logging flags:** Specifies the type of log messages that are generated. If this setting is disabled or not configured, log messages are set to the information level.
- **Upload log to network:** This uploads the log file to the specified network share when the user logs off. The path to the shared folder must be entered as a UNC path and already be created, as Persona Management will not create the shared folder.

- **Debug flags:** This helps us identify the type of debug messages that get created. Debug messages are managed similarly to log messages and, by default, these messages are turned off. You can choose from the following debug options:

<input type="checkbox"/> Debug error messages.
<input type="checkbox"/> Debug IRQL messages.
<input type="checkbox"/> Debug port messages.
<input type="checkbox"/> Debug process messages.
<input type="checkbox"/> Debug registry messages.
<input type="checkbox"/> Debug information messages.
<input type="checkbox"/> Debug directory messages.
<input type="checkbox"/> Debug stream context messages.
<input type="checkbox"/> Debug create messages.
<input type="checkbox"/> Debug offline file table messages.
<input type="checkbox"/> Debug user table messages.
<input type="checkbox"/> Debug alt path messages.
<input type="checkbox"/> Debug registry filter messages.
<input type="checkbox"/> Debug oplock messages.
<input type="checkbox"/> Debug impersonation messages.
<input type="checkbox"/> Debug name provider messages.
<input type="checkbox"/> Debug lock control messages.
<input type="checkbox"/> Debug set info messages.
<input type="checkbox"/> Debug offline files messages.
<input type="checkbox"/> Debug status log messages.

- **Logging flags:** Helps to identify the type of log messages that are generated. By default, log messages are set to information level. You can choose from the list of options.

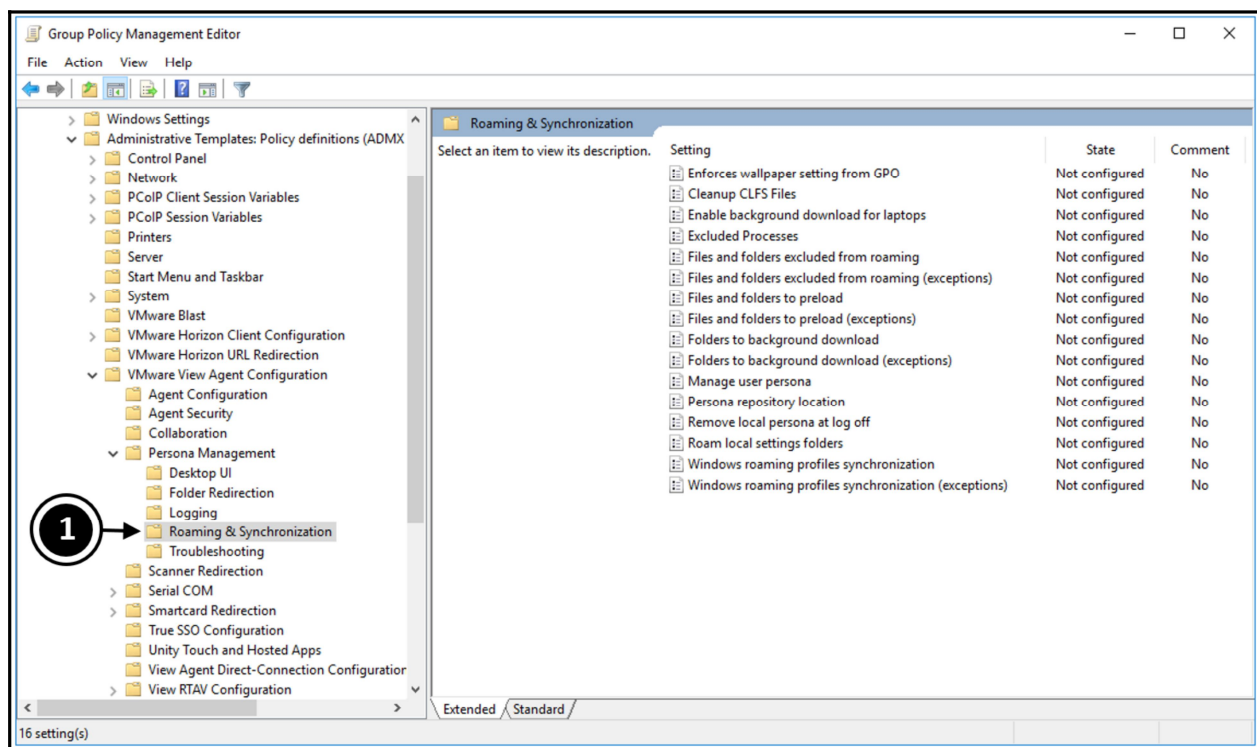
We have now covered all the logging policy settings. In the next section, we are going to discuss the policy configuration options for roaming and synchronization.

Roaming and synchronization policy configuration options

Under this category heading, the policies are all about how files, folders, and user profiles are handled. We will walk through each one and explain what it does, starting with manage user persona.

To configure these policy options, follow the steps as described:

1. Expand out the Computer Configuration section, and then Policies, Administrative Templates Policy definitions, VMware View Agent Configuration, and then finally the Persona Management folder.
2. Now click on the Roaming & Synchronization folder (1), as shown in the following screenshot:



You then have the different policy configuration options shown in the right-hand pane, which are described as follows:

- **Enforces wallpaper setting from GPO:** This policy enforces the desktop wallpaper to be updated based on the **Group Policy Object (GPO)** setting. The policy does not apply if the desktop wallpaper is not set through the GPO.
- **Cleanup CLFS Files:** This will delete files generated by the **Common Log File System (CLFS)**, so `ntuser.dat` and `usrclass.dat` get deleted from the roaming profile when a user logs on. CLFS is part of the Windows OS and is used to create transaction logs and metadata used to access log data. This gets stored in the `Users` folder on the `C:` drive of the machine along with user-level registry information so that we can now manage this with `Persona Management`. Only use this option to repair profiles that are experiencing a problem with these files.
- **Enable background download for laptops:** When enabled, all files in the local profile will be downloaded after a user logs on to a laptop. This option is not for a virtual desktop environment; as it says, it's for a laptop computer. You might well ask, "*Then why is it part of a virtual desktop Persona Management solution?*" Good question. The answer is because `Persona Management` can also be used on physical desktops and laptop computers. We will cover this later in this chapter.
- **Excluded Processes:** Excluded processes are processes where the I/O is disregarded by `Persona Management`. For example, you may want to exclude things such as anti-virus scanning as the scanning process could impact the performance of the virtual desktop machines. Any changes to files and settings in a user profile, made by excluded processes, are still duplicated as part of the profile.
- **Files and folders excluded from roaming:** If you apply this setting, the file and folder paths that are selected and configured will not be replicated with the user's persona. Within a user's persona, there are a few use cases that require specific folders and files to only be available on the local machine, such as temporary or cached files, which are not required to be replicated to the central repository.
- **Files and folders excluded from roaming (exceptions):** With this setting, the selected file and folder paths are exceptions to the paths specified in the **Files and folders excluded from roaming** policy described previously.

- **Files and folders to preload:** This setting allows you to select file and folder paths that get downloaded when the user logs on, and are replicated when files are changed. You can also specify exceptions within these paths in the **Files and folders to preload (exceptions)** policy. In some cases, you may require specific files and folders to be preloaded into the user's locally stored persona. These files will be downloaded from the persona repository when the user logs in.

If you remember how Persona Management works, folders and data only get loaded to the virtual desktop machine when the user requests them. The preload option means we can choose a set of files and folders that automatically get loaded onto the virtual desktop machine at login time, rather than on demand. You might want to do this if there are specific folders that you know a particular user is always going to need. It might be a company-wide folder that everyone uses, which makes it quicker if it gets loaded at login rather than everyone requesting it at once. Choosing this option might mean it would take longer for the login process while the files and folders complete the preload download.

- **Files and folders to preload (exceptions):** The selected file and folder paths configured in this setting are exceptions to the paths specified in the **Files and folders to preload** policy described previously.
- **Folders to background load:** After a user has logged on, the configured folder paths get downloaded in the background. You can optimize the login speed of the virtual desktop machine by downloading the specific folders in the background, meaning that users don't need to wait for large downloads to complete while logging on or when they launch an application that requires them.
- **Folder to background load (exceptions):** This setting configures the selected folder paths. These folder paths are exceptions to the ones listed in the **Folders to background download** policy described previously.
- **Manage user persona:** This setting basically switches Persona Management on or off. When it is disabled, Windows manages the user's persona.
- **Persona repository location:** This is the UNC path that points to the repository of where user profiles will be stored. If you leave this setting blank, then the user profile path in Active Directory will be used. In the example lab, the path to the share is `\\DC\PM_UserProfiles`.

- **Remove local persona at log off:** This setting removes the user's locally stored persona when they log off. When the persona is removed, you can also consider deleting a user's local settings folders. The default setting is to not delete the locally stored profile when the user logs off.
- **Roam local settings folder:** The local settings folders will be roamed, along with the rest of the user's profile. By default, local settings folders are not roamed.
- **Windows roaming profiles synchronization:** With this setting, the selected file and folder paths will be downloaded when a user logs on and then replicated when they log off. Some use cases require specific files and folders to be managed with traditional Windows roaming profile functionality. These will be downloaded when a user logs in, but not synchronized with the repository until the user logs off.
- **Windows roaming profiles synchronization (exceptions):** The file and folder paths selected here are exceptions to the ones listed in the **Windows roaming profiles synchronization** policy, as described in the preceding setting.

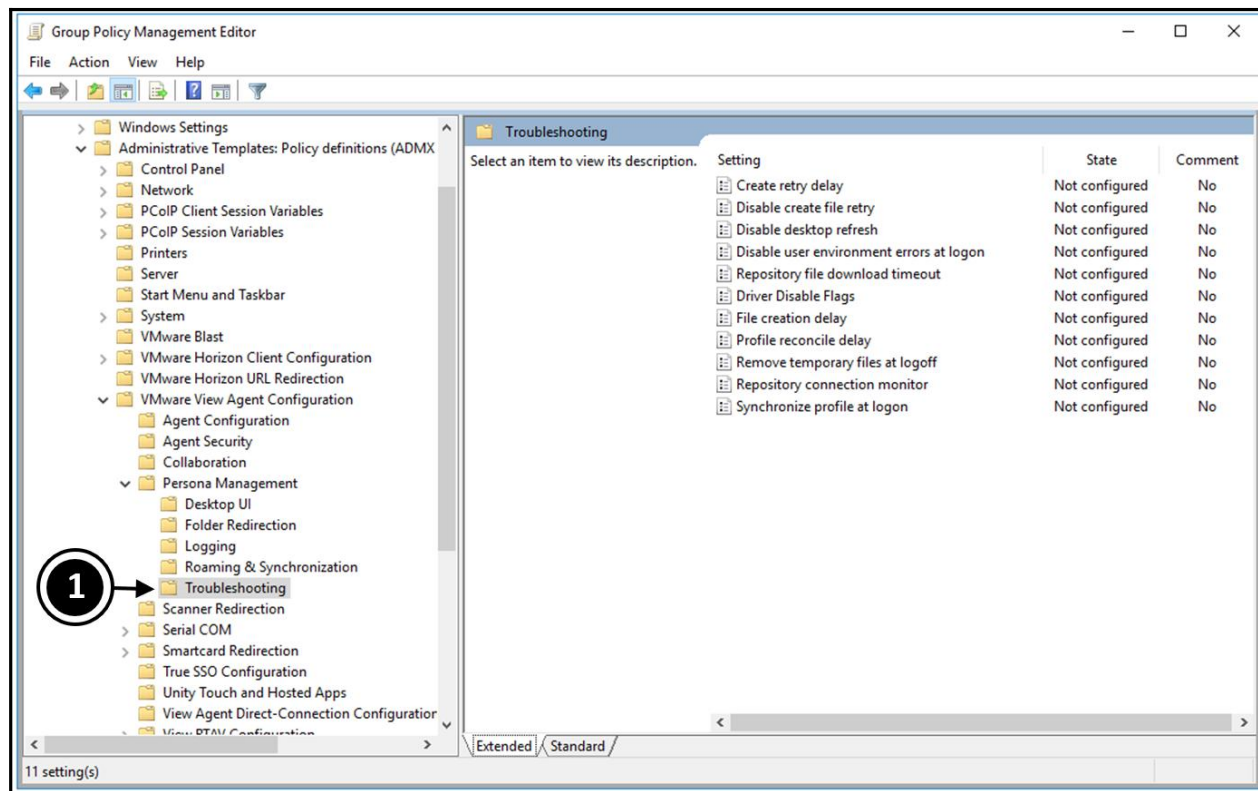
We have now covered all the roaming and synchronization policy settings. In the next section, we are going to discuss the final policy configuration options for troubleshooting.

Troubleshooting policy configuration options

In the troubleshooting policies, you can configure how to manage potential issues with Persona Management by monitoring and setting retry and time delays, for example.

To configure these policy options, follow the steps as described:

1. Expand out the `Computer Configuration` section, and then `Policies, Administrative Templates Policy definitions, VMware View Agent Configuration`, and then finally the `Persona Management` folder.
2. Now click on the `Troubleshooting` folder (1), as shown in the following screenshot:



You then have the different policy configuration options shown in the right-hand pane, described as follows:

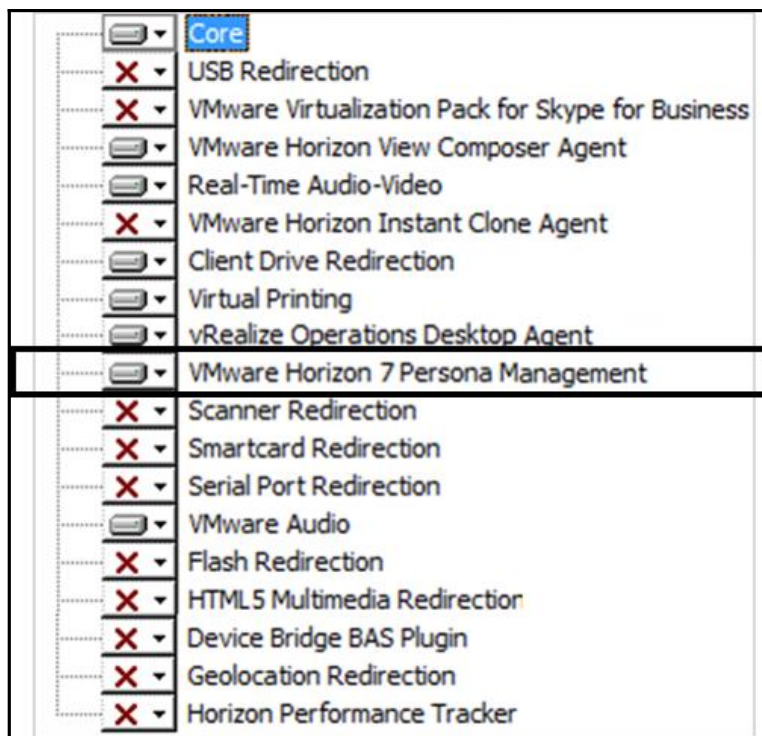
- **Create retry delay:** This allows you to configure a delay in milliseconds between a file creation failure and retrying to create the file again. By default, the delay is set to 500 milliseconds.
- **Disable create file retry:** When enabled, no retry attempt is made after a file creation failure. By default, a retry attempt will be made.
- **Disable desktop refresh:** When enabled, the user's desktop icons are not refreshed after retrieving corresponding .exe files. Enabling this policy may cause icons to not appear on the user's desktop shortcuts if the shortcut points to an executable within the profile, but it will prevent extraneous desktop refreshes. By default, the desktop icons are refreshed.
- **Disable user environment errors at logon:** When enabled, system user environment error messages are disabled during user logons. By default, user environment errors are disabled.

- **Repository file download timeout:** This specifies the time in milliseconds before a download of a file from the remote repository times out. By default, the timeout is 1,800 seconds.
- **Driver Disable Flags:** This allows you to configure driver and service log levels independently.
- **File creation delay:** This indicates the delay in milliseconds between login and the creation of the offline files in the user's profile. By default, the delay is set to 10,000 milliseconds.
- **Profile reconcile delay:** This indicates the delay in seconds between login and starting to reconcile the user's profile. By default, the delay is 10 seconds.
- **Remove temporary files at logoff:** When enabled, files with a `.tmp` file extension will be removed from the user's profile when they log off. View Persona Management uses `.tmp` files for various file synchronization between the local and remote profile. By default, temporary files are removed.
- **Repository connection monitor:** When enabled, View Persona Management will detect when the connection to the persona repository has been lost or performance becomes too slow to synchronize. Once a fast connection is reestablished, all local changes are uploaded and synchronized with the user's remote persona. The frequency at which the network connection is tested and the maximum network latency can be tuned for optimum performance. By default, the test interval is set to 120 seconds and the maximum network latency is set to 40 ms.
- **Synchronize profile at logon:** When enabled, files in the user's local profile are synchronized with the roaming profile when they log on. By default, the user's profile is synchronized when they log on.

We have now completed our overview of the `Persona Management` policy configuration settings options. In order for Persona Management to work on virtual desktop machines, you need to ensure that you have installed it on each virtual desktop machine that you want to manage the user profile on. The Persona Management software is part of the Horizon Agent, and in the next section, we are going to make sure that the Persona Management agent is installed with the Horizon Agent on the virtual desktop machines.

Installing the View Agent for Persona Management

So far in this chapter, we have discussed in detail how to configure the Persona Management policy settings, but what else needs to be installed? Basically, you need to ensure that the Persona Management Agent is on the virtual desktop machines. The Persona Management Agent is one of the options that you need to install when installing the View Agent, as shown in the following screenshot:



During the installation of the Horizon Agent, ensure that you have selected the option to install the Persona Management Agent. We have already covered the installation of the View Agent in [Chapter 7, Building and Optimizing the Virtual Desktop OS](#), so please refer back to that chapter for details on the full installation process for the Horizon Agent.

Installing Persona Management on physical desktops

Persona Management is all about managing a user's profile and data when using the Windows operating system. It makes no difference whether the instance of the Windows desktop operating system is physical or virtual. So, the same is true for the VMware View Persona Management tool. It can be used to manage both virtual desktop machines and physical PCs/laptops.

In this section, we will briefly cover how to install Persona Management on a physical device so that you can manage the user's profile in the same way as you do for the virtual desktop machines in your environment.

The first task you need to perform is to check that you have configured Group Policy for Persona Management on the domain controller. You also need to make sure that you have a separate OU configured for physical devices managed with Persona Management. You don't want to add these physical devices to the existing virtual desktop machine OU as there are a number of other policy settings that do not apply to physical devices.

You then need to install the Persona Management agent onto the device. As part of the Horizon View software download bundle, you will see an installer file for Persona Management.

So, let's get on with the installation of Persona Management on a physical desktop:

1. Locate the installation file, and double-click to launch it. In the example lab, the file is located in the shared software folder, and is called `VMware-Horizon-Persona-Management-x86_64-7.6.0-9539447`, as shown in the following screenshot:

Name	Date modified	Type	Size
View ADM Templates	05/01/2019 10:03	File folder	
VMware OS Optimization Tool	07/12/2018 08:39	File folder	
VMware-Horizon-Agent-x86_64-7.6.0-9539447	02/11/2018 13:23	Application	225,043 KB
VMware-Horizon-Client-4.10.0-11021086	04/01/2019 16:51	Application	195,669 KB
VMware-Horizon-Connection-Server-x86_64-7.6.0-9823717	02/11/2018 13:26	Application	267,730 KB
VMware-Horizon-Extras-Bundle-4.9.0-9539668	04/12/2018 13:21	Compressed (zipp...	5,347 KB
VMware-Horizon-Persona-Management-x86_64-7.6.0-9539447	02/11/2018 13:25	Application	39,685 KB
VMware-Jmp-Installer-7.6.0-9823717	02/11/2018 13:28	Application	115,462 KB
VMware-viewcomposer-7.6.0-9491669	02/11/2018 13:27	Application	47,011 KB

2. You will now see the **Welcome to the VMware Horizon View Persona Management Setup Wizard**.
3. Click the **Next >** button to continue the installation.
4. On the **End-User License Agreement** page, check the box to accept the terms.
5. Click the **Next >** button to continue the installation.
6. There are no configuration or setup options when installing Persona Management. So, click on **Install** to start the installation and copy the Persona Management files.
7. Once the installation is complete, you will see a dialog box that will prompt you to reboot the machine. Click the **Yes** button to reboot the machine.
8. The installation of Persona Management is now complete.

Once the machine has rebooted and is back up and running, check that Persona Management is running. To do this, click on **Start** and then on **Run**. Then, in the **Run** dialog box, type `services.msc` to open the services management screen. Scroll down until you see the entry for **VMware Horizon View Persona Management**, and check that it is running.

The next test is to see whether it is actually working and is managing the user's profile and that files are syncing to the central repository on the file server.

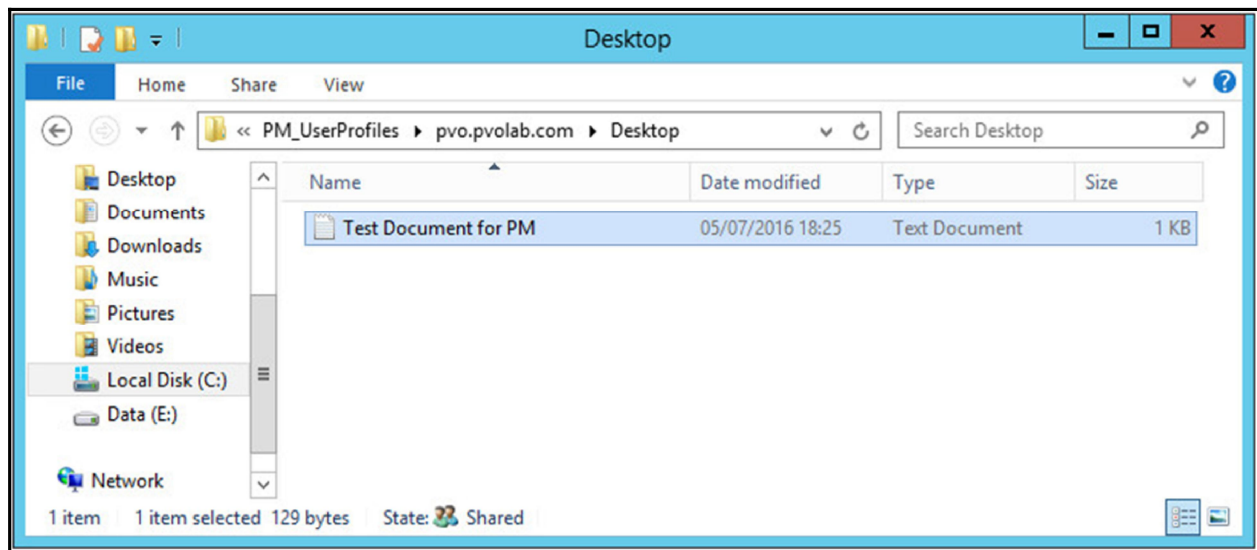
Testing Persona Management

Now that Persona Management is up and running in the environment, you should make sure that it is working correctly by testing it with one of the end users.

To do this, we will log in as a user and make sure the files and folders that we selected in the policy section of this chapter are being redirected. In the example lab, we have logged on to a virtual desktop machine as the user `PVO` and created a test document called `Test Document for PM`, and saved it on the desktop of the virtual desktop machine, as we have configured the desktop to be redirected when we discussed the various policy options and configuration settings.

To check whether Persona Management is working, we will now switch back to the server that is hosting the central repository and make sure the user's folder has been created and that files have been redirected, as per the policy we configured:

1. On the server hosting the Persona Management central repository, open Windows Explorer and navigate to the shared folder that was configured earlier in this chapter to store user profiles and data. This folder is called `PM_UserProfiles`.
2. In the path to the shared folder, you will now see that the username that we logged in as for the test, `PVO`, is now part of the path. This is down to the path name that we configured being appended with the `%username%` variable.
3. Now, if you click and open the `Desktop` folder, you can see the text document that was created and saved on the desktop of the virtual desktop machine has now been synchronized with the folder in the central repository, as shown in the following screenshot:



We have now successfully set up, deployed, and tested View Persona Management in the example lab environment. In the next section, we will take a look at some of the best practices to consider when deploying Persona Management.

Persona Management Best practices

In this section, we will highlight some of the best practices for working with Persona Management. We have covered some of these throughout the chapter, so we will just summarize these.

Removing local user profiles at logout

The default setting for this is that the user profiles do not get deleted when the users log off their desktops. This helps with reducing the amount of I/O. However, if you are using floating virtual desktop machines and they are configured to refresh or delete when a user logs off, then you need to set the **Remove local persona option at log off** to **Disable**. As the virtual desktop machine is refreshed by View anyway, there is no need for Persona Management to do it.

Persona Management and Windows roaming profiles

If you are using Persona Management to manage your Horizon View virtual desktop machine and also using Windows roaming profiles for physical devices, it's best practice to configure different profiles for each environment.

When Active Directory Group Policies are being used to manage this, make sure you enable the Persona repository location policy and select the **Override Active Directory** user profile path.

Configuring redirected folders

When you configure Folder Redirection, ensure that the folder path includes the `%username%` variable added at the end of the redirected folder's name.

In the example lab, this was configured as `\\DC\PM_UserProfiles\%username%\`.

Using antivirus with Persona Management

When using an **antivirus (AV)** application with Persona Management, configure it with the default behavior and ensure you do not set it to scan offline files. If you need to perform a virus scan for the desktop, then you need to make sure that the files and folders are preloaded.

Backing up the central repository

VMware recommends that you use your standard practice when it comes to backing up the shared folder that is used to store the profile repository. Avoid things such as Windows Volume backup services as that could cause data loss or corruption.

Using persistent disks

If you have virtual machine users that create large amounts of data and have a dedicated desktop assignment, then it's best practice to use persistent disks for these particular users.

When you configure a persistent disk, it is used to preserve the user data and settings, even when you run a refresh or recompose using Horizon View Composer. The persistent disk acts as a cache for the user profiles and, therefore, limits the amount of I/O traffic.

However, when you use persistent disks, make sure you set the **Remove local persona at logoff** policy to be disabled. If you do not, then the policy will delete the user data from the persistent disk when a user logs off, regardless of the fact that it's a persistent disk. The Persona Management policy will take precedence.

VMware User Environment Manager

The VMware UEM solution was added to the VMware EUC portfolio in February 2015, when VMware acquired a Dutch company called **Immidio**.

VMware UEM allows you to personalize and dynamically configure policies across Windows desktops running as virtual desktop infrastructure, physical desktops, and cloud-based **desktop-as-a-service (DaaS)** environments.

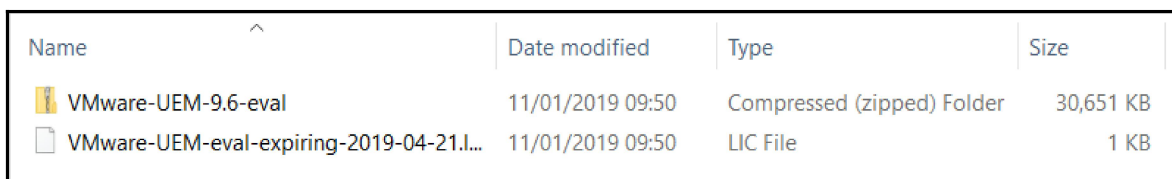
UEM simplifies the management of end user profiles and builds on your existing infrastructure. You are able to manage things such as environmental settings, including network drives and printers. Policies are applied to the end users on demand, as they log in to their desktops.

The UEM solution delivers across the following key areas:

- Application configuration management
- User environment settings
- Personalization
- Application migration
- Dynamic configuration (delivers contextual-based configurations)
- Reduces complex scripting and prevents configuration errors
- Reduces the amount of Group Policies required
- The Centralized Management Console
- Allows management of end user environments at a global level, rather than on an individual basis
- Globally enforces compliance standards
- Increases end user productivity by speeding up login times

So, let's get into the setup and configuration for UEM.

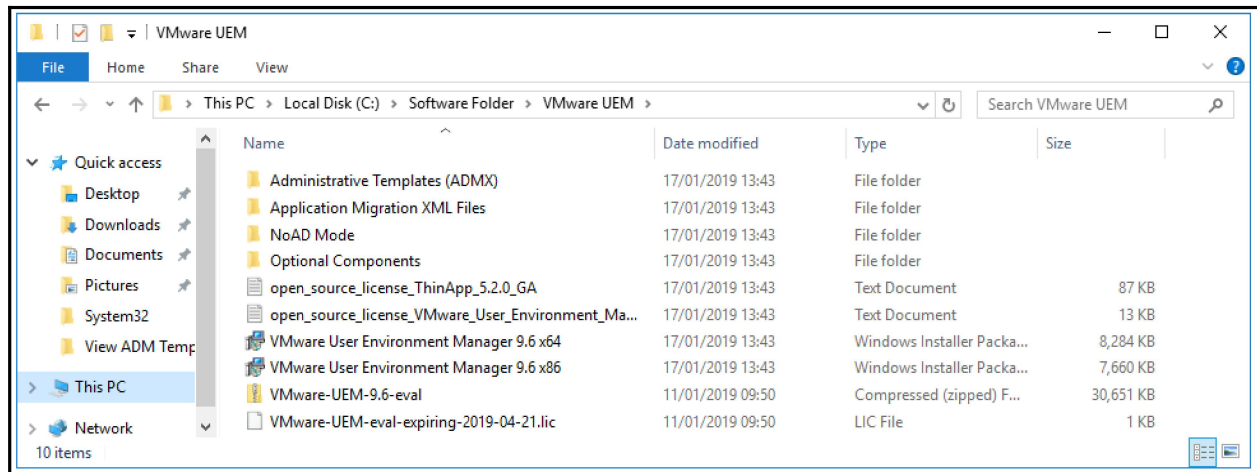
Before we get into the installation and configuration process, you first need to download the UEM software from the VMware website. The UEM software is delivered as a single .zip file, as shown in the following screenshot:



Name	Date modified	Type	Size
VMware-UEM-9.6-eval	11/01/2019 09:50	Compressed (zipped) Folder	30,651 KB
VMware-UEM-eval-expiring-2019-04-21.l...	11/01/2019 09:50	LIC File	1 KB

In the example lab, we have downloaded a trial edition, along with the associated trial license.

Next, extract the .zip file to a shared folder so that you can access the console installer files on other admin machines. In the example lab, we have extracted the files to the shared software folder on the domain controller, as shown in the following screenshot:



Now that you have all the files, you can start the configuration and installation process. The first task is to create two shared folders, as we will discuss in the next section.

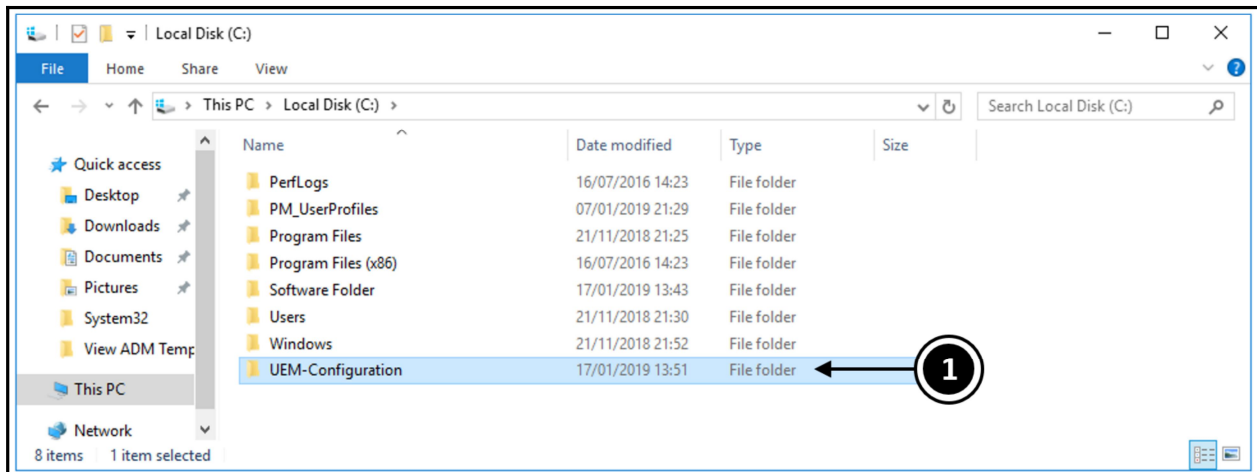
Preparing Active Directory for UEM – Part I

The first task to complete is to create two new shared folders. In the example lab, these will be created on the domain controller. These shared folders are going to be used to store the UEM configuration information and the actual user profile data.

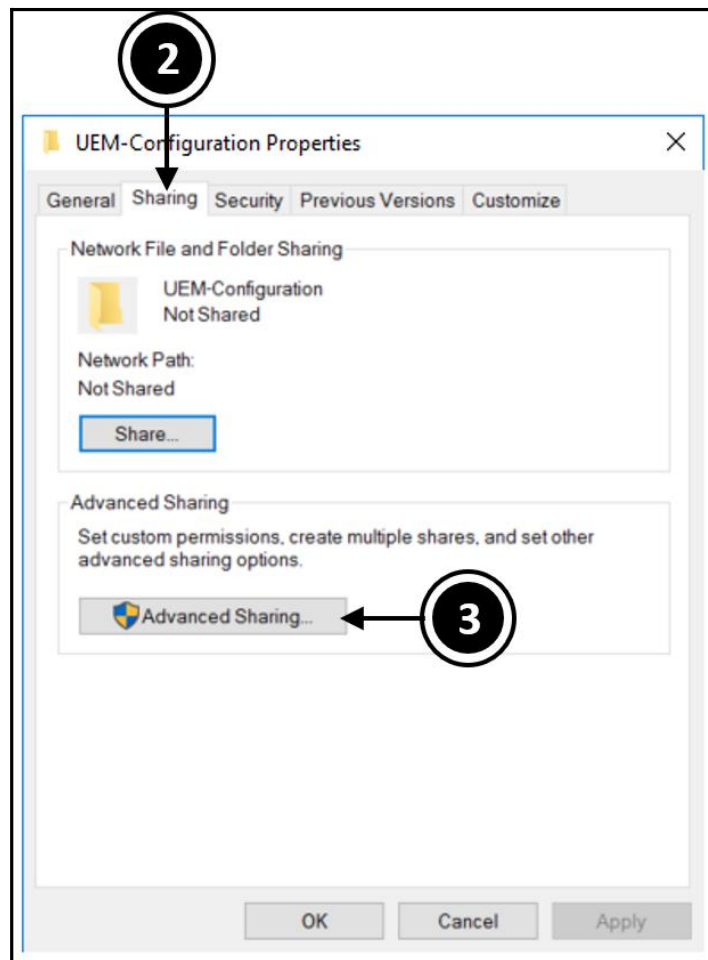
UEM Configuration Share

In this section, we are going to create the shared folder to store the UEM configuration information and then set the permissions for that folder. To do this, follow the steps as described:

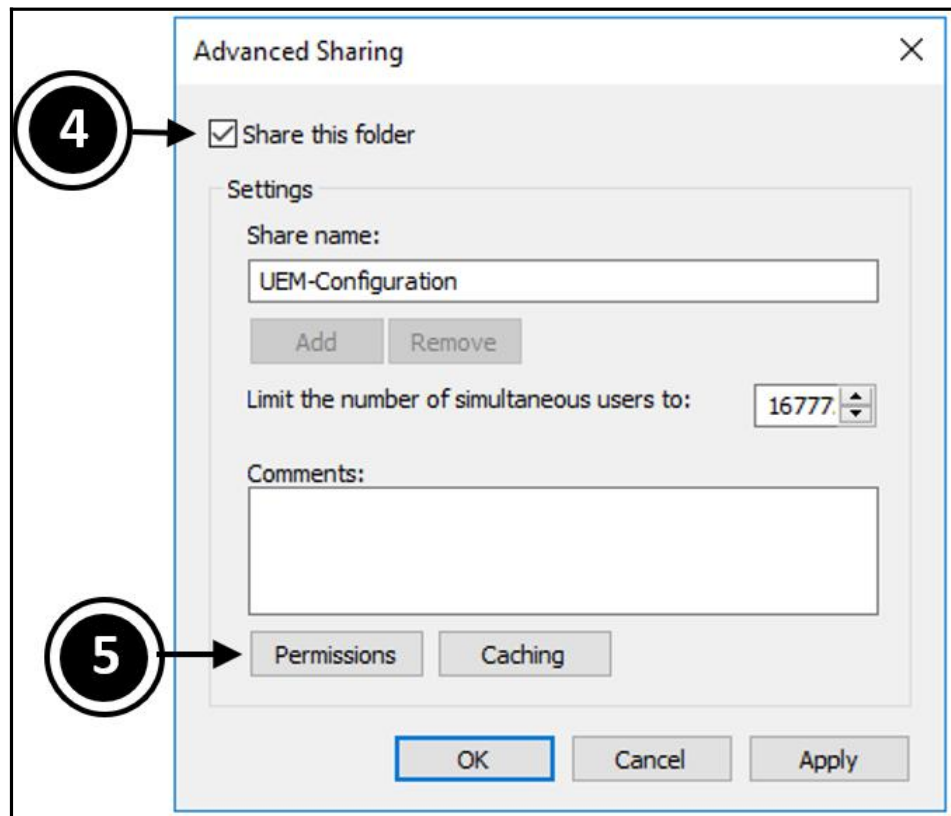
1. Launch Windows Explorer in the file server, or the server you want to store the configuration information on, and create a new folder. In the example lab, we've called this folder `UEM-Configuration (1)`, as shown in the following screenshot:



2. Now, select the UEM-Configuration folder, right-click, and then select **Properties** (2). You will now see the **UEM-Configuration Properties** dialog box, as shown in the following screenshot:

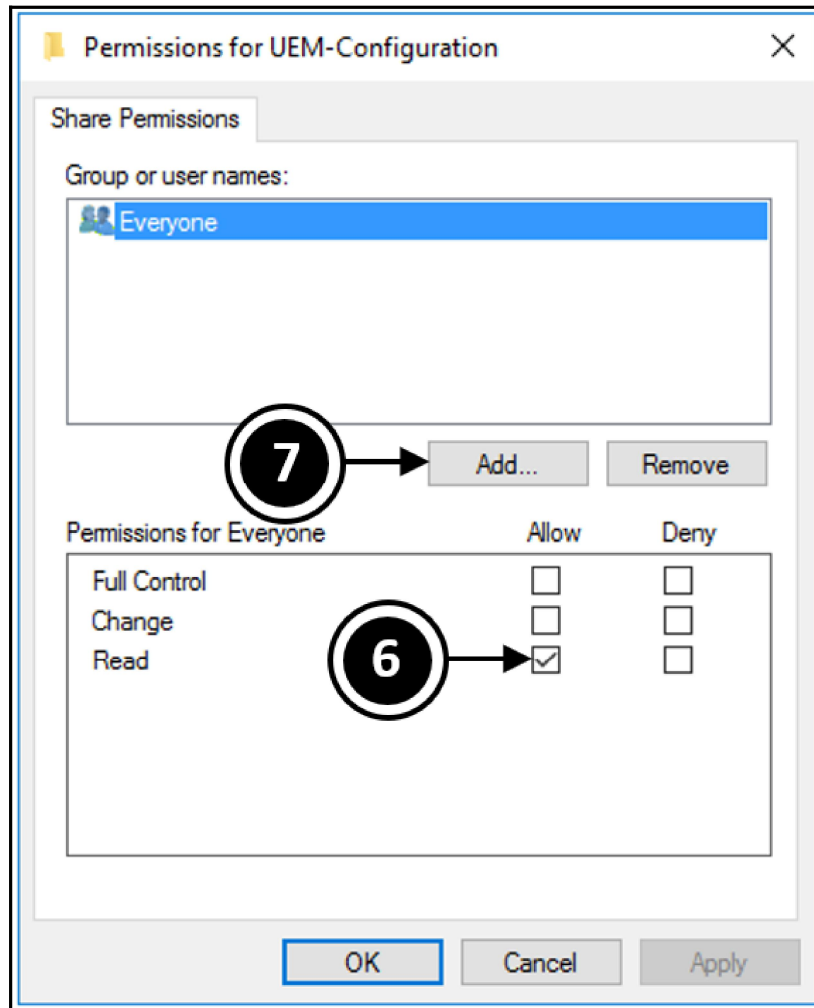


- Click the **Sharing** tab (2), and then click the **Advanced Sharing...** button (3). You will now see the **Advanced Sharing** dialog box, as shown in the following screenshot:

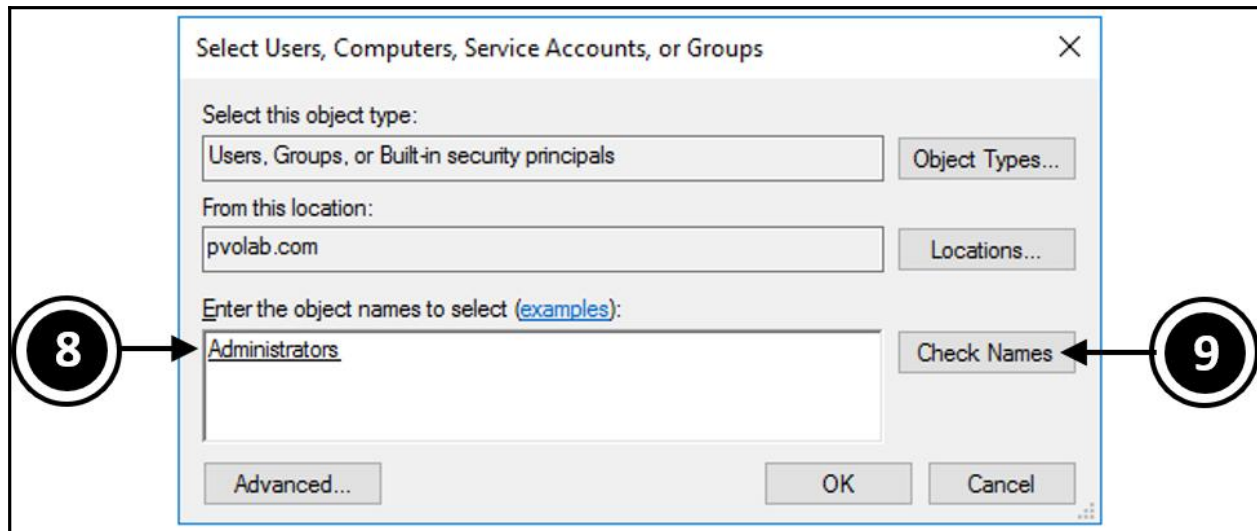


- Check the **Share this folder** tick box (4), and then click the **Permissions** button (5).

5. You will now see the **Permissions for UEM-Configuration** dialog box, as shown in the following screenshot:

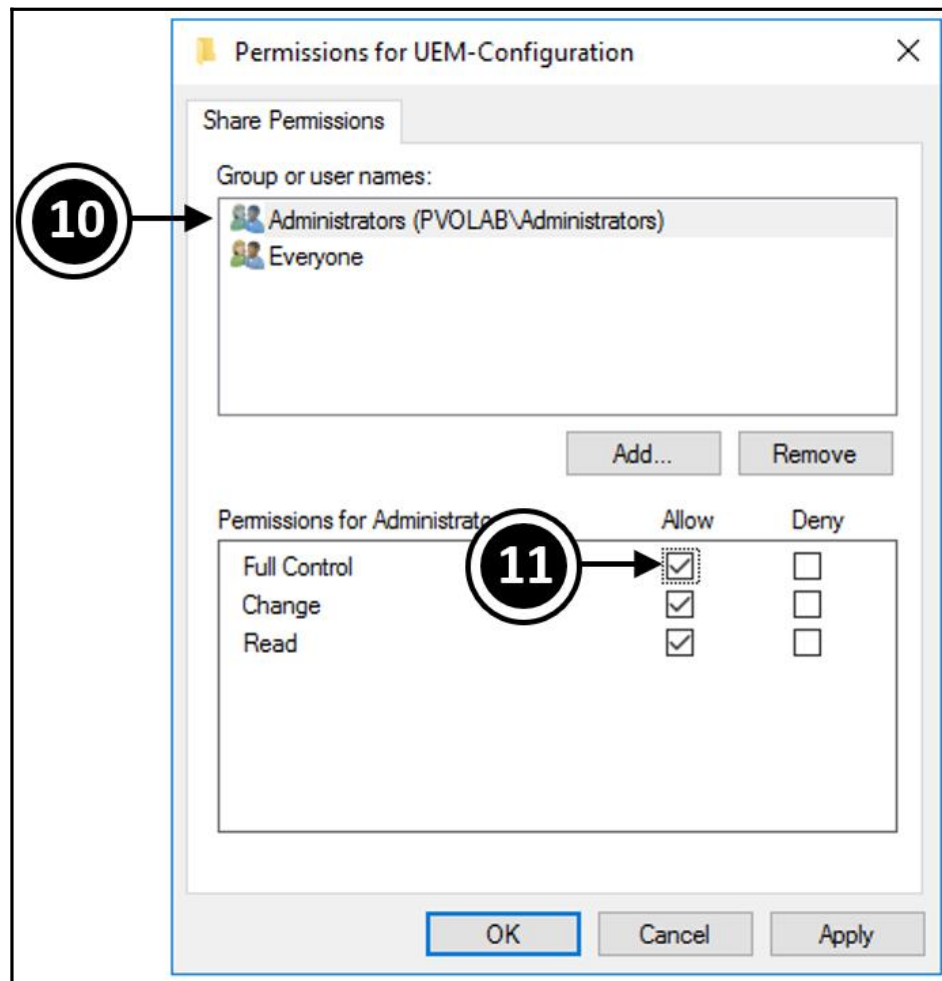


6. Check the box for **Read** (6) to grant this permission to the **Everyone** user group. This is so that each user can read their configuration information, but not change it. Next, we need to add the Administrators group that we created, so to do this, click the **Add ...** button (7). You will now see the **Select Users, Computers, Service Accounts, or Groups** dialog box, as shown in the following screenshot:



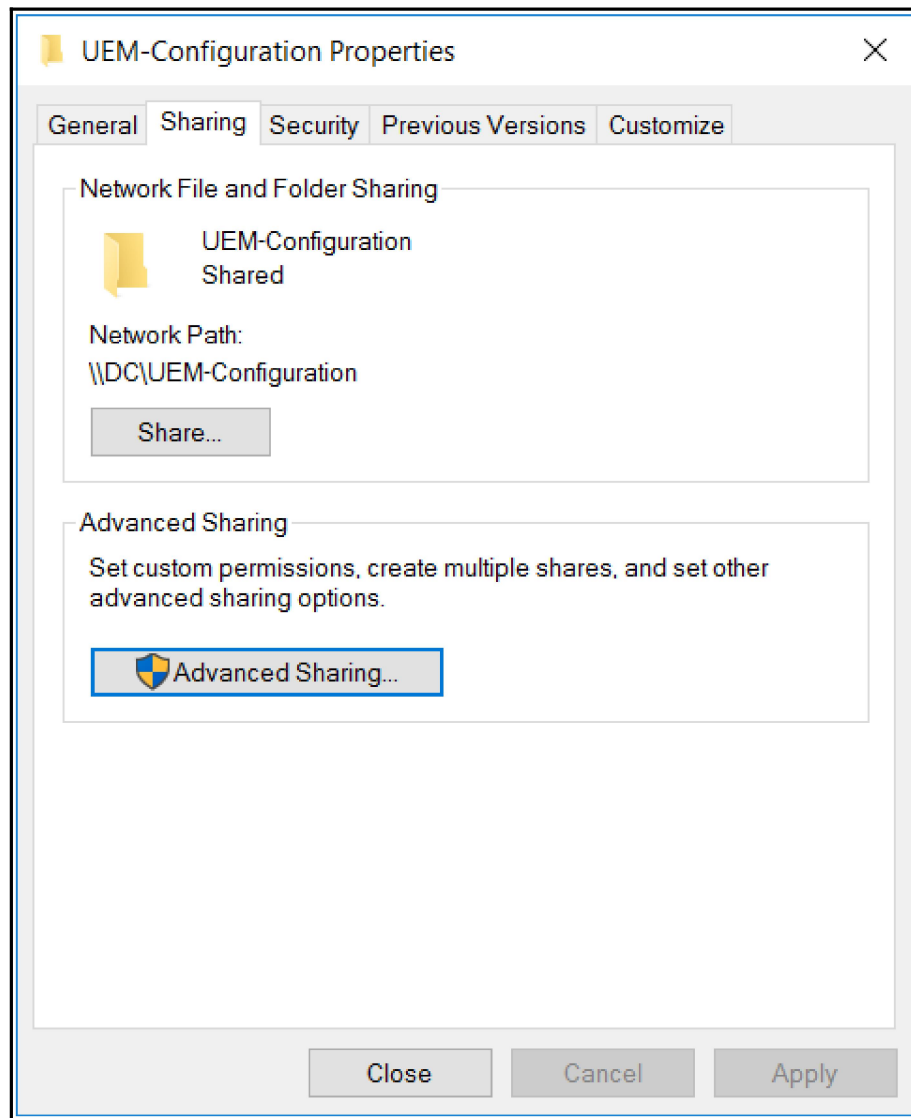
7. In the **Enter the object names to select** box (8), start to type in **Administrators**. You can just type the first part of the name and then click the **Check Names** button (9). The **Administrators** group will then become underlined. In this example, we are adding the **Administrators** group rather than the individual administrator account.

- Click the **OK** button to return to the **Permissions for UEM-Configuration** dialog box, as shown in the following screenshot:



- Click and highlight the **Administrators** group (10), and then under **Full Control**, check the box for **Allow** (11).
- Now click the **Apply** button, and then close the dialog box.
- You will return to the **Advanced Sharing** dialog box.
- Click **OK**.

13. Finally, you will see the **UEM-Configuration Properties** dialog box, which now shows the network path to the share that was just created, `\\DC\UEM-Configuration`, as shown in the following screenshot:



14. Click the **Close** button to complete the configuration.

The share you just created contains the central configuration information for UEM. This information is created using the Management Console and is used for creating and editing UEM configurations. As an administrator, you need to be able to have full control of this share, as you will read and write information to it; however, a user only needs to be able to read the configuration information to work out which configuration needs to be applied to them when they log in.

Next, we need to create a second shared folder for the profile itself.

UEM Profile Archive Share

The next shared folder to create is used to store the UEM profile archive, which will hold all the user's personal settings. Within this folder, a unique subfolder will be created for each of your users.

When a user logs in, their personal settings are read from the share when they launch an application and are then written back when they close an application or log out. Therefore, they will need to have the appropriate permission level to do this.

The UEM profile files are stored as ZIP files and the amount of storage required will depend on the number of users, applications, and backups you have in your environment.

To create the shared folder, follow the steps in the previous section to create a folder called `UEM-Profiles`, and when you get to the configuring permissions stage, you need to set the following permissions on the shared folder:

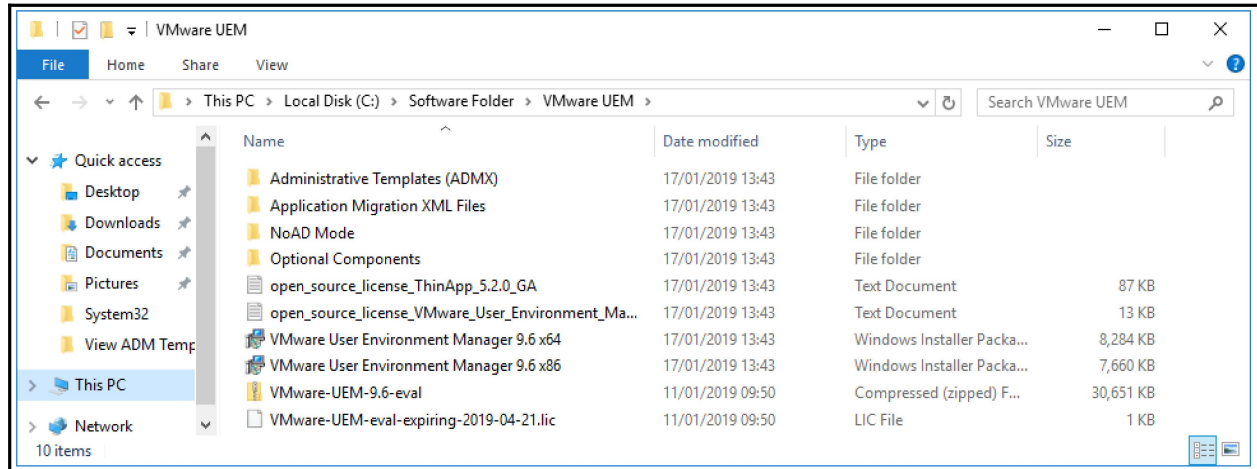
- **Administrators: Full control** on all folders, subfolders, and files
- **Users: Read & execute**, and create folders/append data on this folder only
- **Creator-owner: Full control** of subfolders and files

Now that you have the two shared folders in place, the next step is to install the UEM Management Console before we continue with the configuration. The reason for this is that you need some of the files that get copied during the installation to be able to start configuring Active Directory Group Policy.

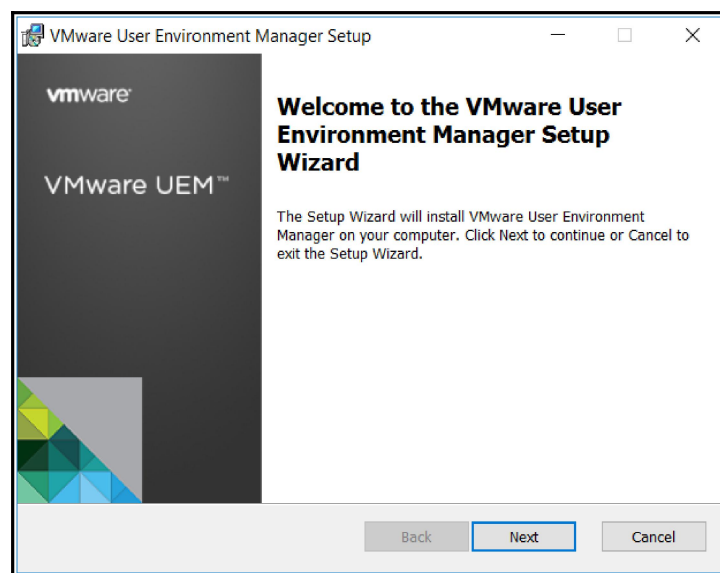
Installing the UEM Management Console

In this section, we are going to install the UEM Management Console by following the steps described as follows:

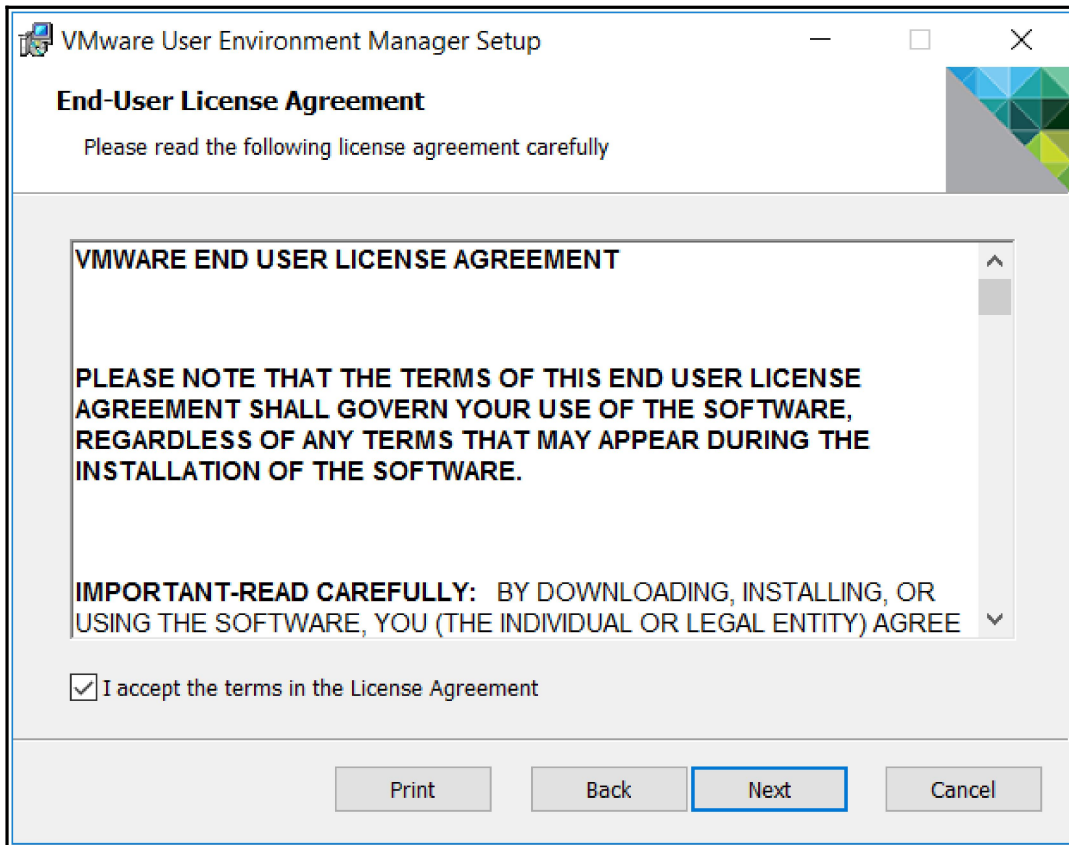
1. Locate the installer software that you copied to the shared software folder on the domain controller, as shown in the following screenshot:



2. Double-click the VMware User Environment Manager 9.6 x64 file to launch the installer.
3. You will now see the **Welcome to the VMware User Environment Manager Setup Wizard** screen, as shown in the following screenshot:

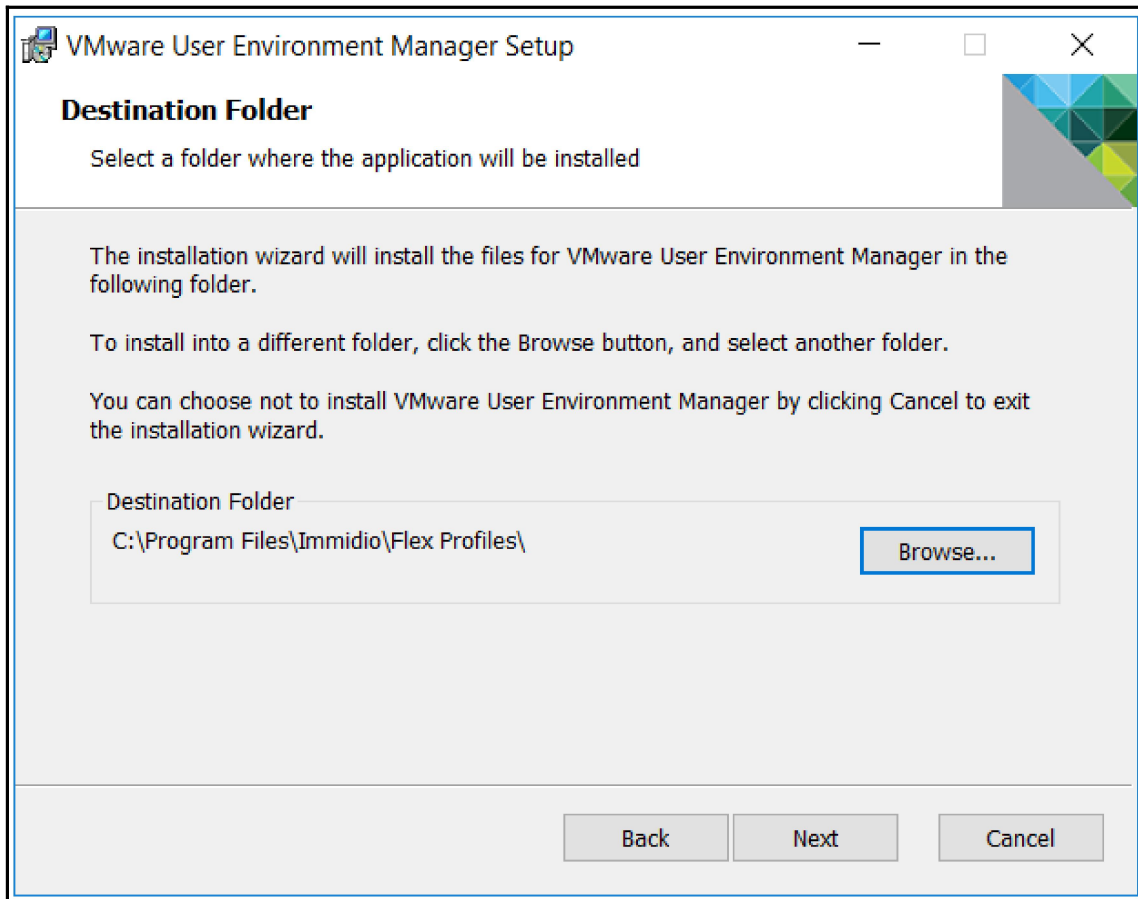


4. Click the **Next** button to continue. You will now see the **End-User License Agreement** box, as shown in the following screenshot:



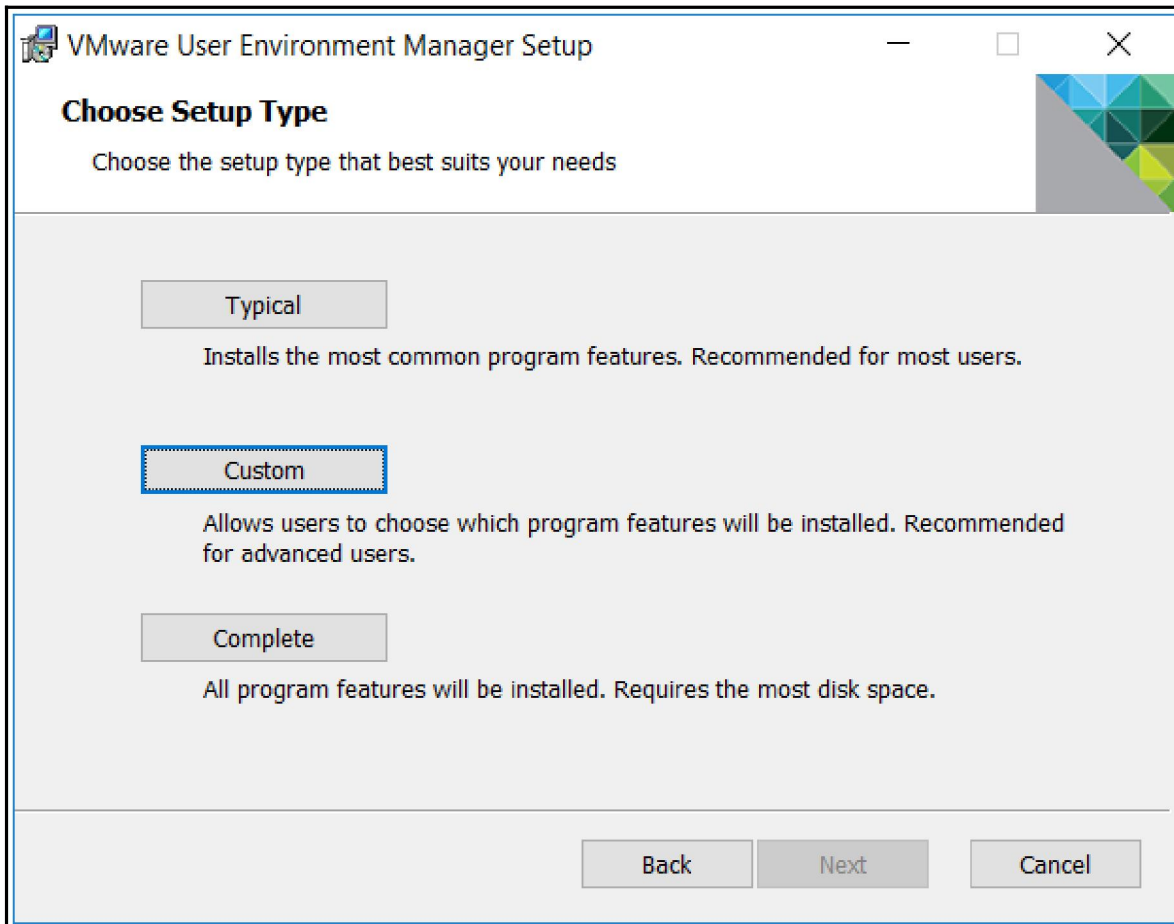
5. Check the box for **I accept the terms in the License Agreement**, and then click **Next** to continue.

6. You will now see the **Destination Folder** box, as shown in the following screenshot:



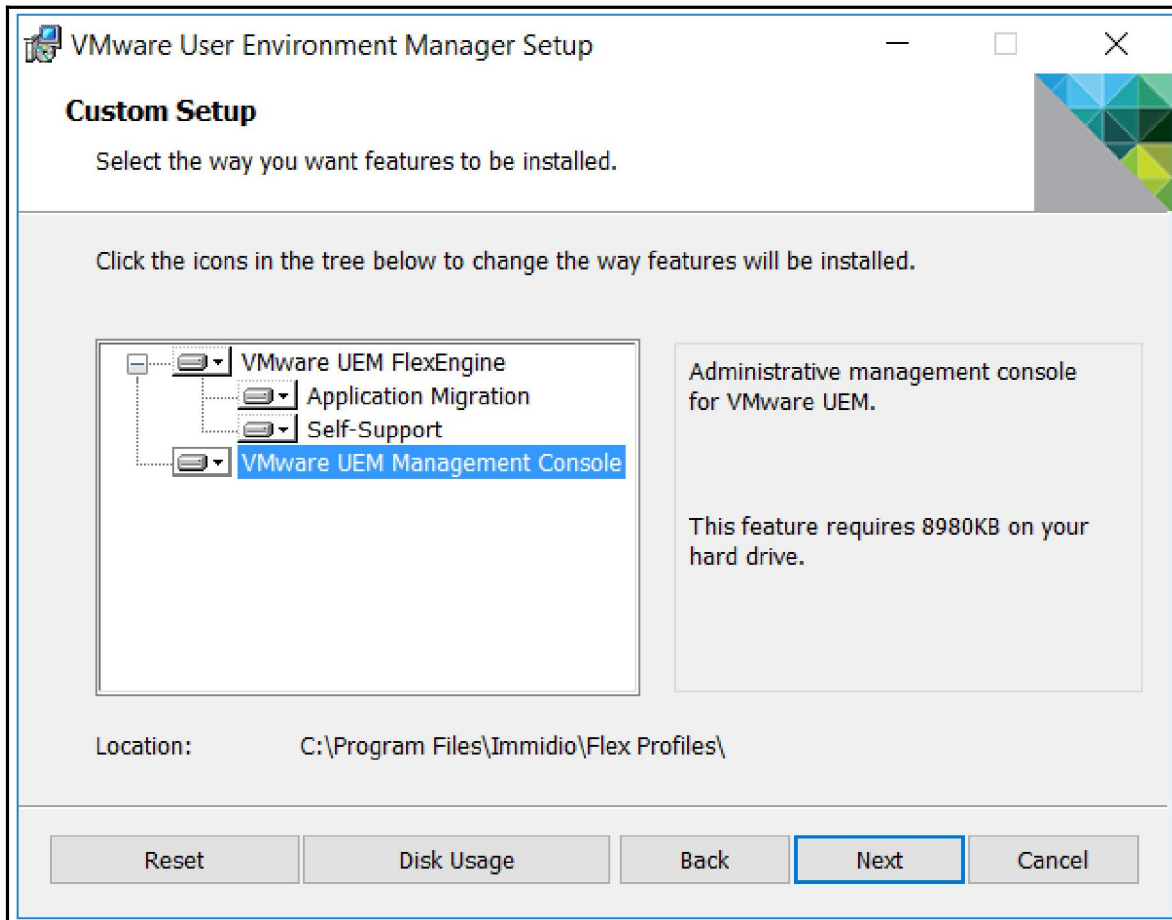
7. You have the option of clicking the **Browse...** button and selecting a different folder into which you can install the UEM software. For the example lab, we are going to go with the default `C:\Program Files\Immidio\Flex Profiles\` folder.

- Click **Next** to continue. You will now see the Choose **Setup Type** box, as shown in the following screenshot:



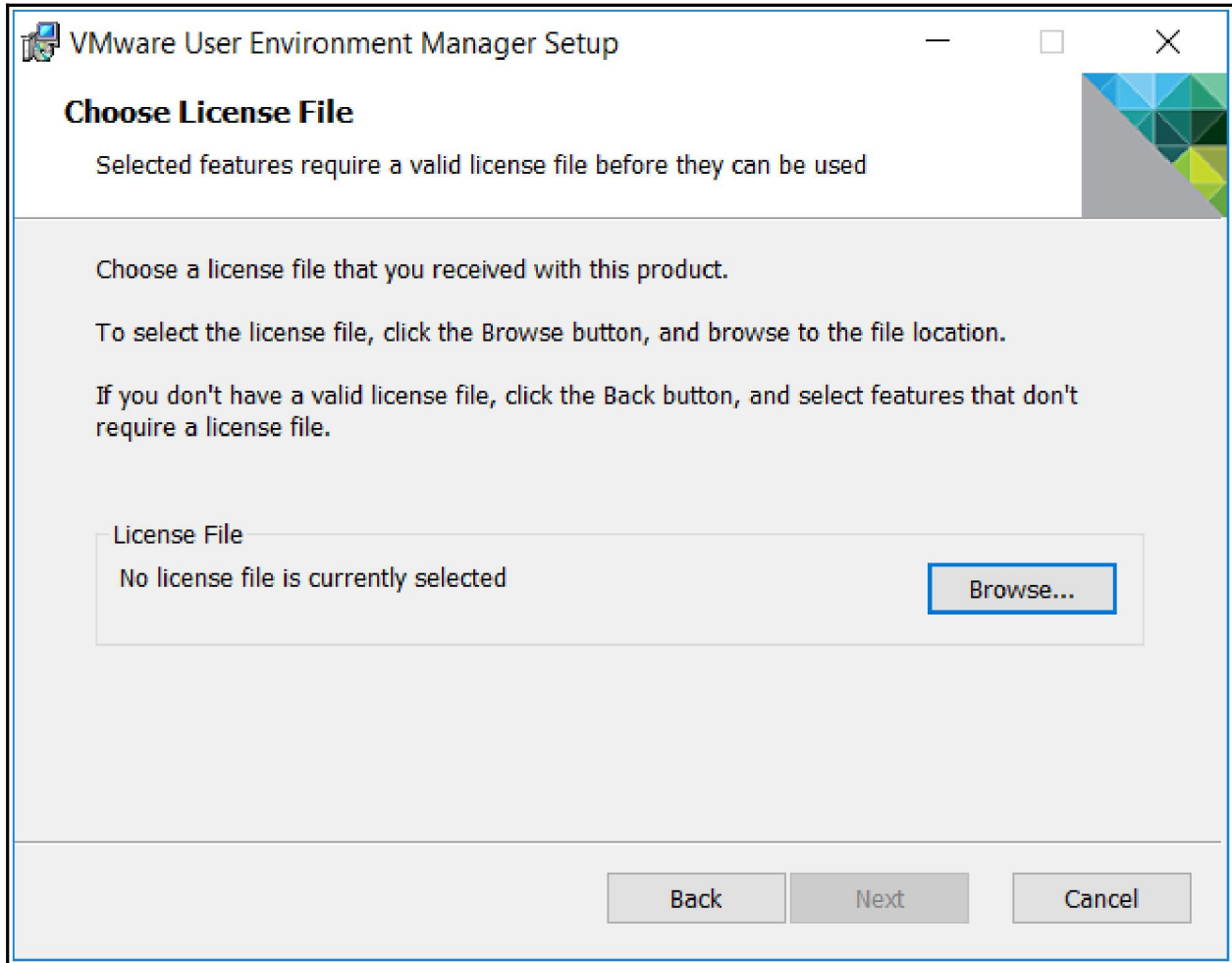
- On this screen, you have the option to choose the type of install. You can choose **Typical** (installs common components), **Custom** (lets you choose what to install), or **Complete** (installs everything). For the example lab, we are going to choose the **Custom** option so that we can the components that get installed.

10. You will now see the **Custom Setup** box, as shown in the following screenshot:

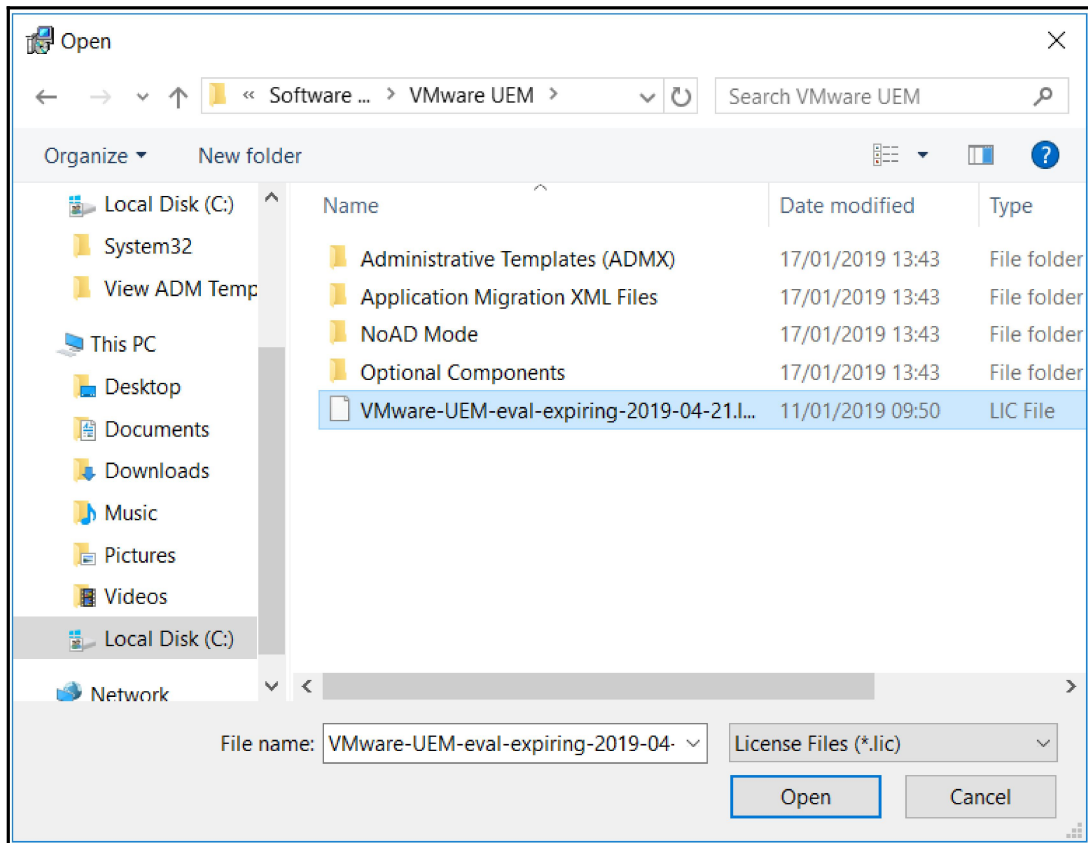


11. By default, the **VMware UEM FlexEngine** will be installed with the option for **Application Migration** and **Self-Support**. The management console, by default, is not installed, however, we are going to install it on this server, so click the option for **VMware UEM Management Console**, and then from the menu, select the option for **Entire feature will be installed on local hard drive**. This will ensure that the Management Console gets installed.

12. Click **Next** to continue. You will now see the **Choose License File** screen, as shown in the following screenshot:



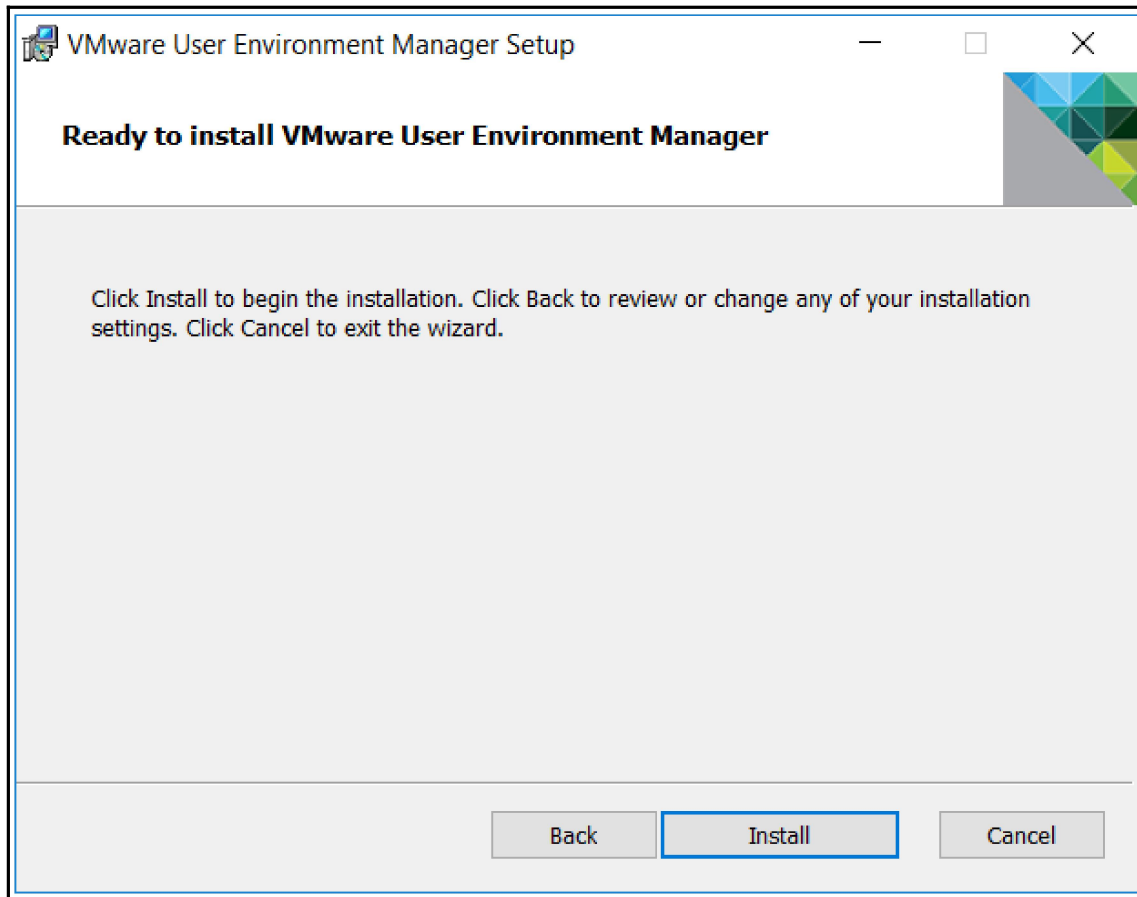
13. Click the **Browse...** button to select the license file. A Windows Explorer **Open** window will open, as shown in the following screenshot:



14. Navigate to the appropriate license file, highlight it, and then click the **Open** button. You will now return to the **Choose License File** screen, which will now display the path to the license file that you just selected, as shown in the following screenshot:

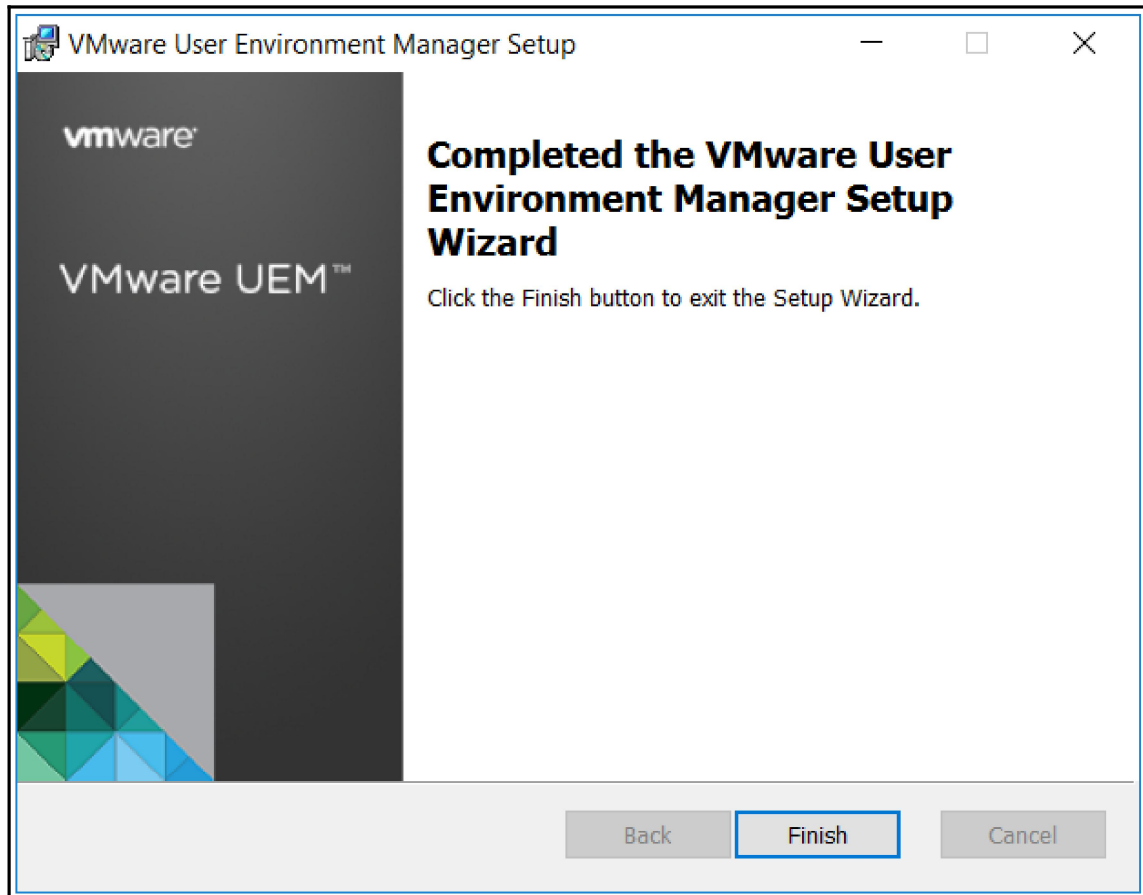


15. Click **Next** to continue. You will now see the **Ready to Install VMware User Environment Manager** screen, as shown in the following screenshot:

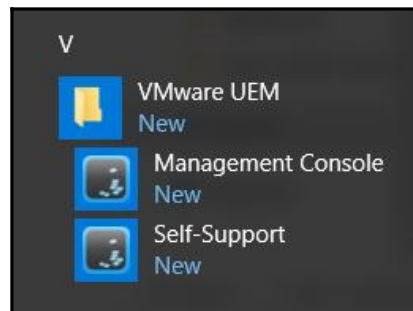


16. Click **Install** to start the installation.

17. Once the installation has finished, you will see the **Completed the VMware User Environment Manager Setup Wizard** screen, as shown in the following screenshot:



18. Click the **Finish** button to complete the install and close the installer. You will now see under the Apps screen, on the desktop of the server, that **VMware UEM** has been installed, as shown in the following screenshot:

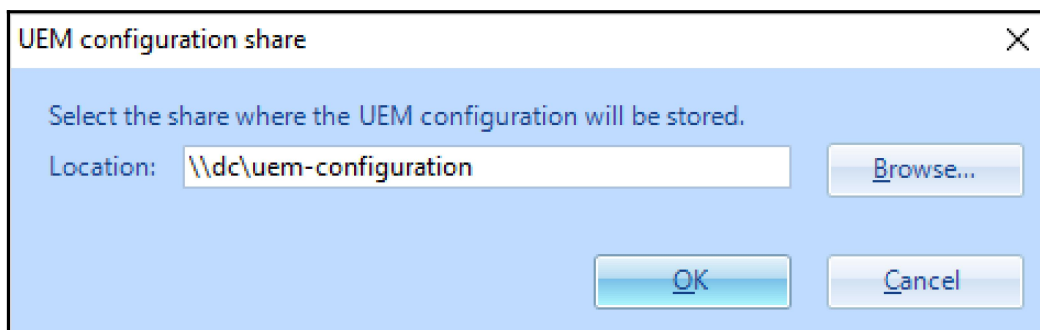


You have now successfully installed VMware UEM.

In the next section, we are going to launch the UEM Management Console for the first time and complete the installation with some additional initial configuration tasks.

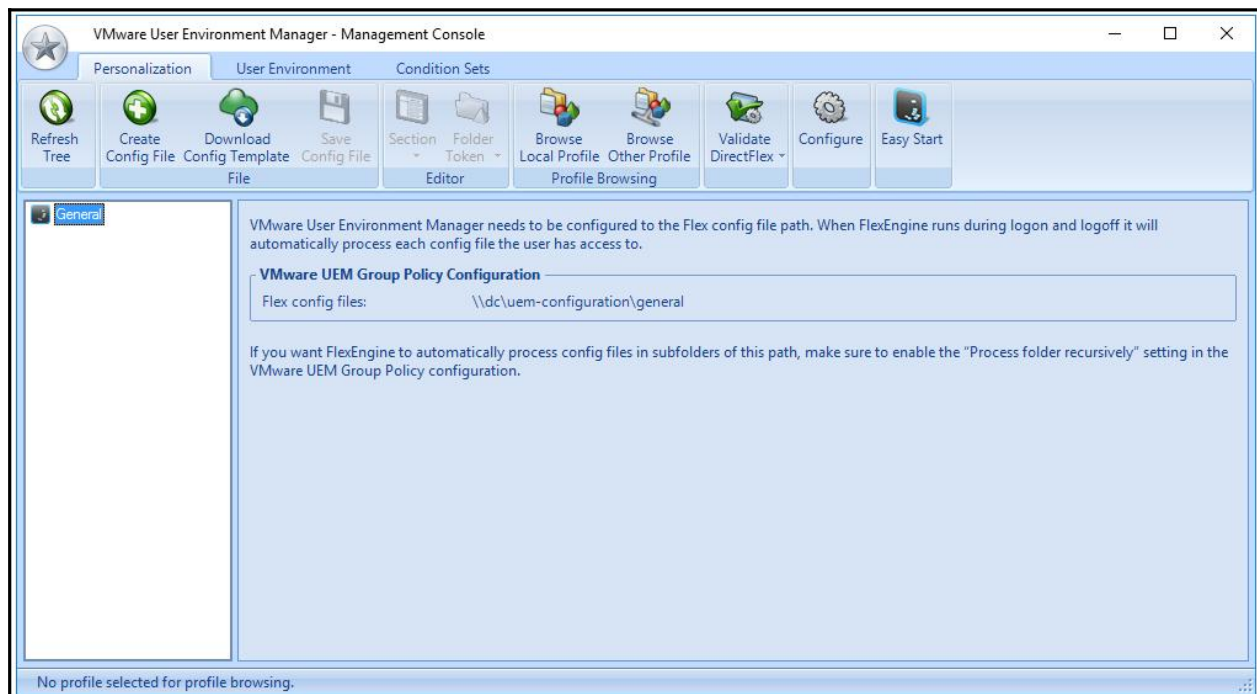
Initial configuration of the management console

First of all, launch the UEM Management Console from the server on which we just installed it. You will see that the first task that you need to complete is to configure the location of the configuration shared folder from the **UEM configuration share** box that pops up on launch, as shown in the following screenshot:



In the **Location** box, type the path to the configuration shared folder. In the example lab, this is `\\dc\uem-configuration`, as shown. Then, click the **OK** button.

You will now see the **Management Console**, as shown in the following screenshot:



We will look at the Management Console and its features more closely later on in this chapter, in the *A high-level overview of UEM the features* section.

In the next section, we will complete the Active Directory configuration tasks.

Preparing Active Directory for UEM – Part II

Now that you have installed the UEM Management Console, you can complete the AD side of the configuration and look at the GPO settings.

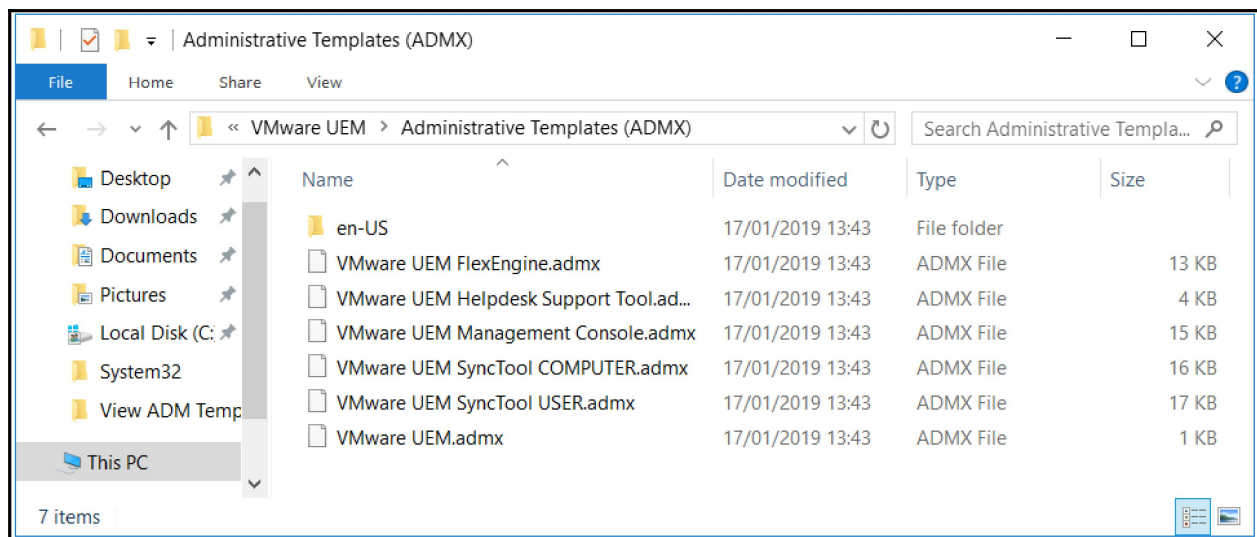
Creating and configuring GPOs

Before you can start configuring the GPOs, you first of all need to copy the policy templates onto the domain controller. Unlike Persona Management, these are delivered as ADMX and ADML files, which will need to be manually copied into the appropriate directory on the domain controller.

Copying the ADMX templates to Active Directory

To copy the ADMX template files, follow these steps as outlined:

1. On the Domain Controller in the example lab, open a Windows Explorer window and navigate to the VMware UEM software, where you unzipped the UEM files. In the example lab, this is in the shared software folder, which is called `VMware UEM`.
2. Double-click and open the `Administrative Template (ADMX)` folder. You will now see the six ADMX template files, as shown in the following screenshot:



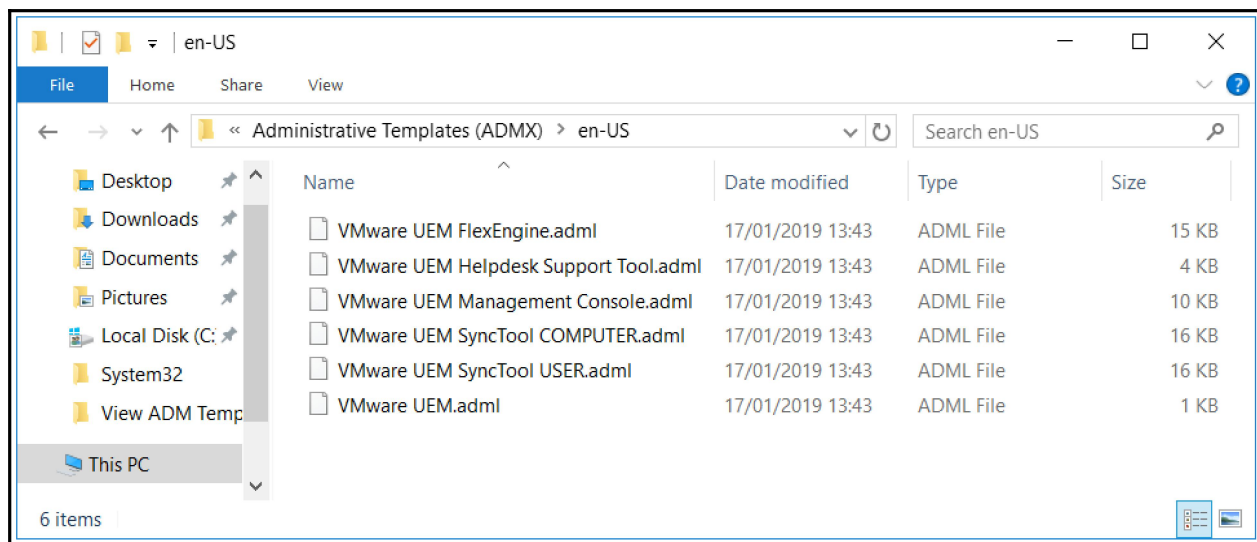
3. Select all the ADMX files, then right-click, and from the contextual menu, select the **Copy** option.
4. Next, navigate to the location to where the files need to be copied. In the example lab, this is the following folder:
`C:\Windows\SYSTEM32\sysvol\pvolab.com\Policies\PolicyDefinitions`

Once the files are copied, in the next section, we will copy the remaining ADML files.

Copying the ADML templates

To copy the ADML template files, follow these steps as outlined:

1. On the Domain Controller in the example lab, open a Windows Explorer window and navigate to the VMware UEM software, where you unzipped the UEM files. In the example lab, this is in the shared software folder, which is called `VMware UEM`.
2. Double-click and open the `Administrative Template (ADMX)` folder, and then you will see the six ADMX template files, as shown in the following screenshot:



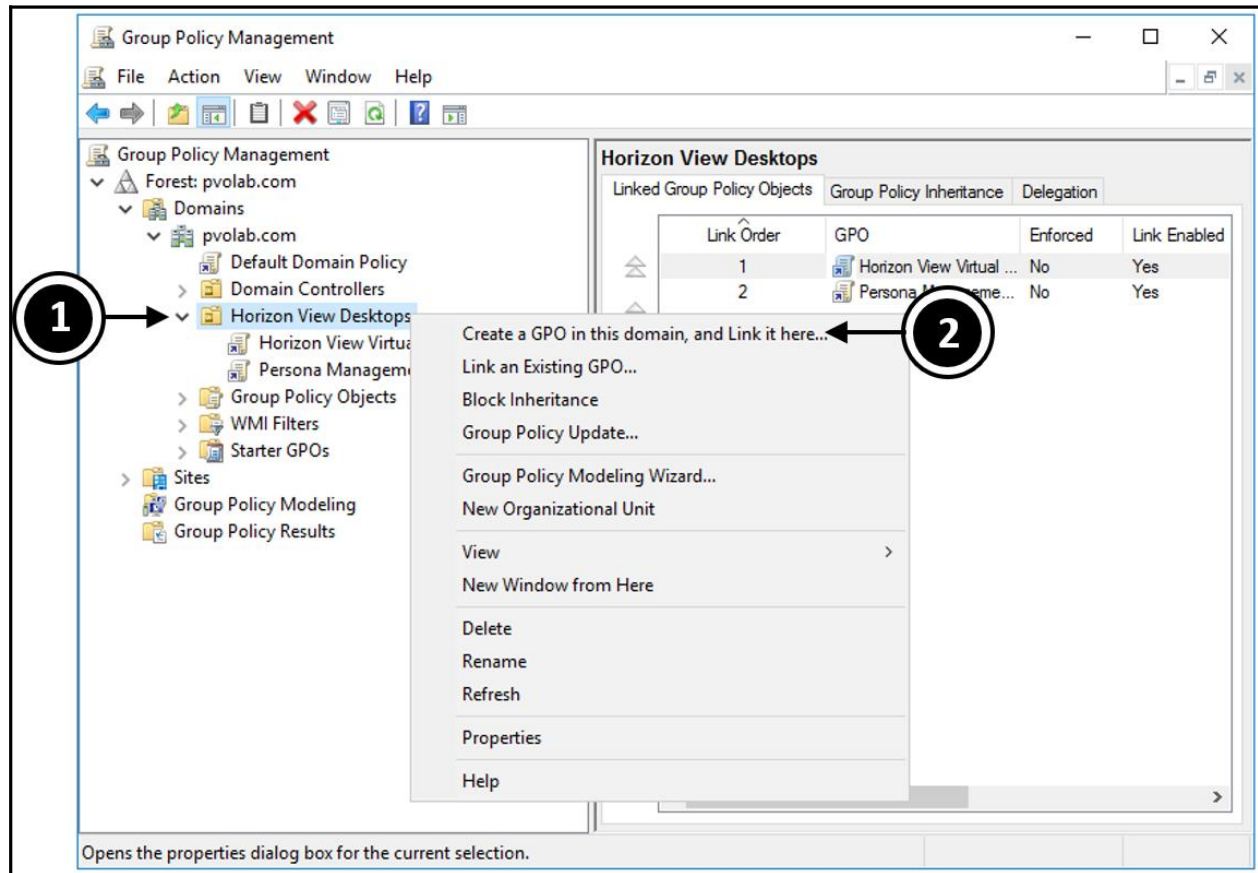
3. Select all the ADML files and then right-click. From the contextual menu, select the **Copy** option.
4. Next, navigate to the location where the files need to be copied to. In the example lab, this is the following folder: `C:\Windows\SYSTEM32\sysvol\pvolab.com\Policies\PolicyDefinitions\en-US`

Now that the template files are copied, in the next section we can start creating and configuring the Group Policy.

Creating a GPO

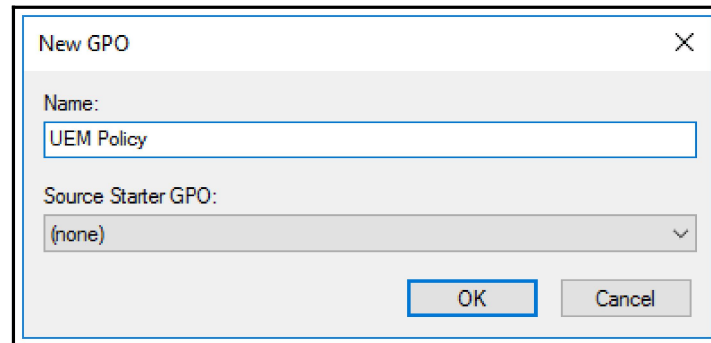
In this section, we are going to create a new Group Policy for UEM. To do this, follow the steps described:

1. From the Domain Controller, and from the Administrative Tools menu, open **Group Policy Management**. The **Group Policy Management** configuration screen will launch, as shown in the following screenshot:

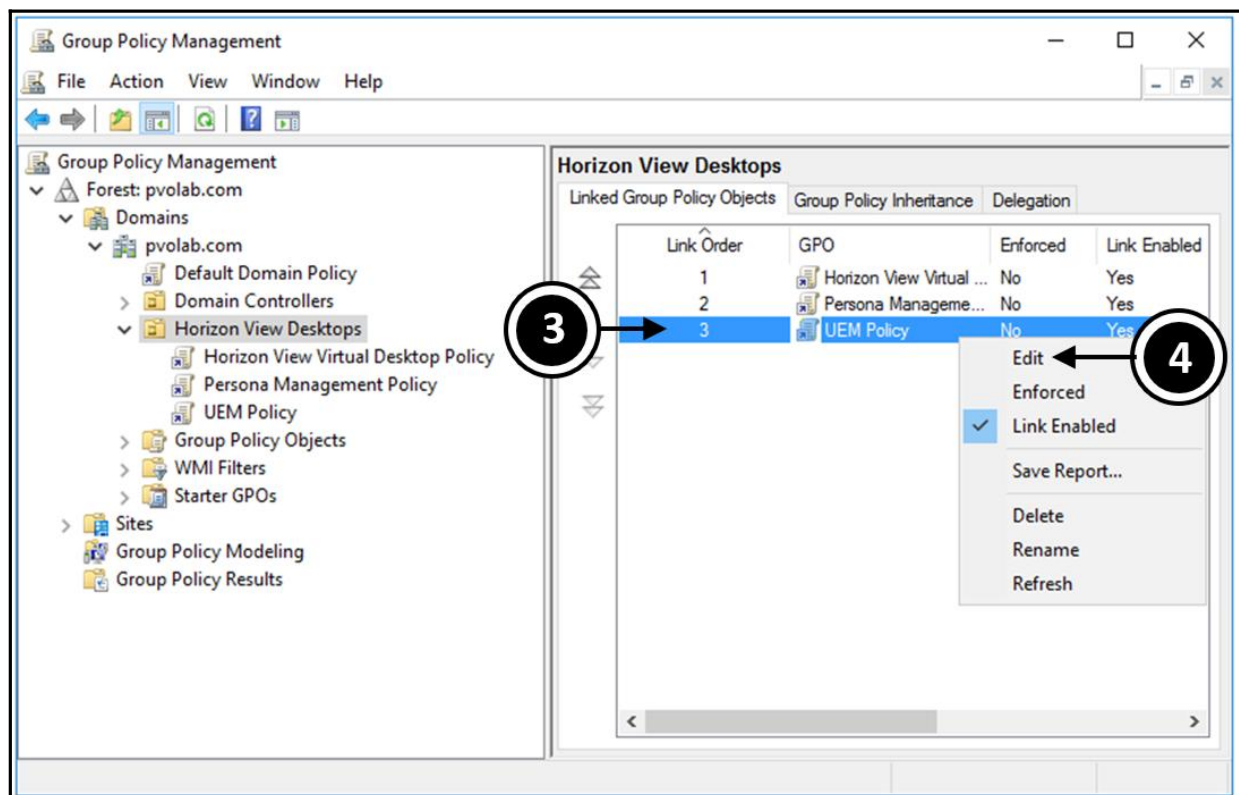


2. Click on the OU where you want to create the policy. In the example lab, we have chosen the **Horizon View Desktops** OU (1). Highlight the OU, and then right-click. From the contextual menu, click **Create a GPO in this domain, and Link it here...** (2).

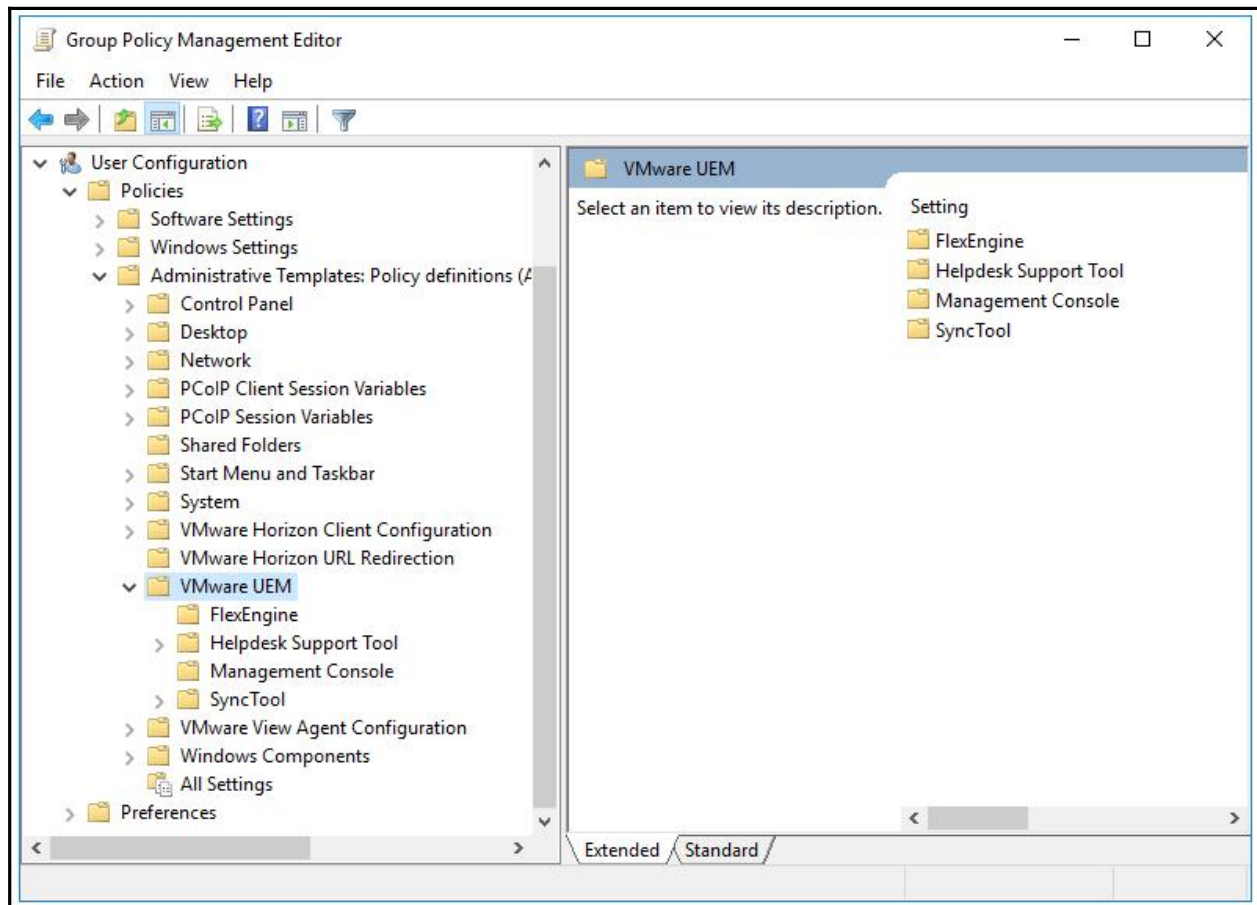
3. You will now see the **New GPO** dialog box, as shown in the following screenshot:



4. In the **Name** box, type in a name for this policy. In the example lab, this is called **UEM Policy**.
5. Click **OK** to continue.
6. You will now return to the **Group Policy Management** screen. The next step is to edit the policy and configure the policy settings. Highlight the newly created **UEM Policy** (3), right-click, and from the contextual menu, click on **Edit** (4), as shown in the following screenshot:



7. You will now see the **Group Policy Management Editor**. Expand the **User Configuration** section, **Policies**, and finally **Administrative Templates**. Then click on the **VMware UEM** folder. You will now see the window shown in the following screenshot:



You will see in the right-hand pane a number of different policy options, which we will take a look at in more detail in the next section.

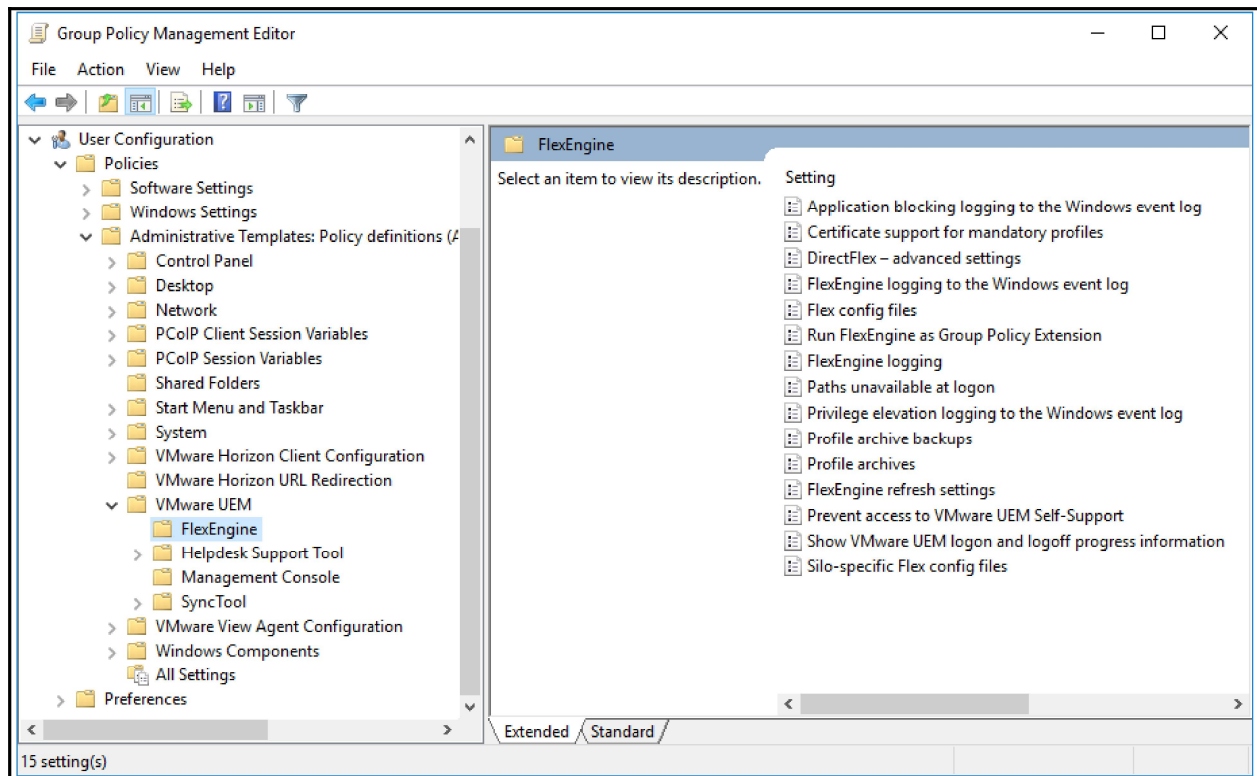
UEM GPO policy configuration options

In this section, we are going to take a look at the different policy configuration options that you need to configure. As there are a fair few policy options, we will just briefly touch on them, but we will look at a little closer at the core policies that need to be configured in order to enable UEM to work.

We will start by looking at the FlexEngine policies.

FlexEngine policy configuration options

The first set of policy options are used to configure the FlexEngine components. The following screenshot shows an overview of the available policies:



Let's have a look at each of these policy options and what they manage:

- **Application blocking logging to the Windows event log:** When enabled, details about blocked application launches are logged to the Windows event log.
- **Certificate support for mandatory profiles:** This setting enables the use of personal certificates for mandatory profiles. You will also need to create a `Flexconfig` file using the **Personal Certificates** Windows Common Setting.
- **DirectFlex - advanced settings:** The default setting is for DirectFlex to export user profile information when users close an application. Enabling **Only export at logoff** delays the export of profile information until the user logs off. This setting can be overridden in the `Flexconfig` file. You can also display a message to the user in the notification area, notifying them that DirectFlex is importing or exporting data. This setting is the **Show DirectFlex notifications** setting.

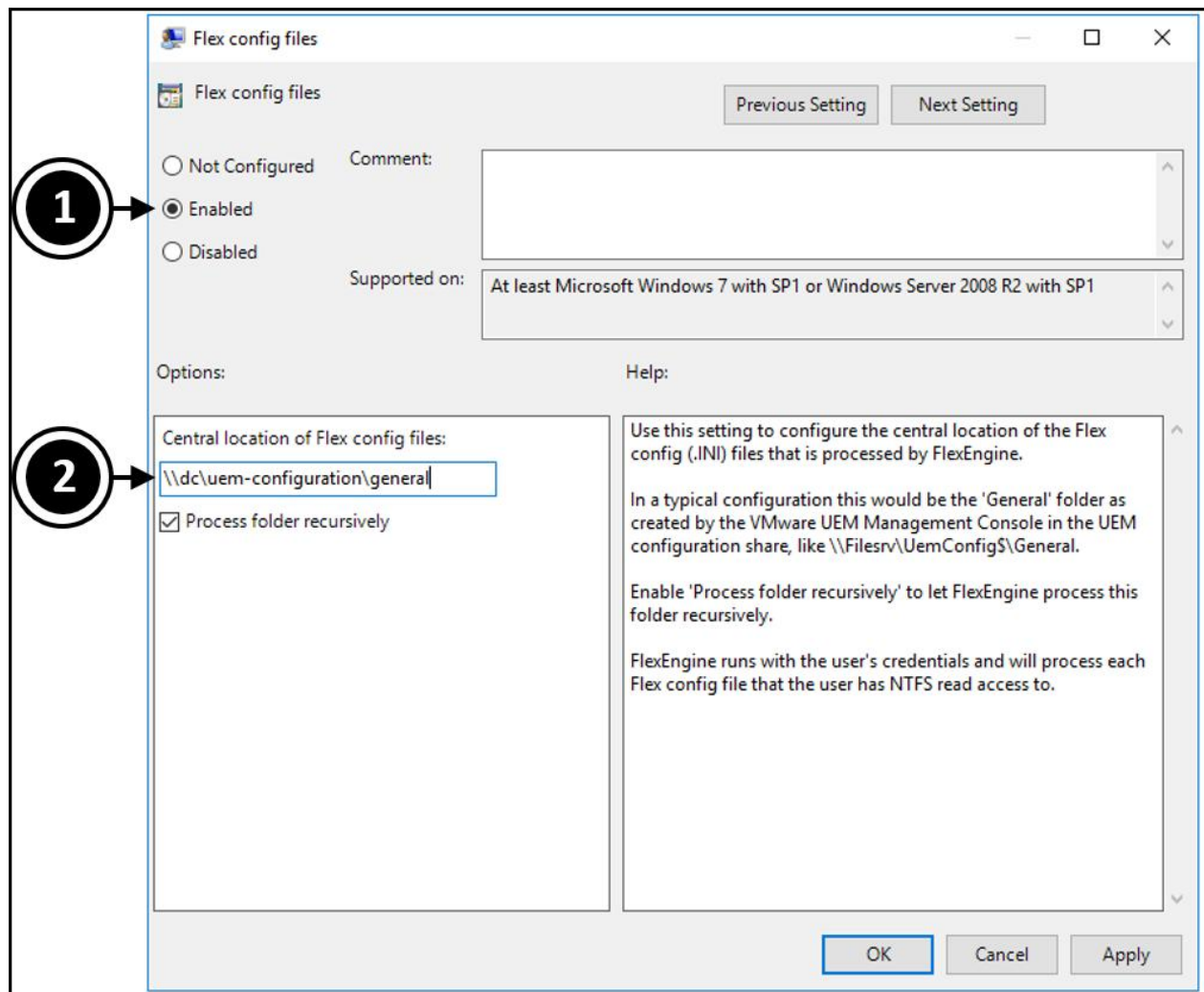
If the import or export occupies less time than the configured notification delay, then no message will be displayed. It is useful to show messages when access to the profile archive path is slow (that is, when imports and exports take longer).

If the notification delay is set to 0, then the messages are displayed immediately.

To show a message specifically in the notification area while DirectFlex is in the process of importing, enable the **Hide DirectFlex exit notification** setting.

- **FlexEngine logging to the Windows event log:** When this setting is enabled, FlexEngine logs path-based import and export messages to the Windows event log. Optionally, Windows event log messages can also be logged for other FlexEngine actions (specifying a size of 0 turns off the corresponding warning).

- **Flex config files:** This is one of the core policy settings that needs to be configured, as it points to the location of the UEM configuration settings that are created in the management console. To configure this policy, complete the following tasks: Click the **Enabled** button (1) to enable the policy, and then in the **Central location of Flex config files** box (2), enter the path details shown in the following screenshot:

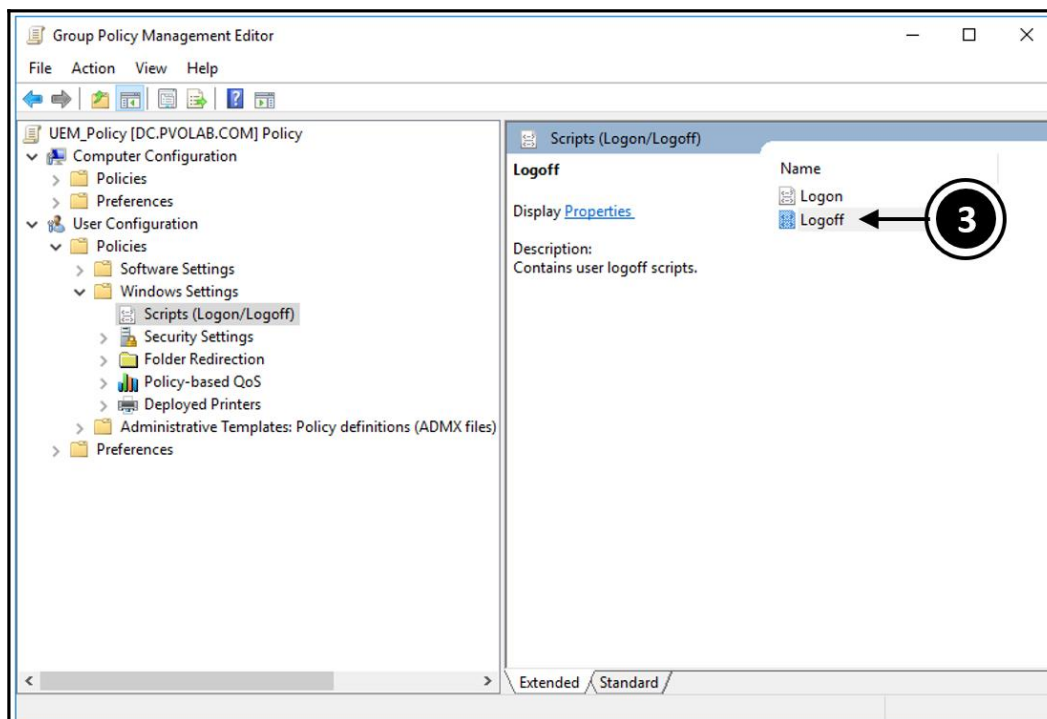


In the example lab, this path is configured as `\\dc\uem-configuration\general`.

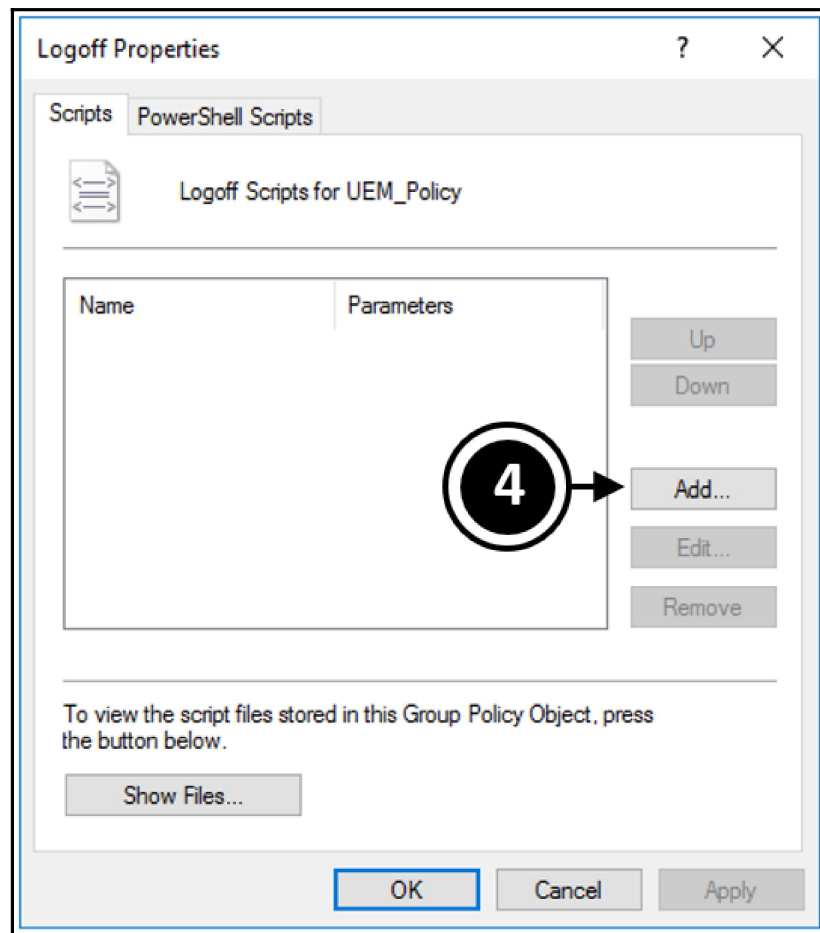


You need to add the `general` folder to the end of the path. This folder is created automatically when you install the Management Console.

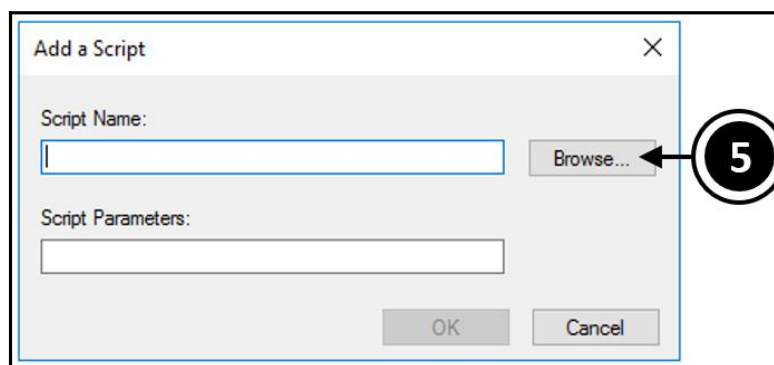
- **Run FlexEngine as Group Policy Extension:** Selecting this option allows the FlexEngine to run automatically during login by running as a Group Policy client-side extension. This policy is simply **Enabled** or **Disabled** by clicking the corresponding radio button. To ensure the FlexEngine Group Policy client-side extension runs at every login, you need to configure the **Always wait for the network at computer startup and logon** policy within this new Group Policy. To do this, follow the steps described:
 1. Navigate to the policy by clicking on Computer Configuration, Policies, Administrative Templates, System, Logon from the **Group Policy Management Editor**. Also, ensure you apply this policy to the OU that contains the clients.
 2. With this policy, you also need to configure the UEM FlexEngine logout command to run from a logout script. This way, the personal settings of the end users will be exported when they log out.
 3. To do this, in the **UEM Policy GPO**, navigate to the User Configuration section and expand out the folders for Policies, Windows Settings, and then click on Scripts (Logon/Logoff), as shown in the following screenshot:



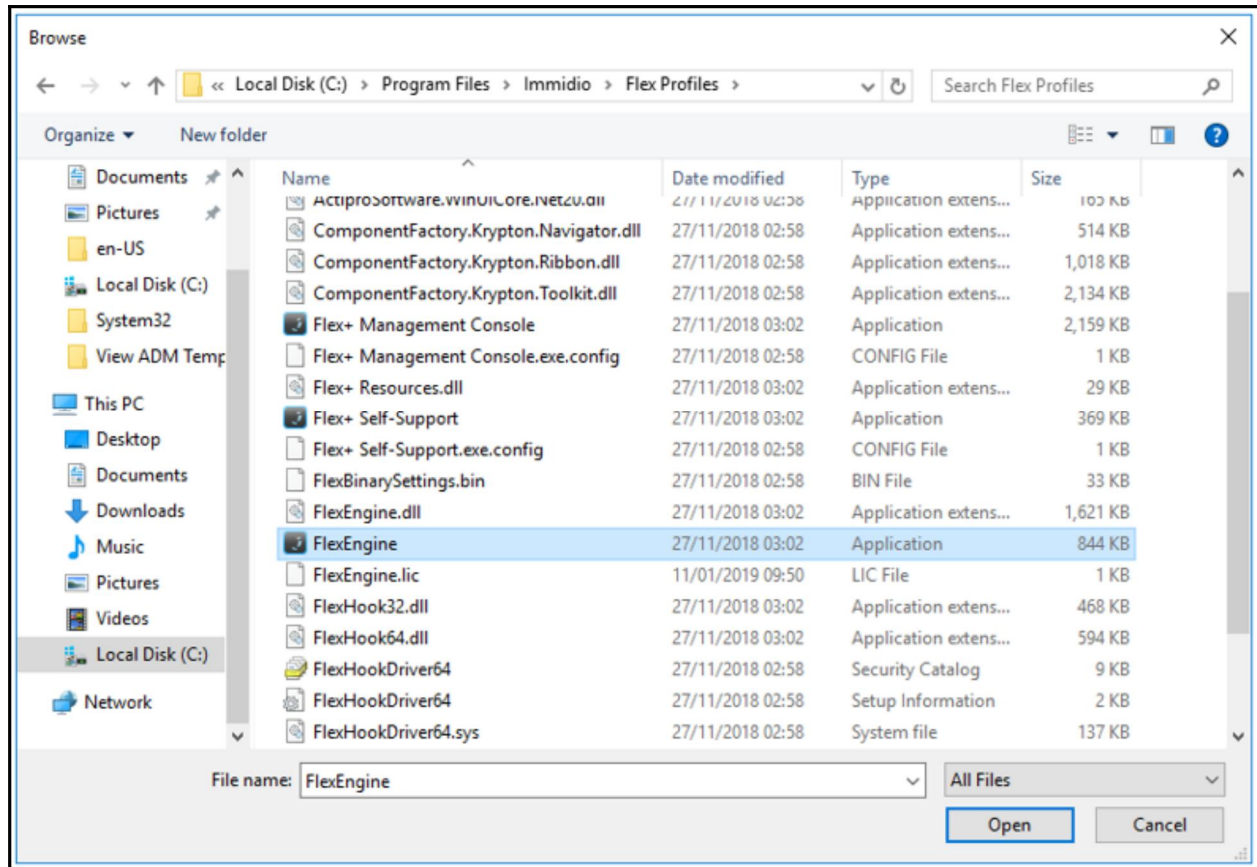
4. In the right-hand pane, double-click on the setting for **Logoff (3)**.
5. You will then see the **Logoff Properties** dialog box, as shown in the following screenshot:



6. Click the **Add...** button (4), and you will now see the **Add a Script** dialog box, as shown in the following screenshot:

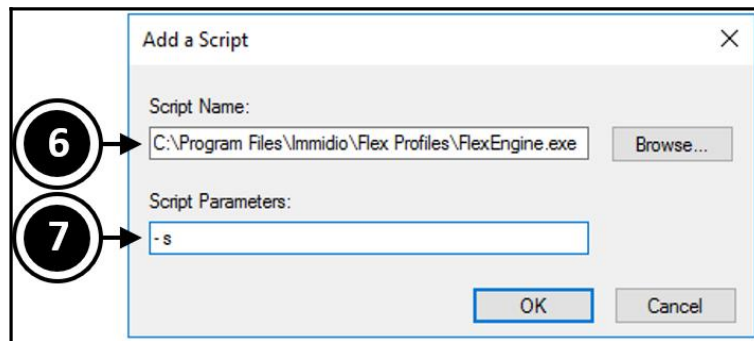


- Click the **Browse...** button (5). You will see a Windows Explorer window open from where you can select the relevant files, as shown in the following screenshot:

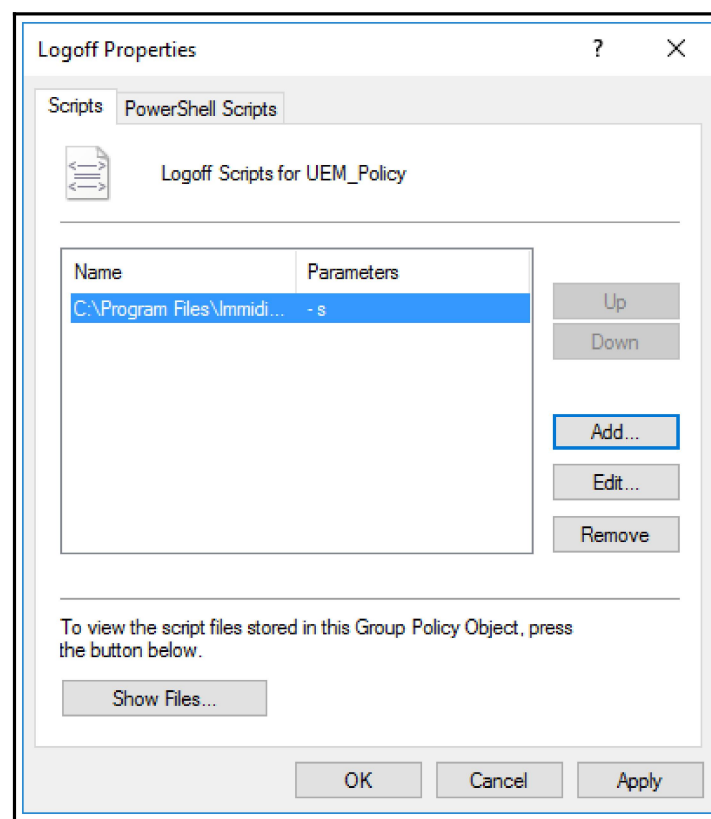


- Navigate to the location where the UEM software was installed and the script files are located. In the example lab, you will find this in the `C:\Program Files\Immidio\Flex Profiles` folder.

9. Scroll down until you find the `FlexEngine` file, and double-click it. You will now return to the **Add a Script** dialog box, as shown in the following screenshot:

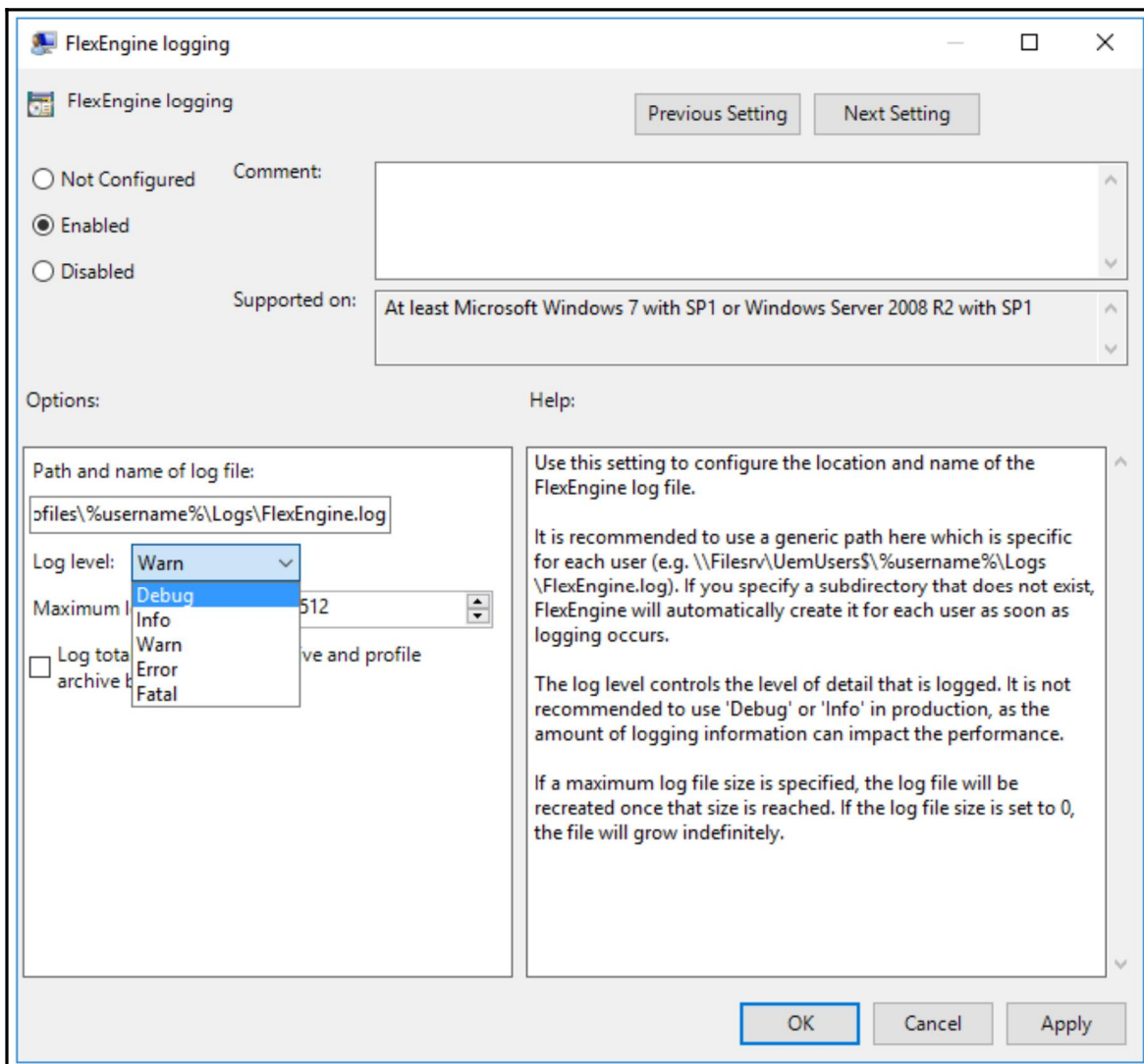


10. You will see that the script name has been added (6).
11. In the **Script Parameters** box (7), you need to add `-s` as a parameter. Now click **OK**.
12. You will now see the **Logoff Properties** box showing the script details added, as shown in the following screenshot:



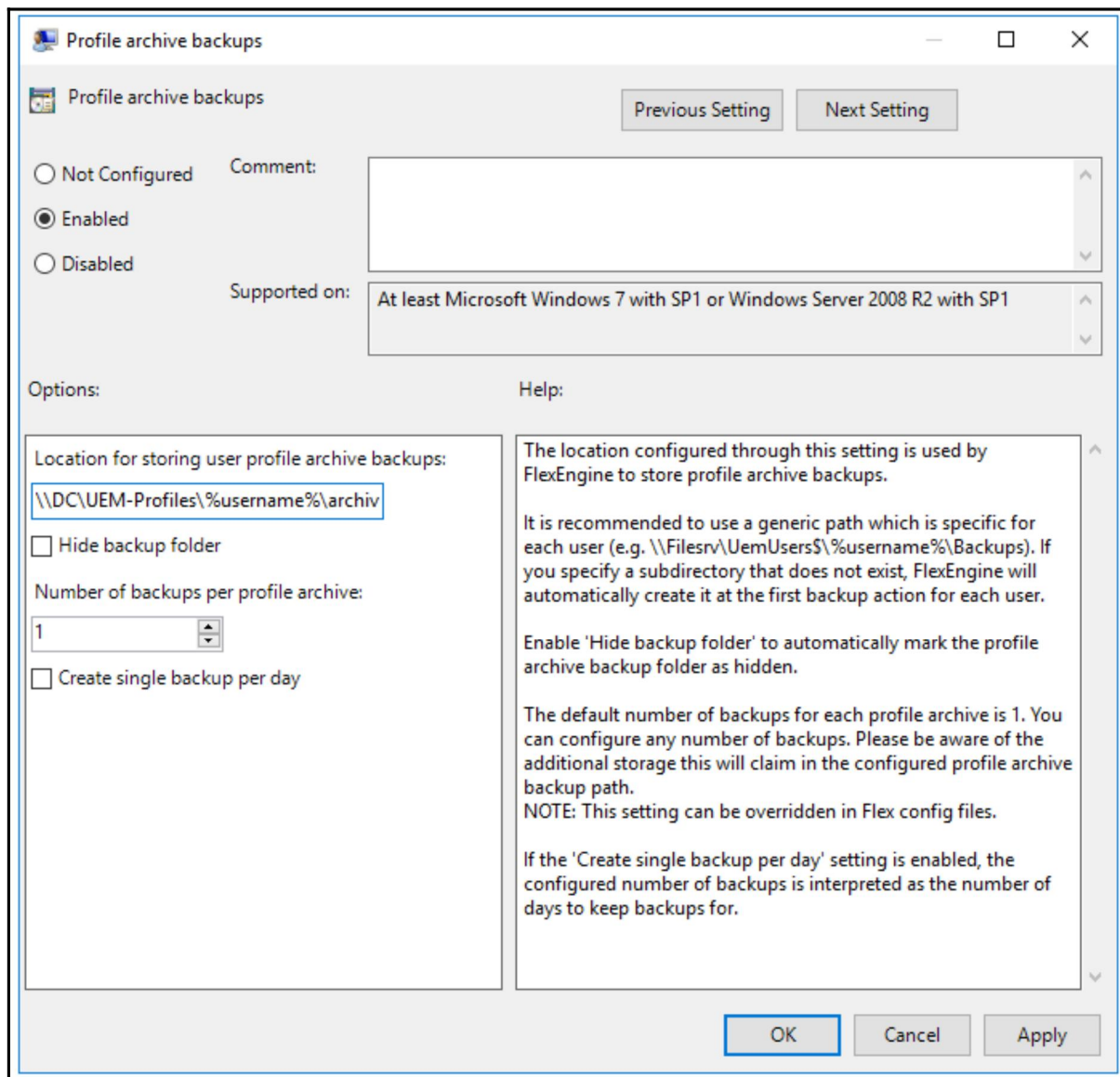
13. Now, click the **Apply** button to complete the configuration.
 14. You will return to the **Group Policy Management Editor** screen, where you can navigate back to the FlexEngine policies and where we can continue to look at the remaining policy configuration options.
- **FlexEngine logging:** This setting configures the location and name of the FlexEngine log file. It is recommended to use a generic path here which is specific for each user, so, for example, in the lab environment, it might look something like \\DC\UEM-Profiles\%username%\Logs\FlexEngine.log. If you specify a subdirectory that does not exist, FlexEngine will automatically create it for each user as soon as logging occurs. This policy also allows you to configure the log level of the detail that is logged. You have the option of selecting **Debug**, **Info**, **Warn**, **Error**, and **Fatal**. VMware recommends that you don't use the **Debug** or **Info** options in a production environment the reason that this amount of logging information can impact performance. If you set a maximum log file size, then the log file will be recreated once it reaches that specified size. If you set the log file size to 0, then the file will grow indefinitely.

The following screenshot shows the **FlexEngine logging** policy configuration screen:



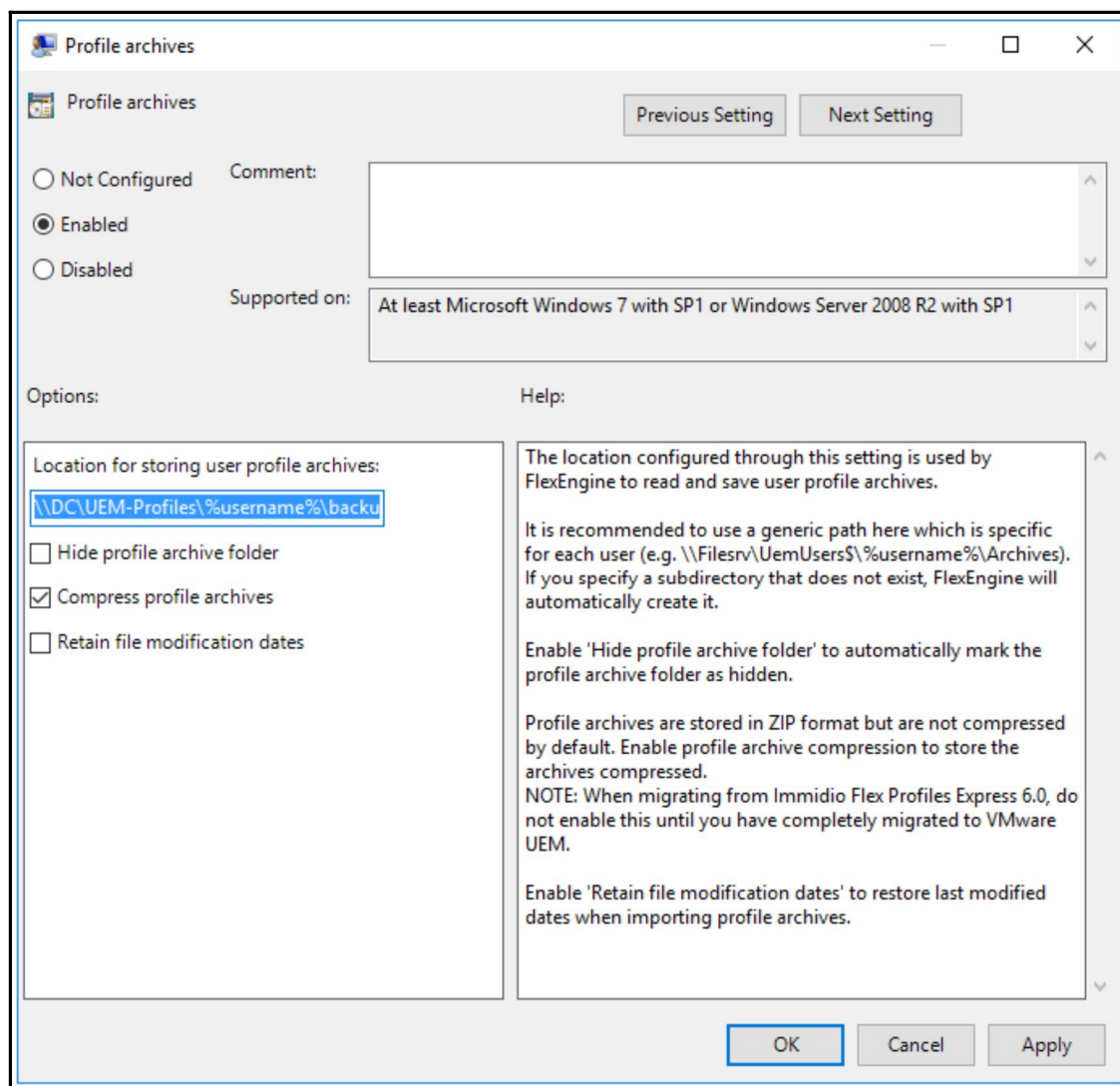
- **Paths unavailable at login:** Allows you to configure the behavior in case the Flex config files path or the profile archive path are not available at logon. If the Flex config path does not exist, then you can opt to either **Logoff** or **Skip import**. If the profile path does not exist, you have the option to **Skip import**, **Apply user environment settings**, or **Logoff**. For each setting, you can also display a warning message.
- **Privilege elevation logging to the Windows event log:** When this setting is enabled, details about elevated application launches are logged to the Windows event log.

- **Profile archive backups:** This is another important configuration option to enable UEM to store profile archive backups. If you click the radio button to enable the policy, you can enter a path in the **Location for storing user profile archive backups** box. In the example lab, the path used is `\\DC\UEM-Profiles\%username%\archive_backups`. You also have the option to **Hide backup folder**, choose the number of backups per profile archive, and to **Create single backup per day**, as shown in the following screenshot:



- **Profile archives:** This is another important configuration option to enable UEM to back up profiles. It is recommended to use a generic path here that is specific for each user. So, for example, in the lab environment, we have used the path `\\DC\UEM-Profiles\%username%\backups`. If you specify a subdirectory that does not exist, FlexEngine will automatically create it. You are also able to **Hide profile archive folder** to mark the profile archive folder as hidden automatically.

Profile archives are stored in the ZIP format but are not compressed by default. To enable compression, check the **Compress profile archives** box to store the archives compressed. These configuration options are shown in the following screenshot:

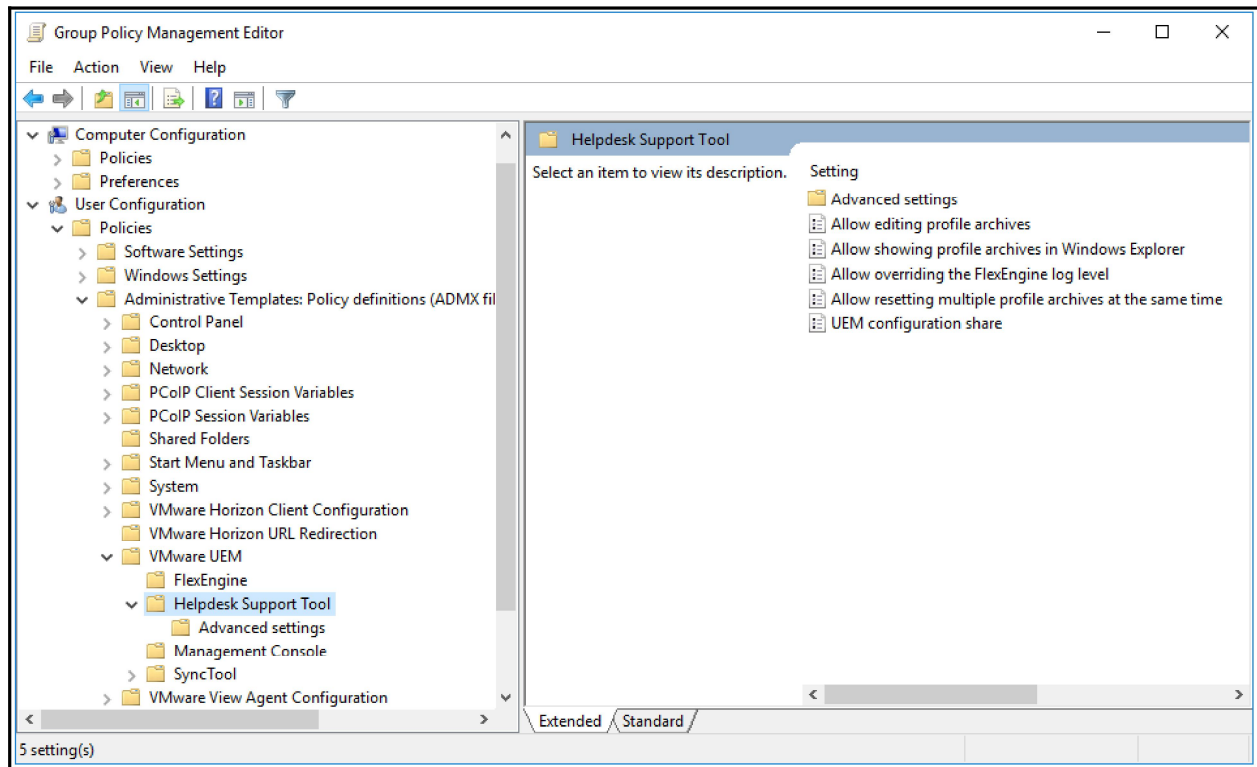


- **FlexEngine refresh settings:** The configuration of this setting is not necessary if you are running FlexEngine as a Group Policy client-side extension.
Enabling the **Refresh Windows appearance** setting refreshes Windows appearance settings at logon, such as the wallpaper . You will also need to create a Flex config file. This file contains the information suitable to be processed by FlexEngine. Enabling the **Refresh mouse settings** will refresh the mouse settings when the user logs in. You will also need to create a Flex config file again. This file contains the **Mouse Windows Common Setting**. Enabling the **Refresh keyboard settings** refreshes keyboard settings at login. You also need to create a Flex config file that contains the **Keyboard Windows Common Setting**.
- **Prevent access to VMware UEM self-support:** This setting prevents users from starting the VMware UEM Self-Support feature.
- **Show VMware UEM logon and logoff progress information:** When this setting is enabled, a splash screen with a progress bar is shown to the end user when FlexEngine is called from a script.
- **Silo-specific Flex config files:** This allows you to specify an additional, silo-specific path for the Flex config files. These are processed as well as the general Flex config files path. The silo-specific suffix is used as a subfolder to the configured profile archive path, and is used to separate profile archives for silo-specific Flex config files from the general ones. If no silo-specific suffix is configured, then the last component of the silo-specific Flex config files path is used.

Next, we are going to look at the Helpdesk Support Tool policy configuration options.

Helpdesk Support Tool policy configuration options

In this section, we are going to look at the Helpdesk Support Tool policy configuration options. The following screenshot shows an overview of the available policies:



Let's have a look at each of these policy options and what they manage:

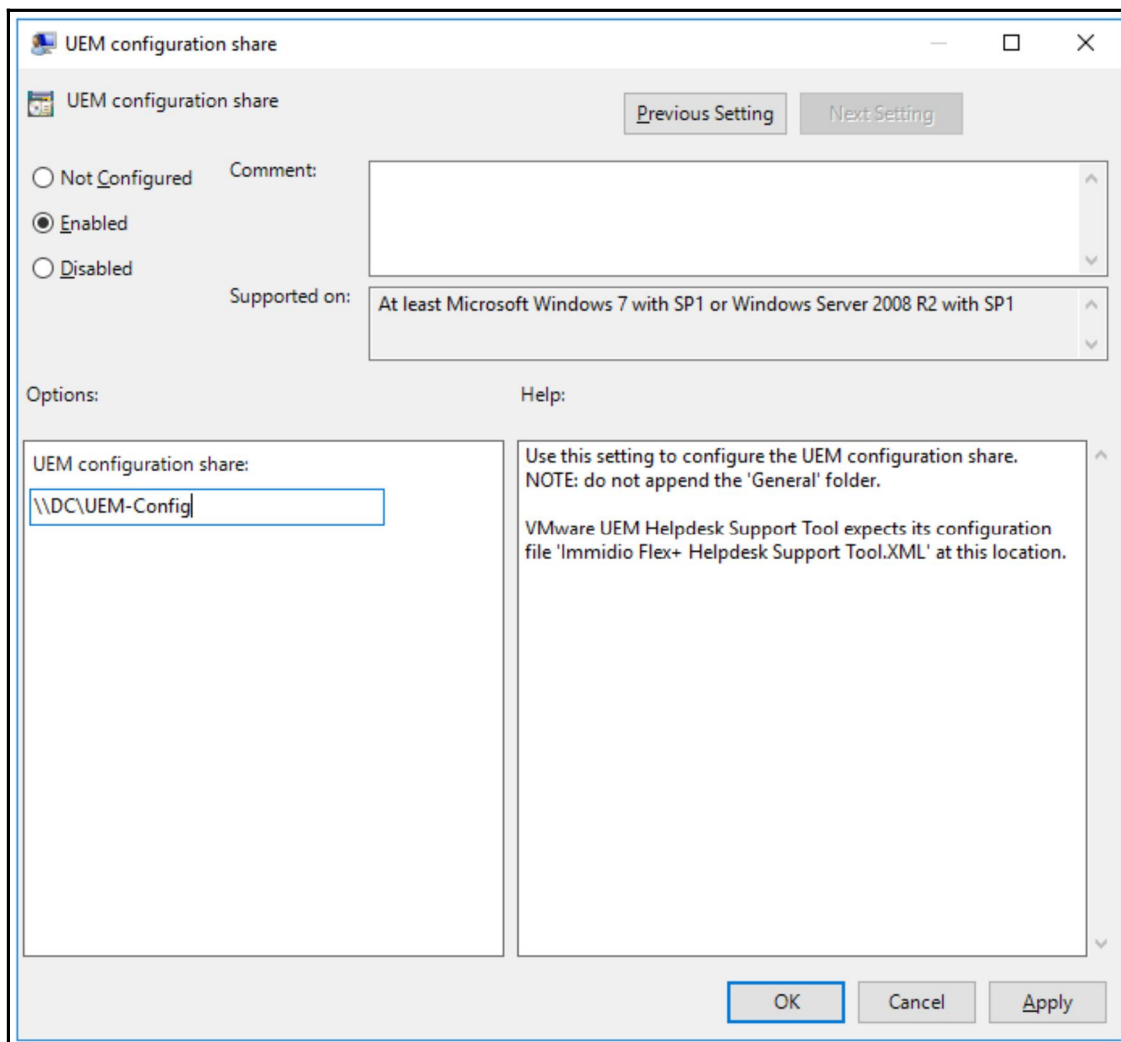
- **Allow editing profile archives:** Enabling this setting allows IT support using the VMware UEM Helpdesk Support Tool to be able to edit profile archives.



IMPORTANT: Take precautions when enabling this setting. VMware recommends only enabling this setting for experienced VMware UEM administrators. Manually editing profile archives is very error-prone and requires extensive knowledge of user profiles, including the registry. Making a mistake could render a profile archive inoperable.

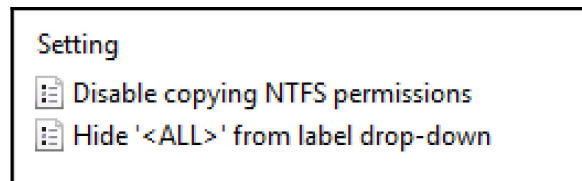
- **Allow showing profile archives in Windows Explorer:** Enabling this setting allows IT support staff using the VMware UEM Helpdesk Support Tool to jump directly to a profile archive in Windows Explorer.

- **Allow overriding the FlexEngine log level:** If you enable this setting, IT admins using the VMware UEM Helpdesk Support Tool can override the configured FlexEngine log level, forcing it to **Debug**.
- **Allow resetting multiple profile archives at the same time:** If you enable this setting, IT admins using the VMware UEM Helpdesk Support Tool can reset multiple profile archives at the same time.
- **UEM configuration share:** Use this setting to configure the UEM configuration share. Do not append the `General` folder. VMware UEM Helpdesk Support Tool expects its configuration file, `Immidio Flex+ Helpdesk Support Tool.XML`, at this location. The UEM configuration share is one of the policies you need to complete in order for UEM to work, so double-click on this policy to configure it, as shown in the following screenshot:



In the **UEM configuration share** box, type in the path details of where you want to store the UEM configuration files. In the example lab, this is entered as \\DC\UEM-Config.

There is also a subfolder containing a couple of additional policy options, as shown in the following screenshot:



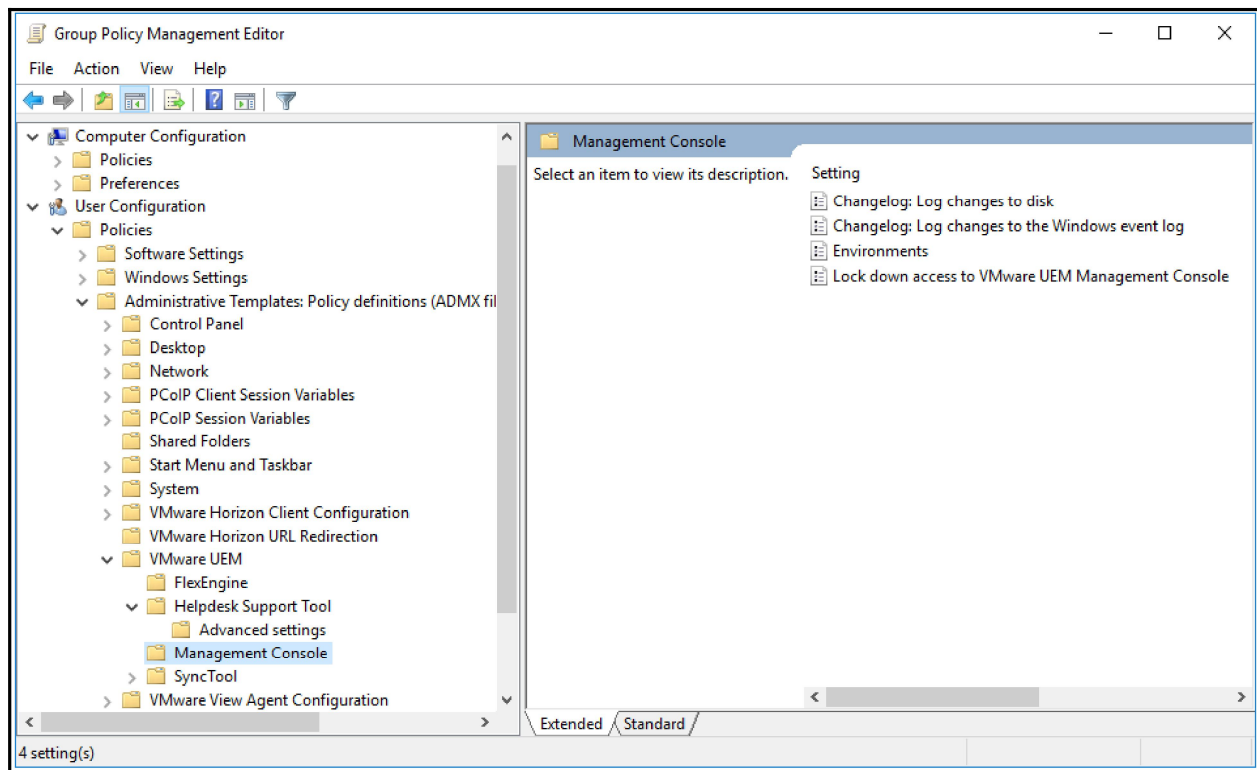
These policy options configure the following details:

- **Disable copying NTFS permissions:** By default, the VMware UEM Helpdesk Support Tool tries to correctly set the NTFS permissions for any files it creates, copies, or modifies. Enabling this setting prevents these actions from being performed.
- **Hide '<ALL>' from label drop-down:** Enabling this setting results in the label drop-down menu not including the <ALL> option.

Next, we are going to look at the Management Console policy configuration options.

Management Console policy configuration options

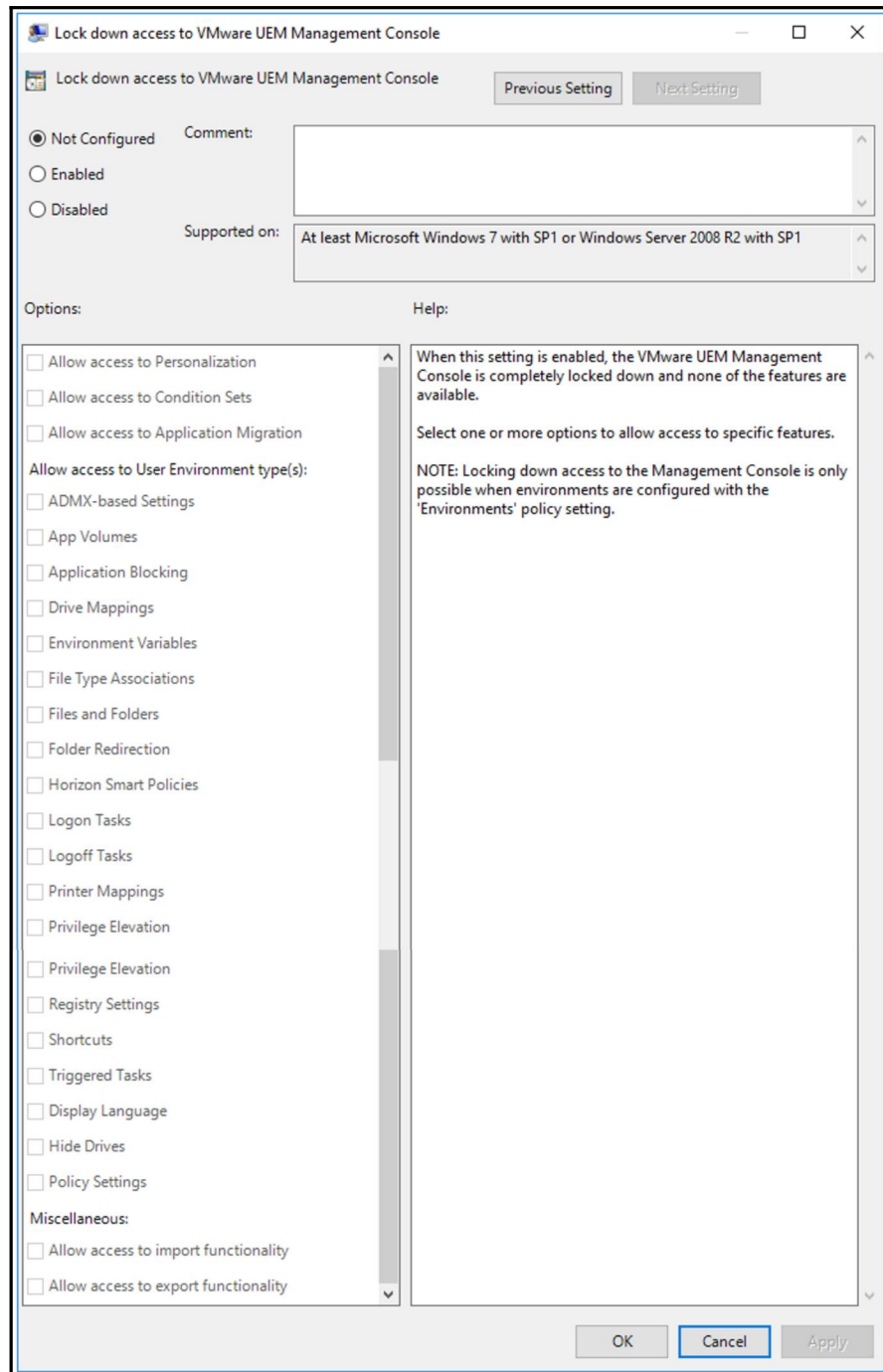
In this section, we are going to look at the Management Console configuration options. The following screenshot shows an overview of the available policies:



Let's have a look at each of these policy options and what they manage:

- **Changelog: Log changes to disk:** Enabling this setting allows you to keep a log of changes made to configuration files. Each change is logged to disk, and this `changelog` can be viewed within the VMware UEM Management Console.
 You can specify the maximum number of changes per configuration file that should be logged. Once this limit is reached for a configuration file, any additional changes to that file result in older change events being removed.
- **Changelog: Log changes to the Windows event log:** Enabling this setting allows you to keep a log of changes made to configuration files. Each change is logged to the Windows event log.
- **Environments:** Use this setting to configure one or more environments for VMware UEM administrators. In the **Environment definition(s)** dialog, click the **Show...** button and then enter the environments name in the first column, and enter the environment's UEM configuration share, for example, `\\DC\UEM-Config$`, in the second column.

- Lock down access to VMware UEM Management Console:** When enabled, the VMware UEM Management Console is completely locked down and no features are available. You have the option of specifying which features you want to allow access to. These features are shown in the following screenshot:

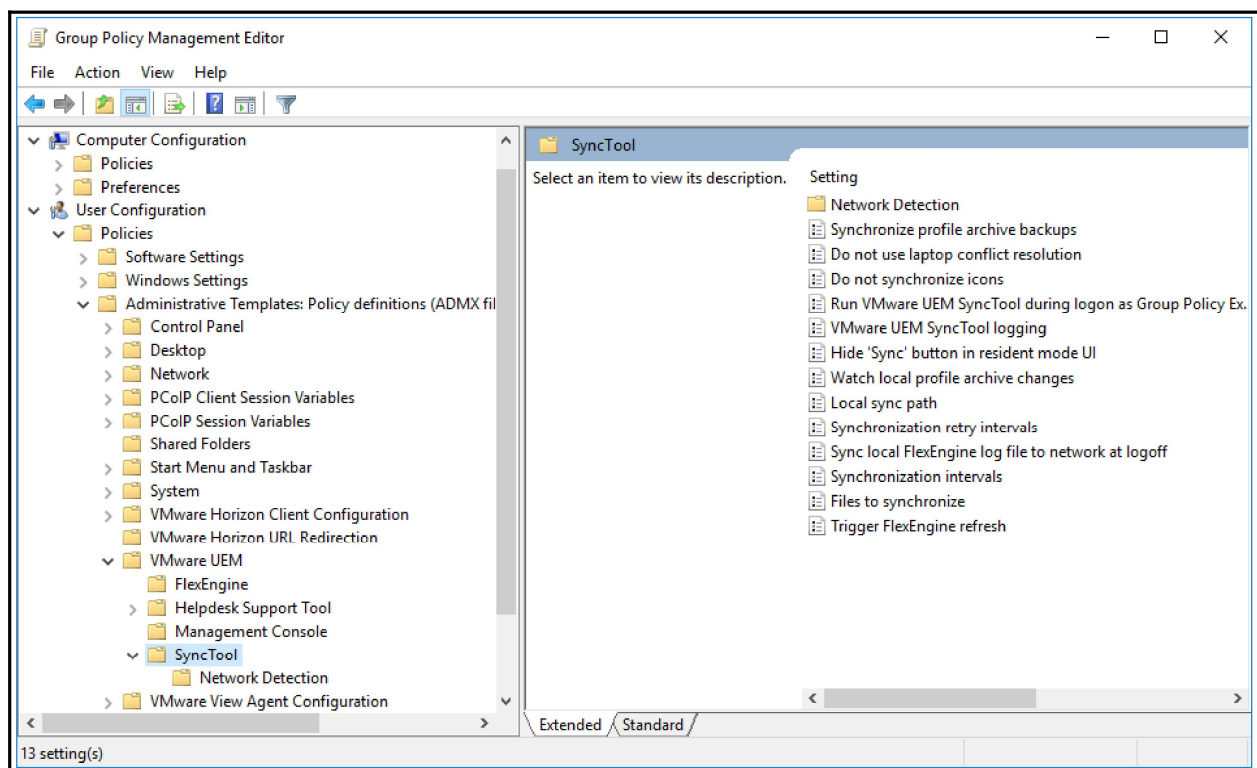


- Locking down access to the Management Console is only possible when environments are configured with the **Environments** policy setting.

Next, we are going to look at the `SyncTool` policy configuration options.

SyncTool policy configuration options

In this section, we are going to look at the `SyncTool` configuration options. The following screenshot shows an overview of the available policies:

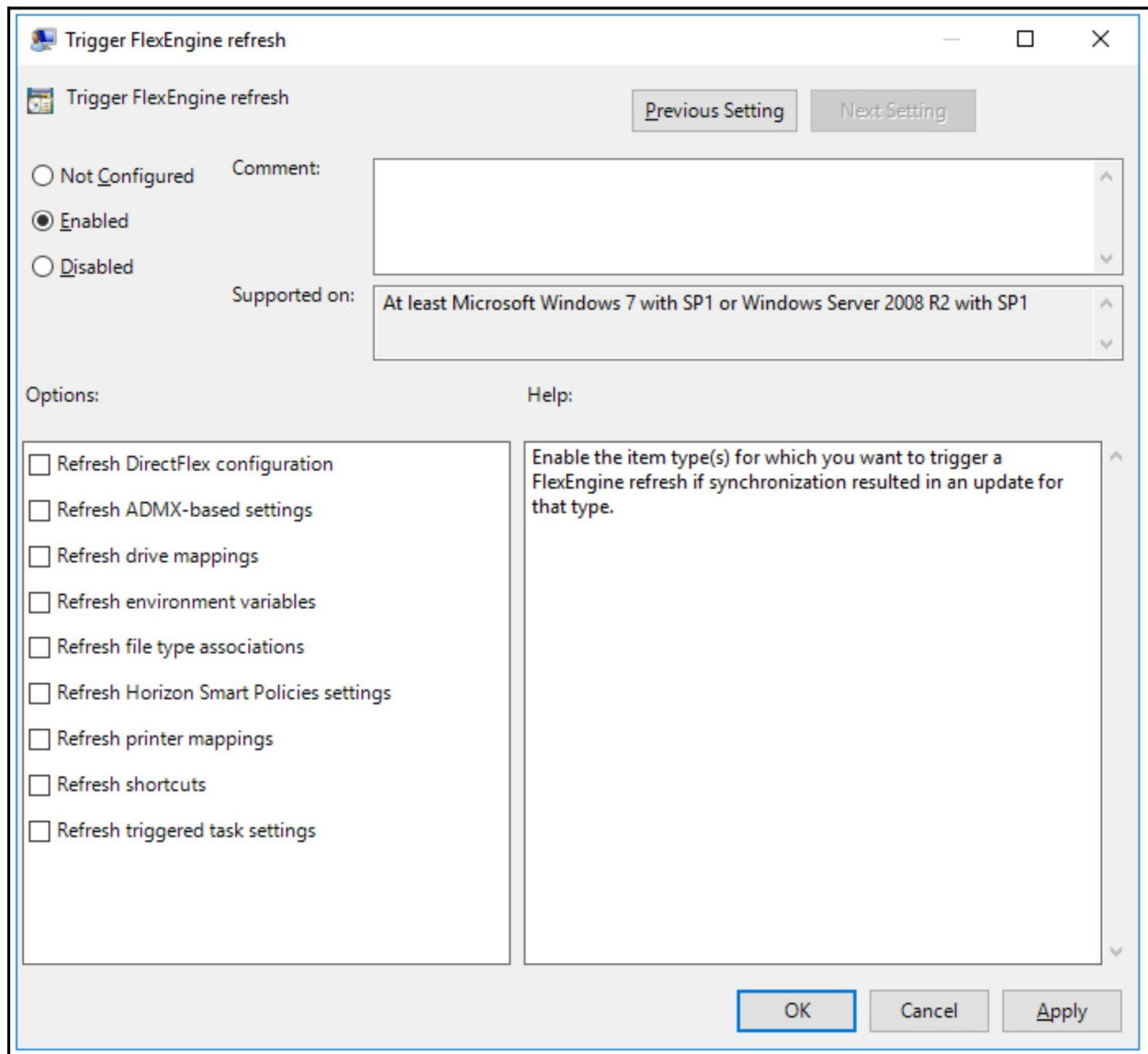


Let's have a look at each of these policy options and what they manage:

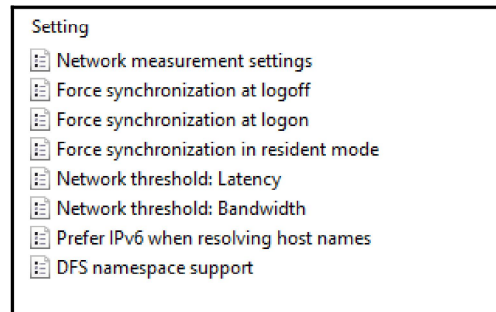
- **Synchronize profile archive backups:** This setting is to configure when the profile archive backups are synchronized. If you have configured backups to be synchronized during a session, you can additionally choose to only do this once per session. Backups are never synchronized at login. If you do not configure this setting, profile archive backups are never synchronized. You have the option to synchronize at logoff, during sessions and at logoff, or just during a session.
- **Do not use laptop conflict resolution:** This setting controls the behavior when a conflict is detected between a local and a central profile archive. A conflict occurs when both the local and central profile archives have changed since the last synchronization. The default setting will be for the local profile archive to win and be applied. If this setting is enabled, conflict resolution for laptops will not be applied and the profile archive with the most recent changes will win and be the one applied.
- **Do not synchronize icons:** If this setting is enabled, any `.ico` files are not synchronized.
- **Run VMware UEM SyncTool during logon as Group Policy Extension:** This setting enables the VMware UEM `SyncTool` to run during logon.
- **VMware UEM SyncTool logging:** If the **Create VMware UEM SyncTool log file** policy is enabled, a file called `FlexSync.log` is created in the configured Local Sync Path.
The log level controls the level of detail that is logged with the options for **Error**, **Warn**, **Info**, and **Debug**. Avoid using **Debug** or **Info** in production, as the amount of logging information can impact performance. If a maximum log file size is specified, the log file will be recreated once the configured size is reached. If the maximum log file size is set to 0, the file will grow indefinitely.
To log the most important sync status centrally, enable the **Create central sync status log file** policy. A file named `FlexSyncStatus-%COMPUTERNAME%.log` will be created during logoff, in the same folder as the log file of FlexEngine. If a maximum size is specified, the sync status log file will be truncated as specified. If the maximum size is set to 0, the file will grow indefinitely.

- **Hide 'Sync' button in resident mode UI:** If this setting is enabled, the **Sync** button is hidden in the resident mode UI.
- **Watch local profile archive changes:** Automatically triggers a synchronization in resident mode as soon as a local modification to a profile archive is detected; for example, when closing an application for which DirectFlex has been configured.
- **Local sync path:** This is the location where VMware UEM `SyncTool` stores all VMware UEM files. This should be configured to a local path that is unique to each user. For example, `%LOCALAPPDATA%\VMware UEM`.
- **Synchronization retry intervals:** During resident mode, if synchronization fails or is not allowed due to network thresholds, a retry is performed periodically. You can often configure the retry happens for the `FlexConfig`, `FlexRepository`, and the `Profile` archives. If you do not configure this setting, then, by default, a retry will happen every 5 minutes.
- **Sync local FlexEngine log file to network at logoff:** If this setting is enabled, the local `FlexEngine` log file will be uploaded to the central location. The name of the log file will be modified to include the computer name.
- **Synchronization intervals:** During resident mode, synchronization will occur periodically. Configure this setting to specify how often this happens. If you do not configure this setting, synchronization takes place every hour.
- **Files to synchronize:** By default, the UEM `SyncTool` synchronizes both Flex configuration files and user-specific profile archives, profile archive backups, and log files. Use this setting to synchronize only the configuration files or the user-specific files.

- **Trigger FlexEngine refresh:** Enable the options for which you want to trigger a FlexEngine refresh if synchronization resulted in an update for that type. The configurable options are shown in the following screenshot:



There is also a subfolder containing additional policy options, as shown in the following screenshot:



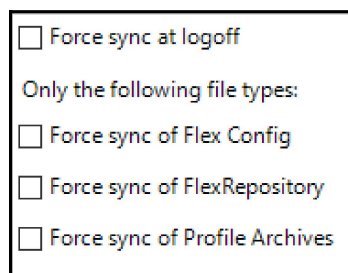
These policy options configure the following details:

- **Network measurement settings:** These settings control how network measurements are performed when network thresholds are configured. The ping cache setting controls how long network measurement results are remembered, to prevent performing multiple measurements for VMware UEM network paths hosted on the same server. If these settings are not configured, 3 pings will be done of 2,048 bytes with a timeout of 5 seconds. The default ping cache is 60 seconds. You can manually configure the values of these settings.



If you have not configured network thresholds, you do not need to configure these settings.

- **Force synchronization at logoff:** When network thresholds do not meet the configured requirements during logoff, synchronization does not occur. These settings will override this behavior. Enable **Force sync at logoff** to always synchronize all VMware UEM files at logoff. If you want to only synchronize certain file types, you can select one or more of the other options from the list, as shown in the following screenshot:





If you have not configured any network thresholds, then you do not need to configure these settings.

- **Force synchronization at logon:** As with the previous policy, **Force synchronization at logon** delivers the same results but this time at user login. Again, if you want to only synchronize certain file types, you can select one or more of the other options from the list, as shown in the previous screenshot. Like the previous policy, if you have not configured network thresholds, you do not need to configure these settings.
- **Force synchronization in resident mode:** Like the previous two policies, **Force sync in resident mode** allows you to always synchronize all VMware UEM files when in resident mode. If you want to synchronize only certain file types, you can select one or more of the other options from the list, as shown in the previous screenshot. Like the previous two policies, if you have not configured network thresholds, you do not need to configure these settings.
- **Network threshold: Latency:** This allows you to specify the maximum latency acceptable for synchronization to occur. This setting can be combined with the bandwidth threshold.
- **Network threshold: Bandwidth:** This allows you to specify the minimum bandwidth that should be available to allow synchronization to occur. This setting can be combined with the latency threshold.
- **Prefer IPv6 when resolving host names:** To perform network measurements, host names must be resolved to IP addresses. This setting controls the behavior when a hostname resolves to both IPv4 and IPv6.



If you have not configured network thresholds, you do not need to configure this setting.

- **DFS namespace support:** When using DFS namespaces to store VMware UEM files, this setting must be enabled to perform network measurements correctly.



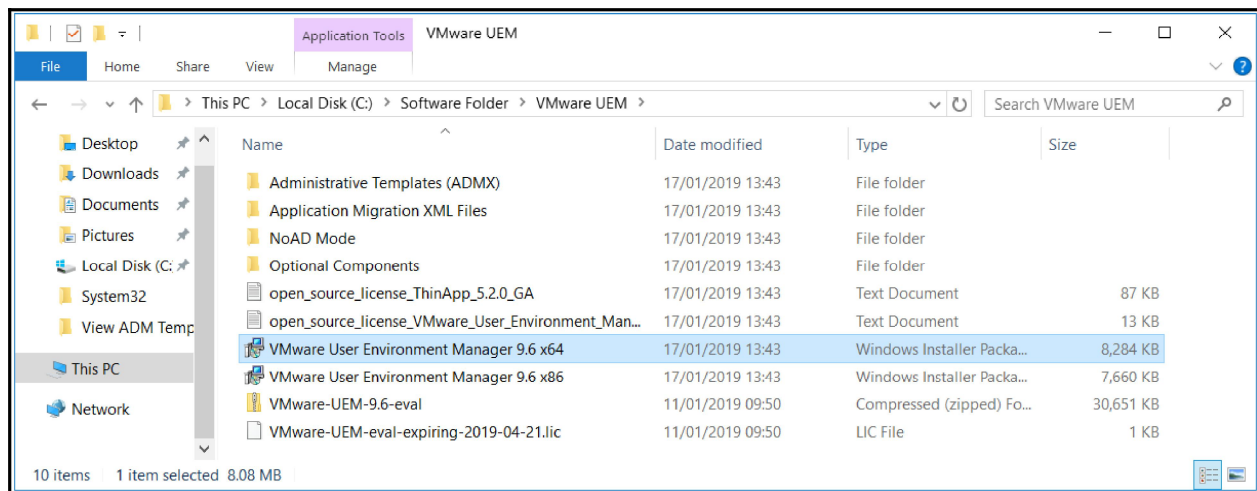
If you have not configured network thresholds, you do not need to configure this setting.

We have now covered all of the available Group Policy settings for UEM. In the next section, we are going to continue the installation process and install the VMware UEM Agent.

Installing the UEM Agent

The final element you need to install is the UEM Agent. This needs to be installed on every desktop that you want to manage using UEM. With VDI, this should be rolled out easily, as you can include the agent as part of the parent image, which then gets automatically deployed as you build and create virtual desktop machines.

To install the UEM Agent, locate the installer software that you copied to the shared software folder on the domain controller. This is the same installer file that we used to install UEM previously. This is shown in the following screenshot:

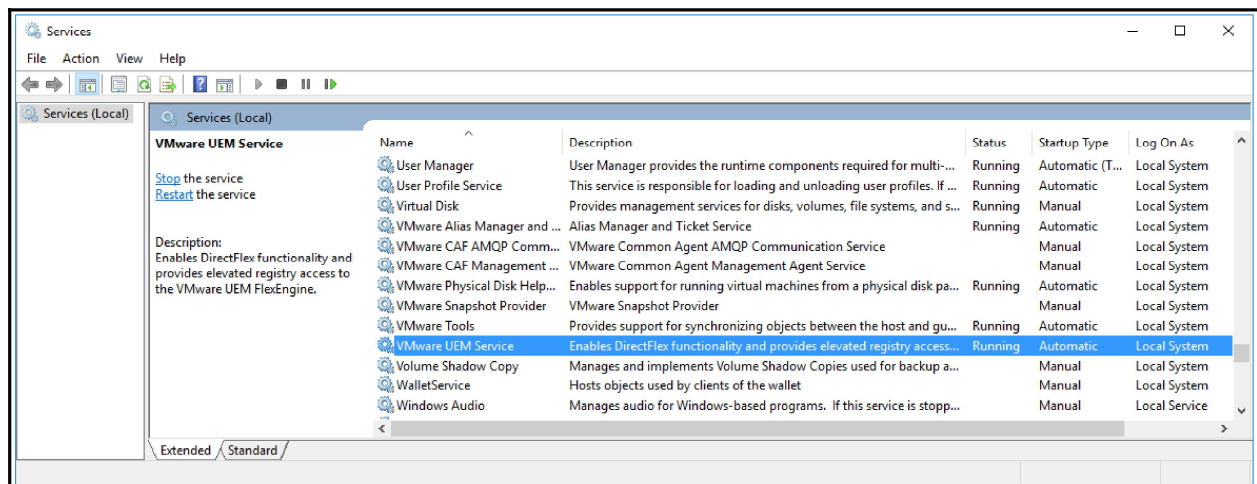


Now follow the steps as described to completed the installation of the UEM Agent:

1. Double-click the VMware User Environment Manager 9.6 x64 file to launch the installer.
2. You will now see the **Welcome to the VMware User Environment Manager Setup Wizard** screen.
3. Click **Next** to continue.
4. You will now see the **VMware End User License Agreement** screen. Check the box to accept the agreement and then click **Next** to continue.
5. Next, you will see the **Destination Folder** screen.
6. Leave the folder as the default and click **Next** to continue.

7. The next screen is for **Choose Setup Type**.
8. On this screen, click the **Custom** button.
9. Now, click the option for **VMware UEM Management Console**, and then from the menu, select the **Entire feature will be unavailable** option. This will ensure that the Management Console is not installed on this machine.
10. Click **Next** to continue.
11. You will now see the **Choose License File** screen. Click the **Browse...** button and from the **Open** dialog box, navigate to the appropriate license file, highlight it, and then click the **Open** button. You will now return to the **Choose License File** screen, which will now display the path to the license file that you have just selected.
12. Click **Next** to continue.
13. You will now see the **Ready to install VMware User Environment Manager** screen.
14. Click the **Install** button to start the install.
15. Once the installation has finished, you will see the **Completed the VMware User Environment Manager Setup Wizard**.
16. Click the **Finish** button to complete the installation and close the installer. You have now installed the UEM Agent on the virtual desktop machine.

To check that the agent has installed, launch the **Services** manager console by opening a **Run** dialog box and typing in `services.msc`. You will then see the following screenshot:



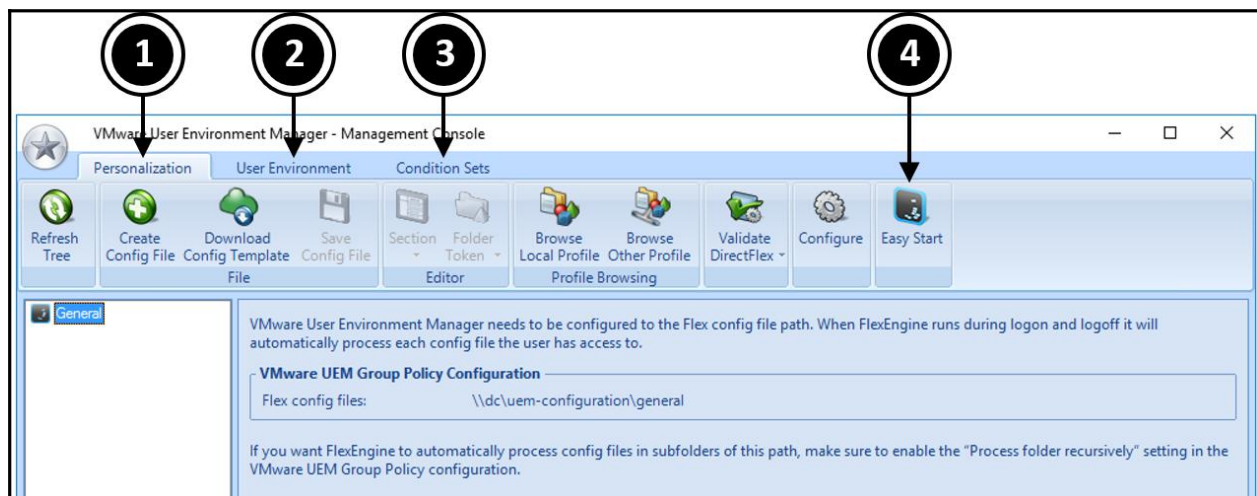
Scroll down to **VMware UEM Service**, and check that the status is set to **Running**.

Once you are happy the agent is installed and running, close the **Services** screen. In the next section, we will take a look at some of the UEM features available in the console.

A high-level overview of the UEM features

Unlike Persona Management, UEM is administrated from a graphical user interface. In this section, we are going to cover a high-level overview of the functionality of UEM by way of an introduction to get you started and show how you would go about configuring user profiles. As there are so many options and configurations, it makes sense to show you how to work with UEM and then let you customize it to match your end user requirements.

To start with, launch the Management Console from the server onto which you installed it. You will see a number of menu options, as shown in the following screenshot:



Across the top, you will see tabs for the following different configuration areas:

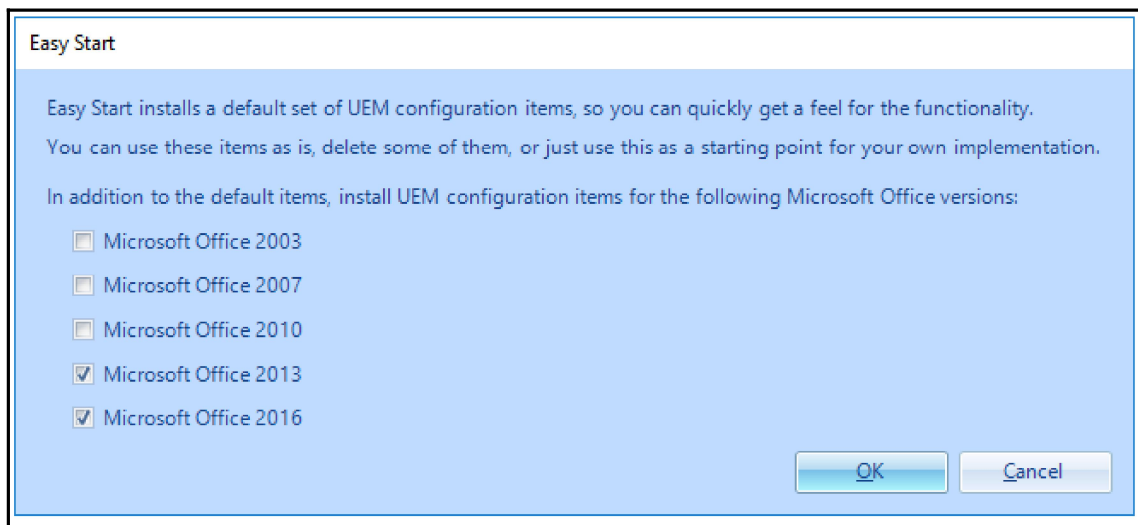
- **Personalization (1)**
- **User Environment (2)**
- **Condition Sets (3)**

There are also a number of icons for creating, downloading, saving, and browsing profiles.

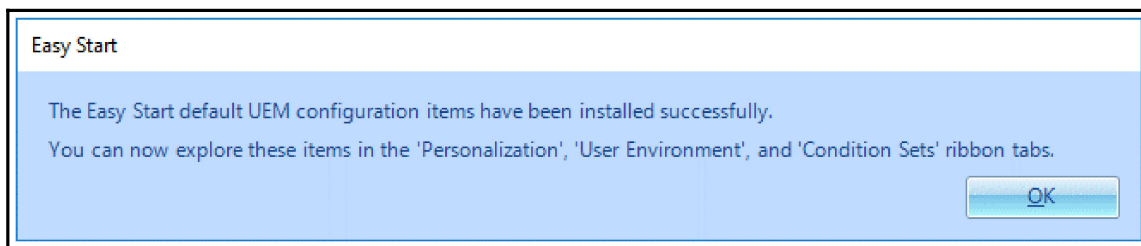
We will cover these options throughout this section, but before we do, you will also see an option for **Easy Start (4)**, so let's start there.

Easy Start

As the name suggests, **Easy Start** allows you to get up and running quickly by installing a common set of default configurations. It also allows you to install the most common settings for various different versions of Microsoft Office quickly, as shown in the following screenshot:

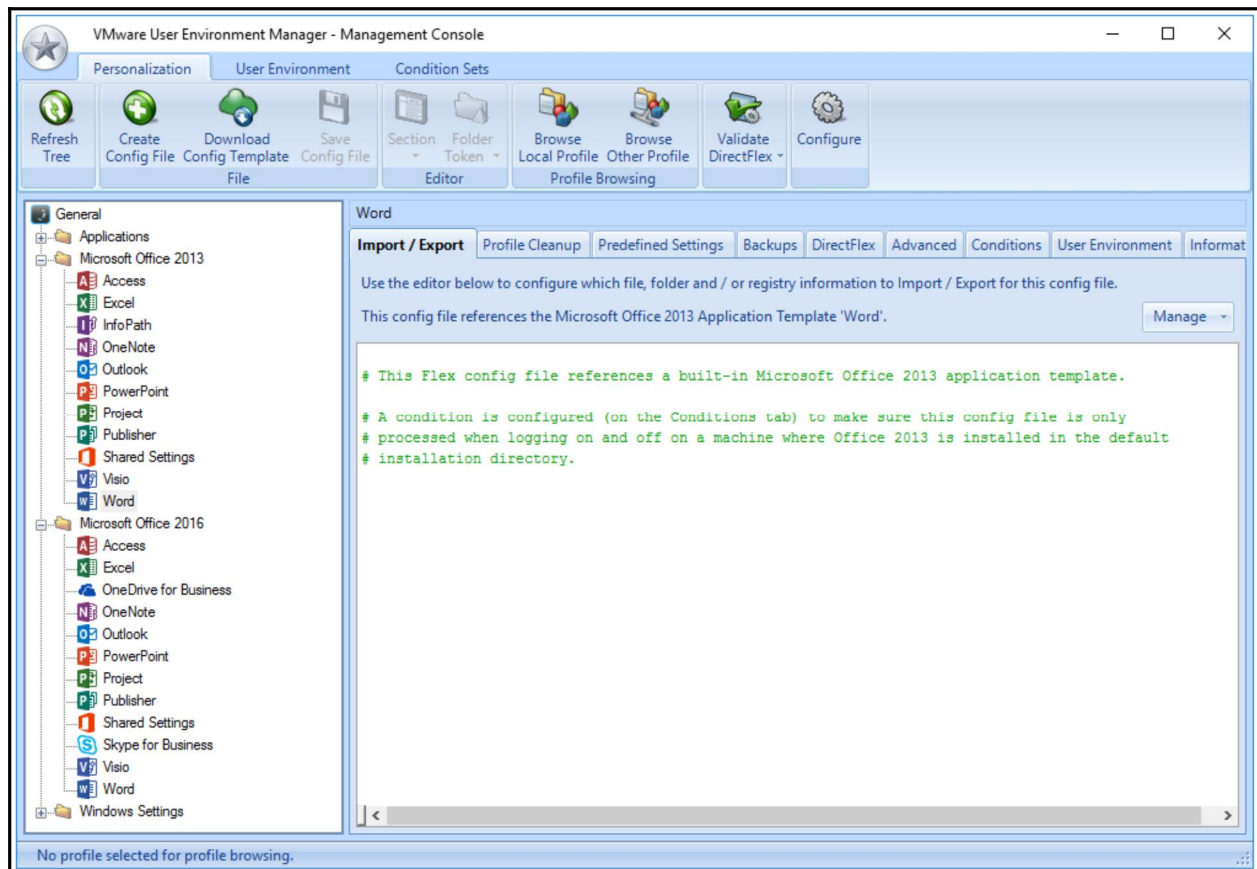


In the example lab, we are going to check the boxes for the versions of Microsoft Office we want to add to the configuration; in this case, **Microsoft Office 2013** and **2016**. UEM will install a set of default configurations relevant to the versions of Office you select. Once selected, click the **OK** button. You will then see the configuration being installed and, once complete, you will see the following screenshot:



Click the **OK** button to close the dialog box.

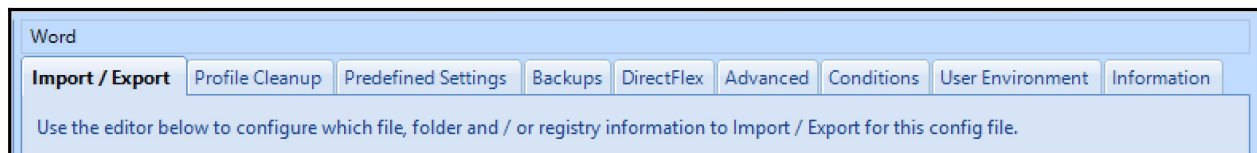
You will return to the main console screen, which will now show the settings you just configured with **Easy Start**. You can, of course, edit these as required, but this gives you a good starting point:



Now that we have some policy templates installed, let's walk through the feature tabs along the menu bar and look at the functionality of each one.

Personalization

As the name suggests, the settings under the **Personalization** tab allow you to personalize the way that apps are delivered to the end users. In the left-hand pane, as part of the default configuration we installed, there are a number of application templates for various applications in your environment. Clicking on an application allows you to configure its behavior when a user launches it. You can add things such as predefined settings, backup policies, and so on from the tabs in the right-hand pane:

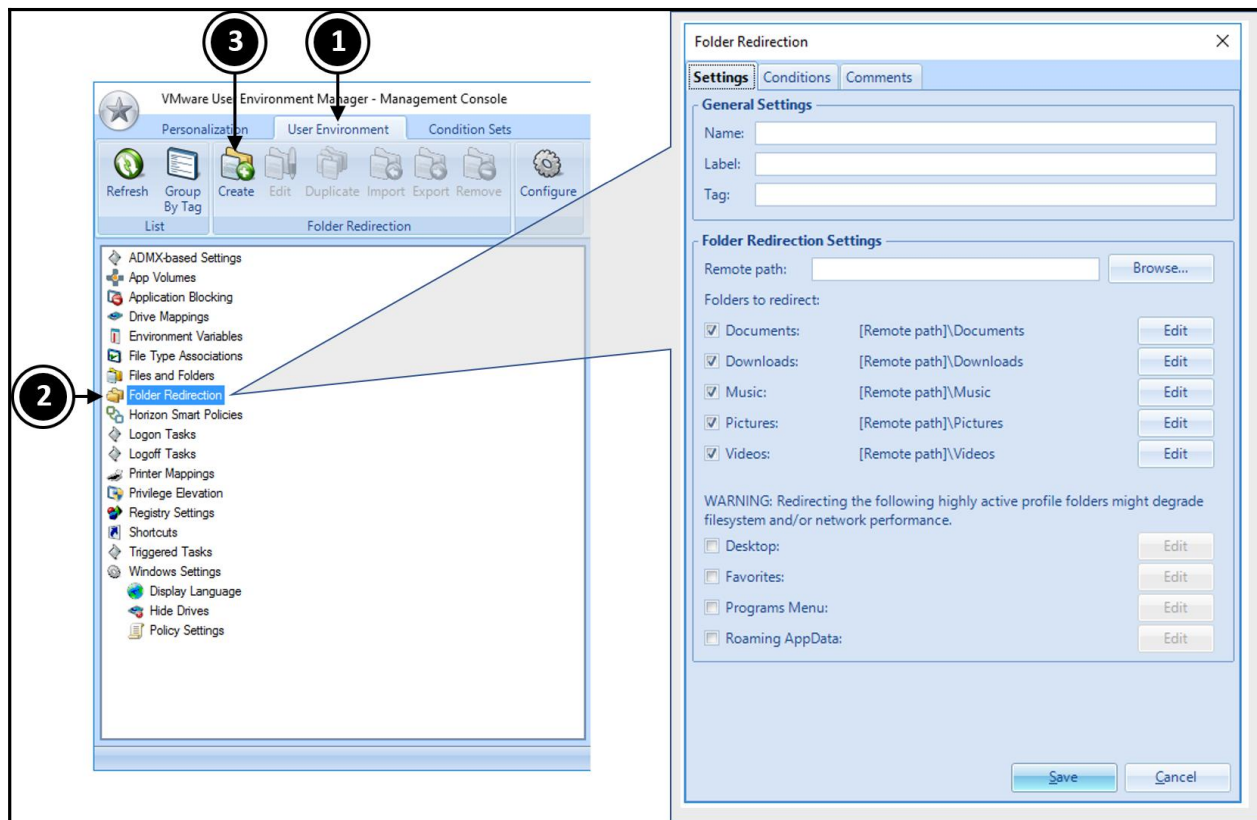


You can also create your own templates by clicking the **Create Config File** button. These config files are stored in the shared folder at `\\DC\UEM-Configuration`, which we created previously.

User Environment

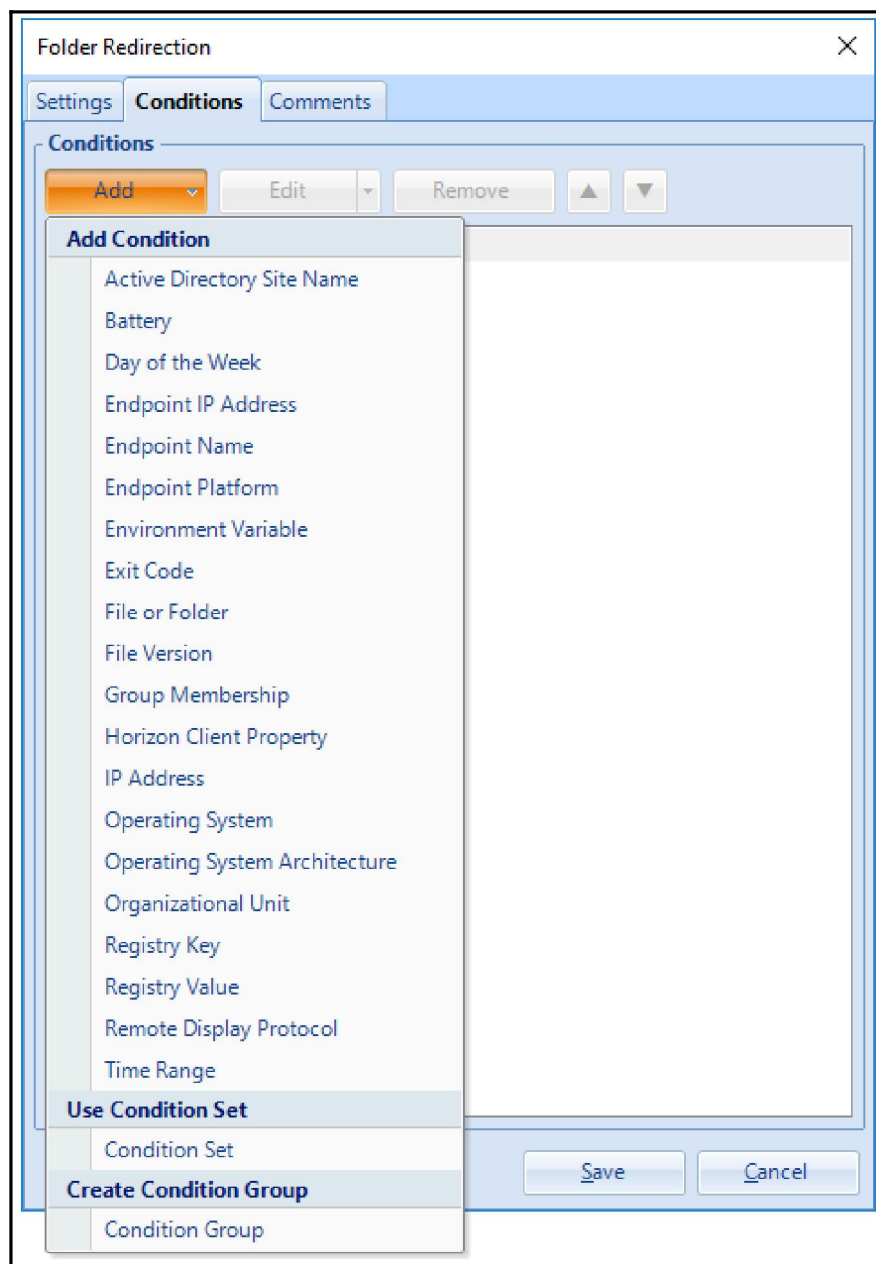
Under the **User Environment** tab, you can configure specific variables to define the user environment, including items such as **Folder Redirection**, **Printer Mappings**, and **Driver Mappings**.

To configure a specific item, click the **User Environment** tab (1) and then from the list of options on the left, select the option you want to create a new setting for. In this example, we have selected **Folder Redirection** (2). Now click the **Create** button (3), as shown in the following screenshot:



You will then see the **Folder Redirection** configuration options. Here, you can change the settings for the type of folders to redirect, for example. There is also a **Conditions** tab that allows you to apply the settings based on the conditions being met.

The conditions are shown in the following screenshot:



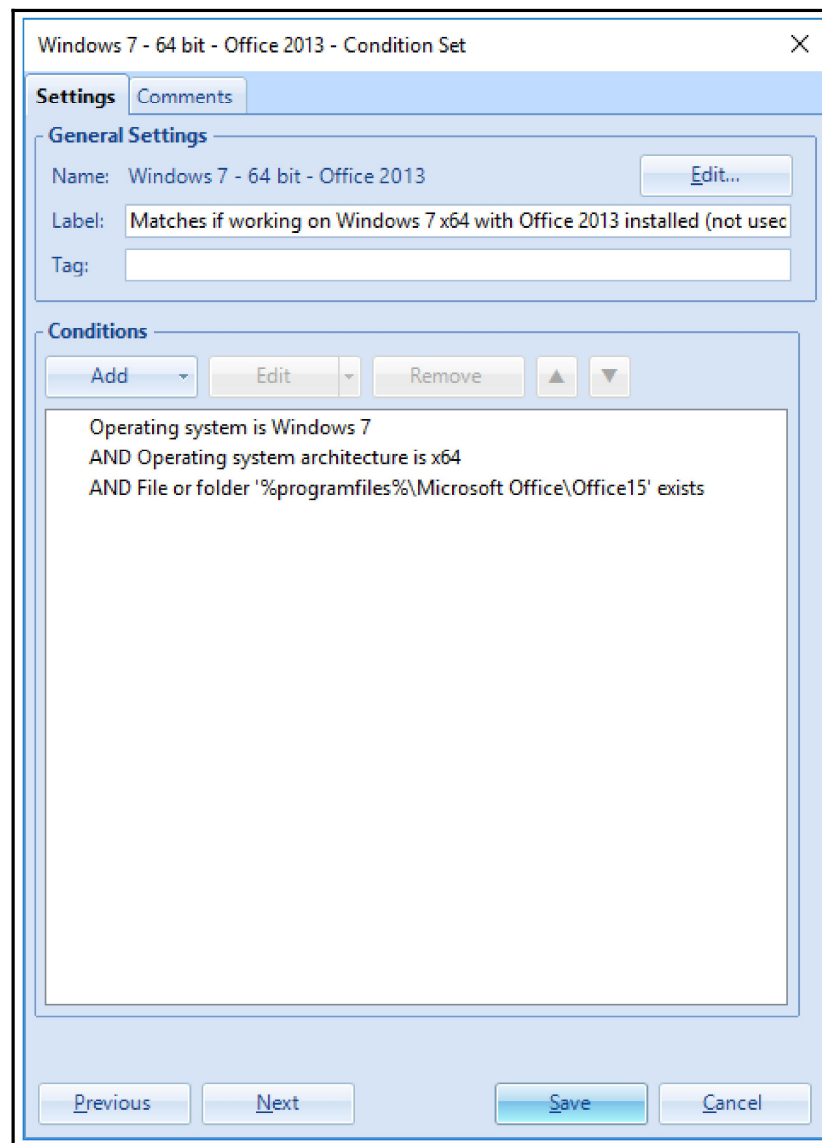
You will also notice you have a separate **Conditions** tab along the top, which we will look at in the next section.

Condition Sets

With the **Condition Sets** option, you can configure particular conditions for when UEM will apply a particular policy or setting.

For example, you may want to install a specific printer or mapped drive based on what the user is running. Maybe this setting would only apply only if the user was running the Windows 7 operating system, if the operating system was a 64-bit version, and they were running Microsoft Office 2013.

In this example, you could create a condition set that looks something like the following screenshot:



In the previous sections, we have only scraped the surface of the features delivered by VMware User Environment Manager. The idea is that we have shown you how to get up and running. Now you have the solution installed, you can now look at the different options and how best to configure them to suit your environment and your end users' requirements.



For more details, refer to the admin guide, which you can find on the VMware UEM documentation page, available <https://docs.vmware.com/en/VMware-User-Environment-Manager/index.html>

Summary

In this chapter, we have discussed why you need to manage your user environment differently when deploying a virtual desktop infrastructure environment. We then went on to look at the two VMware solutions that are part of the Horizon solution: Horizon View Persona Management, and VMware User Environment Manager.

We explored both solutions and what each one offers, as well as why you would want to deploy them. Once we had discussed this, we then went on to examine how each solution is installed and configured, which was followed by an in-depth look at the AD Group Policy settings.

Finally, for UEM, we took a brief look at the Management Console to demonstrate some of the additional capabilities that it offers. In the next chapter, we will discuss the newest feature in Horizon Advanced, Application Publishing.