Quick-Start Tutorial for User Environment Manager
# Table of Contents

Technical Introduction to User Environment Manager and Its Features

Overview ........................................................................................................................................ 5
Packaging and Licensing .............................................................................................................. 6
Features.......................................................................................................................................... 7
Use Cases .....................................................................................................................................10

Components and Architecture of User Environment Manager ................................................ 12
Components of User Environment Manager ..........................................................................13
Architecture of User Environment Manager............................................................................14

Installation ...............................................................................................................................................16
Overview of User Environment Manager Installation Steps..................................................17
Software Prerequisites ...............................................................................................................18
Create and Configure the User Environment Manager Configuration Share .....................19
Create and Configure the Profile Archives Share....................................................................24
Install the User Environment Manager Agent (FlexEngine) on the Desktop or RDSH Server ...............................................................................................................36
Install the User Environment Manager Management Console .............................................41
Configure the User Environment Manager Management Console ......................................44

Initial Configuration Using an Active Directory Group Policy Object................................................48
How the Group Policy Object Settings Work ...........................................................................49
Copy the Administrative Templates to the Domain Controller .............................................50
Create and Configure the FlexEngine Group Policy Object ...................................................54

Initial Configuration Using NoAD Mode ...............................................................................................65
Introduction and Prerequisites for Using NoAD Mode ..........................................................66
Create the User Environment Manager NoAD Configuration File ........................................67
Install the User Environment Manager Agent in NoAD Mode...............................................70

Basic Features .........................................................................................................................................76
Enable the Easy Start Feature....................................................................................................77
Test Application Personalization...............................................................................................83
Create an Application Template with Application Profiler .....................................................93
Configure User Environment Settings....................................................................................106
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Features</td>
<td>124</td>
</tr>
<tr>
<td>Configure Application Blocking</td>
<td>125</td>
</tr>
<tr>
<td>Configure Privilege Elevation for Installing an Application</td>
<td>147</td>
</tr>
<tr>
<td>Horizon Smart Policies</td>
<td>158</td>
</tr>
<tr>
<td>Introduction to Horizon Smart Policies</td>
<td>159</td>
</tr>
<tr>
<td>Create a Basic Smart Policy for Internal Users</td>
<td>163</td>
</tr>
<tr>
<td>Create a Smart Policy Based on User Group</td>
<td>172</td>
</tr>
<tr>
<td>Verify That a Smart Policy Is Being Applied</td>
<td>180</td>
</tr>
<tr>
<td>Summary and Next Steps</td>
<td>186</td>
</tr>
<tr>
<td>Introduction</td>
<td>187</td>
</tr>
<tr>
<td>Terminology Used in This Tutorial</td>
<td>188</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>189</td>
</tr>
<tr>
<td>About the Authors</td>
<td>190</td>
</tr>
</tbody>
</table>
Technical Introduction to User Environment Manager and Its Features
Overview

*VMware User Environment Manager™* delivers personalization and centrally managed policy configurations across virtual, physical, and cloud-based Windows desktop environments. IT administrators control which settings users are allowed to personalize, and administrators can map environmental settings such as network drives and location-specific printers.

User-specific Windows desktop and application settings can be applied in the context of client device, location, or other conditions. Policies are enforced when users log in, launch an app, reconnect, or when some other triggering event occurs.

User Environment Manager also has a feature for configuring folder redirection for storing personal user data, including documents, pictures, and so on.

Purpose of This Tutorial

The Quick-Start Tutorial for User Environment Manager helps you evaluate User Environment Manager by providing a discussion of the product and offering practical exercises. This Overview is first in the series of articles within the Quick-Start Tutorial and introduces User Environment Manager and its benefits, features, components, and architecture. Other articles in the tutorial offer hands-on exercises to set up your own proof-of-concept environment.

**Important:** This tutorial is designed for evaluation purposes only, based on using the minimum required resources for a basic deployment, and does not explore all possible features. This evaluation environment should not be used as a template for deploying a production environment. To deploy a production environment, see the [User Environment Manager Documentation](#).

Audience

This tutorial is intended for IT administrators and product evaluators who are familiar with *VMware vSphere®* and *VMware vCenter Server®*. Familiarity with networking and storage in a virtual environment, Active Directory, identity management, and directory services is assumed. Knowledge of other technologies, such as *VMware Horizon® 7* is also helpful.
Packaging and Licensing

User Environment Manager can be used as a standalone product, to manage applications and Windows environment settings, or it can be used in conjunction with other VMware components. For example, User Environment Manager is a key component of JMP, the next generation of desktop and application delivery. JMP (pronounced \textit{jump}), which stands for Just-in-Time Management Platform, represents capabilities in VMware Horizon 7 Enterprise Edition that deliver Just-in-Time Desktops and Apps in a flexible, fast, and personalized manner.

User Environment Manager can manage applications installed in the base image of a virtual desktop machine or RDSH server, and it can manage applications provided by \textit{VMware App Volumes}. User Environment Manager also includes Horizon Smart Policies, for integrating with Horizon 7 and Horizon Apps. For more information, see the \textit{VMware Workspace ONE and VMware Horizon Packaging and Licensing guide}. 
Features

Following are descriptions of the core features and capabilities of User Environment Manager. In subsequent articles of this Quick-Start Tutorial, you will walk through some of these features and some advanced features, including application blocking, and privilege elevation, which allows end users to install and run applications that normally require administrator privileges.

Centralized and Simplified Management of Windows Environments

With User Environment Manager, you can configure settings and conditions in the Management Console, and the User Environment Manager agent on virtual desktops and RDSH servers can read and apply the settings. For configuring User Environment Manager, you have the flexibility of configuring policies by using any of the following strategies:

- Using an Active Directory Group Policy Object with the VMware-supplied administrative templates.
-Specifying command-line options to use with the FlexEngine executable, which is the User Environment Manager agent.
-Editing the XML Flex configuration file for User Environment Manager. This strategy is called NoAD mode.

You can also use a single instance of the User Environment Manager Management Console to manage multiple User Environment Manager environments.

Dynamic, Contextual Policy Management

With User Environment Manager, you can specify the conditions under which an end user gets certain features, such as the ability to disable saving files to a USB device when outside the corporate network, or other security-related features. You can also configure triggering tasks to determine when to check for certain conditions, such as at login time. For more information, see the blog post Using VMware User Environment Manager to Manage User Profiles with Context-Based Settings.

Consistent User Experience Across Devices and Locations

With User Environment Manager, end users can roam between disparate devices while preserving custom application settings and Windows personalization settings. When a user logs in to a virtual desktop or application, User Environment Manager reads the profile archive file for that user's profile and can, for example, display the desktop background or application settings that the user saved during the last session, regardless of whether the actual endpoint device was a desktop computer at work or an iPad at home.
Easy Start for Adding Applications and Environment Settings to Manage

User Environment Manager takes a whitelist approach to managing the user profile. Given this design approach, IT must specify which applications and settings will be managed. Although this approach takes a little more work up front, this solution prevents excessive profile growth and profile corruption, enables user settings to roam across Windows versions, and provides IT granular control to manage as much or as little of the user experience as needed.

The Easy Start feature gives you a jumpstart on the whitelist of applications and settings you want to manage. With a click of the Easy Start button, you can manage many common Windows applications, including several versions of Microsoft Office. Many Windows environment settings are also added by Easy Start. You can then easily select an application or Windows setting to review and change the default settings.

Application Templates and Application Profiler

Preserving user-specific application settings and applying or enforcing specific default application settings are key features of User Environment Manager. VMware provides application management templates for commonly used software packages, and the VMware User Environment Manager Community Forum contains many more templates created with an included tool called Application Profiler.

For applications that do not have a corresponding application management template, you can use the Application Profiler, a standalone application that analyzes where an application stores its file and registry configuration. The analysis results in an optimized User Environment Manager Flex configuration file, which you can edit in the Application Profiler or use directly. You can also use Application Profiler to set the initial configuration state of applications.

Self-Support Tool

With User Environment Manager Self-Support, end users can restore application settings from a backup or reset the settings to their defaults.

Helpdesk Support Tool

As a User Environment Manager administrator, you can use Helpdesk Support Tool yourself, or you can make it available to another department that is in charge of providing support in the area of personalization. You can use Helpdesk Support Tool to perform the following tasks:

- Reset one or more profile archives for a user.
- Restore a profile archive backup for a user.
- Open a profile archive for a user in Windows Explorer.
• Edit a profile archive for a user.
• View User Environment Manager agent log files for a user, and search for a specific log string.
• View the total size of profile archives and profile archive backups for a user.
Use Cases

This article explains some of the most popular reasons why enterprises use User Environment Manager.

Saving Users' Settings Across Devices

End users are using more devices than ever before, and expect a consistent user experience when accessing corporate resources. As IT explores virtual desktop infrastructure (VDI), published applications, and even cloud computing to deliver these resources, User Environment Manager provides that consistent user experience through personalization.

Personalization abstracts the settings and preferences from the underlying Windows operating system and applications. End users are free to roam from a physical PC to a VDI desktop, or to a cloud-hosted published application. User Environment Manager persists the look and feel of Windows and applications, providing a superior user experience. Get hands-on in the exercise Test Application Personalization.

Improving Logon Times

Windows logon times directly impact the end-user experience. Whether managing physical or virtual PCs, VDI, or published applications, IT constantly struggles to find a balance between customizing the Windows environment and adding time to the user logon process. Tasks such as mapping printers, mapping drives, and applying policies to manage applications often occur during the user logon process. User Environment Manager uses DirectFlex technology to remove much of this overhead from the user logon process. Instead, these tasks are carried out dynamically, if and when they are needed.

Take an AutoCAD engineer as an example. The engineer has access to a shared drive that contains a variety of drawings, as well as a plotter printer. Using a typical logon script would likely map the drive and printer every time the engineer logs in to Windows, whether AutoCAD is used during the session or not. This process results in added logon time for components that are not used. With DirectFlex, User Environment Manager can dynamically map the drive and printer when AutoCAD is launched, and disconnect them when AutoCAD is closed. By removing such operations from the logon process, logon times for end users can be reduced. Get hands-on in the exercise Configure User Environment Settings.

Managing Least Privileges

User Environment Manager is not just about providing enhancements for end users. Many use cases focus on improving IT operations. For example, privilege management can be a daunting task, and many IT administrators are forced to provide Local Administrator privileges to end users to satisfy application demands.
With User Environment Manager privilege elevation, IT can strategically elevate permissions for application installers, as well as executables for applications already installed that require Local Administrator privileges to run. Elevating privileges for specific executables, while removing Local Administrator privileges from end users, can dramatically reduce the risk of a malware or ransomeware attack on your network. Privilege elevation is a key feature in any privilege management strategy. Get hands-on in the exercise Configure Privilege Elevation.

Providing Desktops Just in Time

As enterprises go down the path of VDI, a common question is whether to provide persistent or non-persistent desktops. Although end users enjoy the flexibility to customize their own, personal, persistent VM, IT often prefers the streamlined management of non-persistent VMs. User Environment Manager is a key component of the VMware Just-In-Time Management Platform (JMP), which provides the best of both worlds. To learn more about JMP, and the benefits User Environment Manager provides with this approach, see Deploying JMP (Just-in-Time Management Platform) in Horizon 7.
Components and Architecture of User Environment Manager
Components of User Environment Manager

This section provides a description of each component of User Environment Manager, which can be summarized in three parts:

1. **Management Console** – Primary application interface for IT to configure and manage User Environment Manager.
2. **FlexEngine** – Agent component, which is installed on the virtual or physical machines that you want to manage.
3. **File shares** – User Environment Manager relies on a folder hierarchy, which you will create in a later exercise. User Environment Manager stores configuration files in the configuration share. User data is stored in the profile archives share.

Before beginning the installation, its important to understand the terminology specific to User Environment Manager. The following User Environment Manager documentation topic, *User Environment Manager Infrastructure and Terminology*, provides a comprehensive list of User Environment Manager terminology.

(Approximate read time: **3 minutes**)
Architecture of User Environment Manager

This section provides an overview of the architecture so you can see how the components relate to each other. The following figure shows the architecture of a User Environment Manager installation. In the following descriptions, you refers to you, the IT administrator. All components of User Environment Manager that you deploy communicate between each other by using the SMB protocol.

- **User Environment Manager GPO** – You create a GPO for each Active Directory organizational unit (OU) you want to manage. The OU typically contains the computer objects for virtual machines you want to manage. You can then edit this GPO and apply User Environment Manager settings from administrative templates included in the User Environment Manager installation package.

- **User Environment Manager Management Console** – You use this User Environment Manager administrative UI to configure application settings, Windows environment manager settings, conditions under which the settings go into effect, and various other configuration settings and Horizon Smart Policies for things like printer mapping, attaching devices to the virtual desktop or application, and the ability to copy and paste text.

- **User Environment Manager Application Profiler** – For the few applications for which you cannot find an already-created application template, you can use this standalone application that analyzes where the application stores its file and registry configuration, and also set the initial configuration state of the application.

- **Central configuration share** – You create this file share to store the Management Console configuration and User Environment Manager configuration files. The User Environment Manager agent (FlexEngine) on virtual desktops and RDSH servers reads the configuration file on this share and applies the settings specified in the configuration file.

- **Network folder per user** – In this file share that you create, each folder, or profile archive, contains ZIP files where the User Environment Manager agent (FlexEngine) stores the
personalized settings of a user. For each User Environment Manager (Flex) configuration file that you create, FlexEngine creates a profile archive for each user.

- **User Environment Manager Helpdesk Support Tool** – This tool provides capabilities to support and maintain the User Environment Manager profile archives and profile archive backups.

- **Clients with User Environment Manager FlexEngine** – The agent software, FlexEngine, runs on each virtual desktop or RDSH server whose applications are to be managed. This agent reads the centralized configuration file, applies User Environment Manager settings, and saves those user settings that end users are allowed to control. In this client-server architecture, the FlexEngine agent software plays the *client* role, and the User Environment Manager Flex configuration file plays the *server* role.

- **SyncTool** – Laptop users who are not always connected to the corporate network need access to their User Environment Manager configuration files while offline. SyncTool makes all VMware User Environment Manager configuration files available locally and synchronizes changes when users connect to the corporate network. Additionally, users with a slow WAN connection can use local User Environment Manager configuration files, thus limiting network traffic and avoiding continuously roaming personal settings.
Installation
Overview of User Environment Manager

Installation Steps

The exercises in this Quick-Start Tutorial provide step-by-step guidance on completing each of the tasks outlined here, in the topic Overview of the User Environment Manager Deployment. (Approximate read time: 2 minutes)
Software Prerequisites

Before you can deploy User Environment Manager, you must verify that the Windows operating system versions and, optionally, the virtualization software you plan to use, meet certain requirements, as described in the following topic, Software Requirements. (Approximate read time: 2 minutes)
Create and Configure the User Environment Manager Configuration Share

The User Environment Manager configuration share is a central share on a file server. It contains all the configuration files for personalization and application configuration management. The FlexEngine agent on the managed machine reads configuration data from the User Environment Manager configuration share when a user logs in or logs out of the environment, or when the user opens or closes applications that are configured with DirectFlex.

Configuration Share Prerequisites

To complete this exercise, you will need the following.

• An Active Directory group containing one or more end-user accounts.
  In this exercise, the AD group Domain Users is used.

• An Active Directory group containing one or more IT Administrator accounts.
  In this exercise, the AD group Desktop Admins is used.

• A file server with a certain amount of storage and network connection speed, as described in the following User Environment Manager Configuration Share section.

(Approximate read time: 2 minutes)

1. Create the File Share Folder

1. On a file server, create a folder titled UEM_Config.
2. To configure sharing, right-click the UEM_Config folder and select Properties.
3. On the Sharing tab, select Advanced Sharing.
2. Configure Advanced Sharing

![Advanced Sharing dialog box]

Select Permissions to configure the share permissions.

3. Grant Read Permissions to End Users

![Permissions dialog box]

Select the Read check box for the Domain Users group, or whichever group you selected in Configuration Share Prerequisites.
4. Grant Read and Change Permissions to Administrators

Select the Read and Change check boxes for the Desktop Admins group, or whichever group you selected in Configuration Share Prerequisites.

5. Configure NTFS Permissions on the UEM_Config Folder
In the UEM_Config Properties dialog box, on the Security tab, select Edit.

6. Grant Full Control for Administrators

![Permissions for UEM_Config dialog box]

1. In the Group or user names list, select the Desktop Admins group.
2. In the Permissions for Desktop Admins list, select Full Control.

7. Grant Read & Execute Permissions for End Users

![Permissions for UEM_Config dialog box]

Quick-Start Tutorial for User Environment Manager
1. In the **Group or user names** list, select the **Domain Users** group.
2. In the **Permissions for Domain Users** list, select **Read & execute**.

   After you select **Read & execute**, the **List folder contents** and **Read** check boxes are automatically selected.

The following [Config Share](#) video provides a detailed demonstration of the steps outlined in this exercise. If you need additional detail, you can find it here. If you already have a configuration share, feel free to skip the video. This video is **2 minutes**.
Create and Configure the Profile Archives Share

The profile archives share stores the personal settings for users. The User Environment Manager agent (FlexEngine) creates a subfolder for each user. The share contains User Environment Manager profile archives, which are ZIP files. FlexEngine reads personal user settings from the profile archives share when a user logs in to the environment or launches a DirectFlex-enabled application. FlexEngine writes the modified settings when the user logs out, or closes a DirectFlex-enabled application.

Profile Archives Share Prerequisites

To complete this exercise, you need the following.

- An Active Directory group containing one or more end-user accounts.
  This should be the same group you used in Configuration Share Prerequisites. In this exercise, the AD group Domain Users is used.
- An Active Directory group containing one or more IT Administrator accounts.
  This should be the same group you used in Configuration Share Prerequisites. In this exercise, the AD group Desktop Admins is used.
- A file server with a certain amount of storage and network connection speed, as described in the following User Environment Manager Profile Archives Share topic. (Approximate read time: 4 minutes)

1. Create the Share Folder

1. On a file server, create a folder titled UEM_Profiles.
2. To configure sharing, right-click the UEM_Profiles folder and select Properties.
3. On the Sharing tab, select Advanced Sharing.

Quick-Start Tutorial for User Environment Manager
2. Configure Advanced Sharing

Select **Permissions** to configure the share permissions.

3. Grant Read and Change Permissions to End Users
Select the **Read** and **Change** check boxes for the **Domain Users** group, or whichever group you selected in **Profile Archives Share Prerequisites**.

4. **Grant Read and Change Permissions to Administrators**

Select the **Read** and **Change** check boxes for the **Desktop Admins** group, or whichever group you selected in **Profile Archives Share Prerequisites**.
5. Configure NTFS Permissions on the UEM_Profiles Folder

In the UEM_Profiles Properties dialog box, on the Security tab, select Advanced.
6. Add Desktop Admins as a Principal

1. Select Add.
2. In the Permission Entry for UEM_Profiles dialog box, click **Select a principle**, and add the **Desktop Admins** group as a principal.
7. Configure NTFS Permissions for Administrators

1. Verify that Desktop Admins is listed as the principal.
2. Verify that the Applies to drop-down list is set to This folder, subfolders and files.
3. Select the Full control check box.
8. Add Domain Users as a Principal

1. Select Add.
2. In the Permission Entry for UEM_Profiles dialog box, click Select a principle, and add the Domain Users group as a principal.
9. Configure Basic NTFS Permissions for End Users

1. Verify that Domain Users is listed as the principal.
2. Select the Read & execute, List folder contents, and Read check boxes.
3. Select Show advanced permissions.
10. Configure Advanced NTFS Permissions for End Users

1. Verify that the Applies to drop-down list is set to This folder only.
2. Select the Traverse folder / execute file, List folder / read data, Read attributes, Read extended attributes, Create folders / append data, and Read permissions check boxes.
11. Add the Creator Owner as a Principal

1. Select **Add**.
2. In the Permission Entry for UEM_Profiles dialog box, click **Select a principle**, and add the **Creator Owner** account as a principal.
12. Configure NTFS Permissions for the Creator Owner

1. Verify that Creator Owner is listed as the principal.
2. Set the Applies to drop-down list to Subfolders and files only.
3. Select the Full control check box.

The NTFS permissions for the UEM_Profiles folder should look like this.
The following Profile Share video provides a detailed demonstration of the steps outlined in the previous section. If you already created the configuration share, feel free to skip the video. If you need additional detail, you can find it here. This video is 2 minutes.
Install the User Environment Manager Agent (FlexEngine) on the Desktop or RDSH Server

FlexEngine, the User Environment Manager agent component, applies the policies that the IT administrator creates with the User Environment Manager Management Console. FlexEngine can be installed on physical, virtual, and cloud-based Windows devices. To install this component, you run the same VMware User Environment Manager Setup wizard that you will run later, to install the management console.

If you plan to create pools of virtual desktops or farms of RDSH servers, you can install FlexEngine on the master VM before creating the pool or farm. For example, in the following exercise, FlexEngine is installed on a Windows 10 virtual machine, referred to as the template VM. This template VM is later used to create a pool of Horizon 7 instant-clone desktops.

Prerequisites for FlexEngine Installation

To perform this exercise, you need the following:

- **User account** – When you log in to the OS to run the installer, the account you use must have administrative privileges.
- **Installer** – If necessary, you can download the installer from the Product Evaluation Center or the VMware Downloads page. The installer is an architecture-specific (x86 or x64) MSI file.
- **License** – The installation wizard prompts for the path to a valid license file unless VMware Horizon Agent is already installed in the VM. (User Environment Manager is included with Horizon 7 Enterprise Edition.) See Licensing Requirements.
- **Windows Registry** – The Windows Registry on the VM must be accessible to User Environment Manager so that new entries can be written. See Registry Access Requirements.
- **Internet access** – The installation process includes a certificate revocation check to verify the digital signature of the MSI file. This check requires Internet access.
- **Windows OS** – The machine must be running a supported Windows version. For the example in this exercise, Windows 10 is used.

**Note:** For the purposes of this exercise, you can install the agent on a physical or a virtual machine that you want to manage. For details about how to create a VM used for virtual desktops for RDSH hosts in a VMware Horizon 7 setup, see Preparing Virtual Machines for Desktop Pools, part of the Reviewer’s Guide for View in Horizon 7 series.

Following is a list of supported operating systems, taken from Software Requirements.
1. Place the Installer in a Suitable Location

For this example, we downloaded the installer to a template VM hosted on a VMware ESXi™ server. To connect to this VM, called Win10-template_JMP, you would select the VM in the inventory list and select Launch Remote Console.

If you are performing this exercise in your own lab, you can download and extract the User Environment Manager installer file, and copy the file to the system where it will run or to a location accessible to the system.
2. Run the Installer

1. Browse to the location of the User Environment Manager installation package.
2. Double-click the installer file to start the wizard, and follow the prompts.

3. Choose the Setup Type
Select Custom to review the installation options. The VMware UEM FlexEngine agent component is selected, along with the optional components: Application Migration and Self-Support.

4. Complete the Wizard

Select Next and follow the rest of the prompts to complete the wizard.

5. Verify Installation
1. Navigate to the **Programs and Features** control panel.
2. Verify the **VMware User Environment Manager** agent was successfully installed.

The following [Install FlexEngine](#) video provides a detailed demonstration of the steps outlined in this section. If you need additional detail, you can find it here. If you already installed FlexEngine, feel free to skip the video. This video is **2 minutes**.
Install the User Environment Manager Management Console

You use this administration console to configure User Environment Manager and to manage personalization and application configuration settings for end users. You can install the User Environment Manager Management Console on any supported Windows desktop or server that you want to use for managing User Environment Manager.

To install this component, you run the same VMware User Environment Manager Setup wizard that you ran to install the User Environment Manager agent (FlexEngine).

Prerequisites for Management Console Installation

To perform this exercise, you will need the following:

- **User account** - When you log in to the OS to run the installer, the account you use must have administrative privileges.
- **Installer** - If necessary, you can download the installer from the Product Evaluation Center. The installer is an architecture-specific (x86 or x64) MSI file.
- **Windows OS** - The system must be running a supported Windows version. See Software Requirements.
- **Internet access** - The installation process includes a certificate revocation check to verify the digital signature of the MSI file. This check requires Internet access.

1. Run the Installer

1. Download and extract the User Environment Manager installer file, and copy the file to the system where it will run or to a location accessible to the system.
2. Double-click the installer file to start the wizard, and follow the prompts.
2. Choose the Setup Type

Select Custom.

3. Complete the Wizard
1. Disable the VMware UEM FlexEngine components and enable the VMware UEM Management Console component.
2. Follow the rest of the prompts to complete the wizard.

A VMware UEM Management Console shortcut appears on the Start screen.

The following Install Management Console video provides a detailed demonstration of the steps outlined in this section. If you need additional detail, you can find it here. If you already installed the User Environment Manager console, feel free to skip the video. This video is 1 minute.
Configure the User Environment Manager Management Console

The first time you start the User Environment Manager Management Console, you are prompted to supply the path to the file share you set up in Create and Configure the User Environment Manager Configuration Share. Configuring the console consists of entering this file path and either accepting the default configuration or making changes by selecting or deselecting check boxes.

1. Start User Environment Manager

From the Start screen, start the User Environment Manager Management Console.
2. Enter the UNC Path to the Configuration Share

When the console opens, in the Location text box, browse to or enter the UNC path to the configuration share; for example, \file\UEM_Config is the path if the name of the file server is file and the name of the share folder is UEM_Config.

If you have not already set up a configuration share, see Create and Configure the User Environment Manager Configuration Share.
3. Verify the Configuration File Has Been Created

Browse to the UEM_Config folder on the file share and verify that the management console configuration file has been created. The next time you open the console, this configuration file is read. You are not prompted to supply the path again.

4. Configure General Settings
Accept the default general configuration settings or use the check boxes to enable the desired features. To learn more about these features, see the VMware User Environment Manager Administration Guide. The App-V and SWV tabs contain settings for Microsoft Application Virtualization support and Symantec Workspace Virtualization support, respectively.

The following Management Console Config video provides a detailed demonstration of the steps outlined in this section. If you need additional detail, you can find it here. This video is 1 minute.
Initial Configuration Using an Active Directory Group Policy Object
How the Group Policy Object Settings Work

After installing User Environment Manager, you have a couple of options for configuration. You can use the VMware-provided administrative templates for Active Directory Group Policy Objects, or you can use the XML-based option called NoAD mode.

This section assumes you have chosen to use AD GPOs.

The FlexEngine GPO has required and optional settings, and provides administrators with the flexibility to manage multiple environments. The following Configuring the FlexEngine Group Policy Object topic provides additional detail on the configuration options for the FlexEngine Group Policy Object.

(Approximate read time: 2 minutes)
Copy the Administrative Templates to the Domain Controller

To configure settings for end users, you can use the administrative templates that are provided in the download package.

You must copy the administrative template files to the correct folder on the domain controller.

1. Copy the Administrative Templates Folder to the Domain Controller

   ![Administrative Templates Folder Image]

   The Administrative Templates (ADMX) folder is included in the same download package that contains the User Environment Manager installer. If necessary, you can download this package from the VMware Download page.

2. Copy the Administrative Template Files

   ![Administrative Template Files Image]
Select and copy all the ADMX files inside the Administrative Templates (ADMX) folder.

3. Paste the ADMX Files in the Correct Location

Paste the files in the PolicyDefinitions folder on the domain controller. The location of this folder might vary, but often the location is C:\Windows\PolicyDefinitions.

**Note:** If you use a central store for administrative templates, you should instead copy the files to the Sysvol share on the primary domain controller, in the following location:

```
\\<PDC-name>\SYSVOL\<domain-name>\Policies\PolicyDefinitions
```

In this path, <PDC-name> is the name of the primary domain controller, and <domain-name> is the fully qualified DNS name of the domain in which the domain controller is located.
4. Copy the Language Files

1. Open the en-US folder included in the Administrative Templates (ADMX) folder.
2. Select and copy all the ADML files in the en-US folder.

5. Paste the ADML Files in the Correct Location

Paste the ADML files into the en-US folder inside the PolicyDefinitions folder on the domain controller. The location of this folder might vary, but often the location is C:\Windows\PolicyDefinitions\en-US.

Note: If you use a central store for administrative templates, you should instead copy the files to the Sysvol share on the primary domain controller, in the following location:

\\<PDC-name>\SYSVOL\<domain-name>\Policies\PolicyDefinitions\en-US
The following ADMX video provides a detailed demonstration of the steps outlined in this section. If you need additional detail, you can find it here. If you already installed the ADMX and ADML files, feel free to skip the video. This video is 1 minute.
Create and Configure the FlexEngine Group Policy Object

Now that you have copied the User Environment Manager administrative templates to the correct location on the domain controller, you can create a GPO and use the templates with this GPO. In this exercise, you configure all the required policy settings to enable User Environment Manager, and you create some optional policies.

The GPO you create in this exercise applies to an organizational unit (OU) that contains instant-clone virtual desktops. You configure the following policies, some of which are user-based, and some, computer-based:

- **Enable FlexEngine to wait for the network at computer startup and logon** – (Required) This computer-based setting ensures that FlexEngine (that is, the User Environment Manager agent) Group Policy client-side extension runs every time a user logs in. If this extension does not run, User Environment Manager settings cannot be applied.
- **Enable Group Policy loopback processing mode** – This computer-based setting is necessary because the GPO is applied to an OU containing computer rather than user objects.
- **Set the path to the User Environment Manager configuration share** – (Required) This user-based setting is necessary so that the agent can read the configuration file and apply the appropriate application and environment settings for the end user.
- **Enable the FlexEngine to run as a Group Policy extension** – (Required) With this user-based setting enabled, the settings that User Environment Manager manages are applied earlier during the login phase than if FlexEngine were instead run from a login script.
- **Set the path to the Profile Archives share** – (Required) This user-based setting is necessary so that the agent can read the archive settings for a specific user to apply the correct profile. The agent also saves user settings in this folder.
- **Set the path to the Profile Archives backups** – With this user-based setting, you can specify the location and number of backups to retain.
- **Enable FlexEngine logging** – With this user-based setting, you can specify the location, logging level, and file size of the log file for the User Environment Manager agent.
- **Enable a logoff script** – (Required) With this user-based setting, you specify a command-line command so that when a user logs out, FlexEngine reads the settings configured through the User Environment Manager Group Policy Object and stores the settings.

Prerequisites for Configuring the GPO

Before you begin this exercise, verify the following:

- You have completed all the Installation exercises, and you know the paths to the User Environment Manager configuration share and the profile archives share.
- The User Environment Manager ADMX and ADML files are placed on the domain controller, as described in Copy the Administrative Templates to the Domain Controller.
- You have credentials for a computer that can access the Microsoft Group Policy Management Console (GPMC) and the domain controller.
There are a number of ways to configure and apply GPOs. This exercise provides only one example.

1. Create a GPO for an OU That Contains Virtual Desktops

1. Open Microsoft GPMC.
2. Browse to an OU containing the computer object that contains your virtual desktops.
3. Create a new GPO, and link it to this OU.
2. Enable FlexEngine to Wait for the Network

1. Edit the new GPO in the Group Policy Management Editor.
3. Edit the policy setting Always wait for the network at computer startup and logon and set it to enabled.

This setting ensures that the FlexEngine Group Policy client-side extension runs every time a user logs in. For more information, see Troubleshoot GPO Settings.
3. Enable Loopback Processing

2. Edit the policy setting Configure user Group Policy loopback processing mode and set it to enabled.

4. Locate the Flex Config Files Policy
1. Navigate to User Configuration > Administrative Templates > VMware UEM > FlexEngine.
2. Double-click the Flex config files policy setting.

**Note:** If you cannot find the VMware UEM FlexEngine policies, verify that you copied the administrative templates to the correct location, as described in Copy the Administrative Templates to the Domain Controller.

### 5. Configure the Flex Config Files Policy

1. Enable the policy. This is a mandatory setting to enable FlexEngine.
2. Provide the path to the configuration share you created as part of the exercise Create and Configure the User Environment Manager Configuration Share.

Be sure to append **General** to the end of the path because this folder is automatically created by User Environment Manager.
6. Set FlexEngine to Run as a Group Policy Extension

1. In the Group Policy Management Editor dialog box, navigate to User Configuration > Administrative Templates > VMware UEM > FlexEngine, and double-click the Run FlexEngine as Group Policy Extension policy setting.

2. Enable the policy. This is a mandatory setting to enable FlexEngine.

   It is required to either enable this policy or configure a policy to run FlexEngine as a Logon script. We recommend enabling this policy rather than running FlexEngine as a Logon script.
7. Configure the Profile Archives Policy

1. In the Group Policy Management Editor dialog box, navigate to User Configuration > Administrative Templates > VMware UEM > FlexEngine, and double-click the Profile archives policy setting.
2. Enable the policy. This is a mandatory setting to enable FlexEngine.
3. Provide the path to the profile archives share you created as part of the exercise Create and Configure the Profiles Share.

Be sure to append %username%\Archives to the end of the path so that a unique subfolder can be created for each user. The personal user settings are read from this share at login or at application start and are written back at application exit or at logout.

The policies circled in the following figure represent a minimum configuration for FlexEngine.
8. Configure the Profile Archives Backup Policy

1. In the Group Policy Management Editor dialog box, navigate to User Configuration > Administrative Templates > VMware UEM > FlexEngine, and double-click the Profile archives backups policy setting.
2. Enable the policy. This policy is recommended but not required.
3. Provide the path to the profile archives share you created as part of the exercise Create and Configure the Profiles Share.
Append `%username%\Backups` to store the profile backups in the user directory. For this example, the following path is used: `\file\UEM_Profiles\%username%\Backups`

4. Enter 5 for the number of backups.

9. Configure FlexEngine Logging

![FlexEngine logging](image)

1. In the Group Policy Management Editor dialog box, navigate to User Configuration > Administrative Templates > VMware UEM > FlexEngine, and double-click the FlexEngine logging policy setting.
2. Enable the policy. This policy is recommended but not required.
3. Provide the path to the profile archives share you created as part of the exercise Create and Configure the Profiles Share.
   Append `%username%\Logs\FlexEngine.log` to store the log files in the user directory. For this example, the following path is used: `\file\UEM_Profiles\%username%\Logs\FlexEngine.log`
4. Set the log level to Debug.

**Important:** Setting the log level to Debug should only be used for evaluation or troubleshooting purposes. For production implementations of User Environment Manager, consider enabling debug logging for individual users as described in the VMware KB article [Enabling debug logging for a single user in VMware User Environment Manager (2113514)](https://kb.vmware.com/s/article/2113514).

The following figure shows the recommended FlexEngine policies to enable and configure for User Environment Manager.
10. Add a Windows Logoff Policy

1. Navigate to User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff).
2. In the right pane, double-click Logoff to open the Logoff Properties window.
3. Select Add.
11. Configure the Logoff Script

1. Enter the path to the location where **FlexEngine.exe** is installed on the Windows virtual desktops.
   The default path is `C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe`.
2. Enter `-s` in the **Script Parameters** field.

   The `-s` flag tells FlexEngine to store the settings configured through the User Environment Manager Group Policy Object. The settings are stored in the **Archives** folder for the user on the profile archives share.

The following [ADMX](#) video provides a detailed demonstration of the steps outlined in this section. If you need additional detail, you can find it here. This video is 1 minute.
Initial Configuration Using NoAD Mode
Introduction and Prerequisites for Using NoAD Mode

NoAD mode is a way to configure User Environment Manager without requiring Active Directory. For example, you can use NoAD mode if your environment has limited Active Directory access, and administrators are not permitted to set GPOs.

NoAD mode is always recommended for cloud-based implementations. For more information, see Benefits of VMware Horizon Cloud on Microsoft Azure & VMware User Environment Manager.

Another use case is when you are working with a proof-of-concept environment. You can implement User Environment Manager in NoAD mode quickly because there is no need to change a GPO, configure logon and logoff scripts, or wait for Active Directory replication.

Using NoAD mode is a two-part process:

1. You configure User Environment Manager by creating an XML-based configuration file. This file contains all the same settings that you would otherwise configure using GPO settings. VMware provides an example file for this purpose. You can copy the file to the correct location on the configuration share and edit the file with a text editor to specify the settings you want to use.

2. You install the User Environment Manager agent in NoAD mode on the virtual desktops or RDSH servers to be managed. This process involves using a command-line command that tells the agent the path to the XML-based NoAD configuration file. The agent can then read this configuration file to determine which User Environment Manager settings to apply.

Prerequisites

In the examples for the following exercises, we use a virtual desktop VM that is part of a VMware Horizon 7 setup, though this is not required. If you are using a Horizon 7 environment, you will need to have access to a desktop or RDSH server VM, and you will need VMware Horizon® Client™ for logging in to the VM after you install the User Environment Manager agent.

Before you begin the exercises in this chapter, you must complete the Installation exercises.
Create the User Environment Manager NoAD Configuration File

VMware provides a sample XML configuration file to simplify using NoAD mode. You can either copy this file from the User Environment Manager installation package you downloaded, or copy contents of the file from a topic in the product documentation. At a minimum, you must edit only a few required settings in the sample file.

With the NoAD mode configuration file in the correct location on the configuration share, you can install the User Environment Manager agent on managed endpoints. As part of this agent installation, you specify the path to the NoAD configuration file you create in this exercise.

Prerequisites for Creating the NoAD Configuration File

Before you begin this exercise, you must have completed all the Installation exercises, and you must know the paths to the User Environment Manager configuration share and the profile archives share.

1. Create a NoAD Folder on the Configuration Share

1. Navigate to the `<configuration-share>`\`general\FlexRepository`\`general\FlexRepository\NoAD` folder on the configuration share.
2. Create a new folder called NoAD.

The path to the folder must be `<configuration-share>`\`general\FlexRepository\NoAD`. For the example used in this exercise, the path is `\file\UEM_Config\general\FlexRepository\NoAD`
2. Create a NoAD.xml File in the NoAD Folder on the Configuration Share

You have two options for creating the NoAD.xml file:

- You can copy and rename the NoAD Sample.xml file, located inside the NoAD Mode folder, from the installation package. If necessary, you can download this package from the VMware Download page.
- You can manually create an empty text file inside the NoAD folder on the configuration share, rename the file NoAD.xml, and copy and paste the contents from the Sample NoAD.xml topic.

3. Edit the NoAD.xml File to Specify Configuration Settings

The only required settings you must edit are:
• Path to the profile archives share (ProfileArchivePath) – Replace the text `filesrv\UemUsers$` with the name of the file server and share folder you created as part of the exercise Create and Configure the Profiles Share.

The `%username%\Archives` portion of the path allows a unique subfolder to be created for each user. The personal user settings are read from this share at login or at application start and are written back at application exit or at logout.

• Path to the log file (LogFileName) – Replace the text `filesrv\UemUsers$` with the name of the file server and share folder you created as part of the exercise Create and Configure the Profiles Share.

For the example in this exercise, the settings are:

```plaintext
ProfileArchivePath="\File\UEM_Profiles\%username%\Archives"
LogFileName="\File\UEM_Profiles\%username%\Logs\FlexEngine.log"
```

4. Set the Logging Level to Debug

1. In the line `LogLevel="1"` change the 1 to 0, which changes the level of logging from Info to Debug.

   For a complete list of the various logging levels and their corresponding settings, see Configuring FlexEngine Logging Settings.

2. Save and close the NoAD.xml file.

**Important:** Setting the log level to Debug should only be used for evaluation or troubleshooting purposes. For production implementations of User Environment Manager, consider enabling debug logging for individual users as described in the VMware KB article Enabling debug logging for a single user in VMware User Environment Manager (2113514).

**Note:** This exercise demonstrates using only a few of the many possible configuration settings. For information about all of the other settings, see Configuring User Environment Manager with NoAD Mode, and see the VMware KB article Configuring advanced UEM settings in NoAD mode (2148324).
Install the User Environment Manager Agent in NoAD Mode

Rather than running the interactive VMware User Environment Manager Setup wizard, as you did in Install the User Environment Manager Agent (FlexEngine) on the Desktop or RDSH Server, for NoAD mode, you run the installer using a command-line command. You also specify command-line options that provide the path to the XML-based NoAD configuration file you created in Create the User Environment Manager NoAD Configuration File.

Prerequisites for Installing the Agent in NoAD Mode

The prerequisites for installing FlexEngine in NoAD mode are the same as for installing the agent without using NoAD mode.

To perform this exercise, you need the following:

- **User account** – When you log in to the OS to run the installer, the account you use must have administrative privileges.
- **Installer** – If necessary, you can download the installer from the Product Evaluation Center or the VMware Downloads page. The installer is an architecture-specific (x86 or x64) MSI file.
- **Windows OS** – The machine must be running a supported Windows version. See Software Requirements.

**Note:** For the purposes of this exercise, you can install the agent on a physical or a virtual machine that you want to manage. For details about how to create a VM used for virtual desktops for RDSH hosts in a VMware Horizon 7 setup, see Preparing Virtual Machines for Desktop Pools, part of the Reviewer’s Guide for View in Horizon 7 series.

- **License** – The installation wizard prompts for the path to a valid license file unless VMware Horizon Agent is already installed in the VM. (User Environment Manager is included with Horizon 7 Enterprise Edition.) See Licensing Requirements.
- **Windows Registry** – The Windows Registry on the VM must be accessible to User Environment Manager so that new entries can be written. See Registry Access Requirements.
- **Internet access** – The installation process includes a certificate revocation check to verify the digital signature of the MSI file. This check requires Internet access.

In addition, you must know the path to the **NoAD.xml** configuration file you created in the exercise Create the User Environment Manager NoAD Configuration File.

**Important:** The VM you use for this exercise must not already have FlexEngine installed. If you plan to use the same VM that you used in the earlier exercise Install the User Environment Manager Agent (FlexEngine) on the Desktop or RDSH Server, you first must uninstall the agent before you re-install the agent in NoAD mode.
1. Place the Installer in a Suitable Location

For this example, we downloaded the installer to a template VM hosted on an ESXi server. To connect to this VM, called Win10-template_JMP, you would select the VM in the inventory list and select Launch Remote Console.

If you are performing this exercise in your own lab, you can download and extract the User Environment Manager installer file, and copy the file to the system where it will run or to a location accessible to the system.
2. Open a Command Prompt in Administrative Mode

Log in to the virtual desktop or RDSH server VM, right-click the cmd application and select Run as administrator.

3. Enter the Command to Install the Agent

1. Change directories to the directory where the msiexec.exe file is located.
2. Enter the command to run the file. The syntax of the command is:

```command
msiexec.exe /i "<installer-file>" /qn /l* InstallUEM.log NOADCONFIGFILEPATH=\<config-share>\General
```

In this example,
• `<installer-file>` is the path to the agent installer located on a file share, and because there are spaces in the installer file name, the path is enclosed in quotation marks:

"\file\software\infra\UEM\VMware User Environment Manager 9.3 x64.msi"

• `<config-share>\General` is the path to the configuration share:

\file\UEM_Config\General

The NoAD.xml file you created in Create the User Environment Manager NoAD Configuration File resides in the subfolder `FlexRepository\NoAD\` inside the General folder.

Important: In this example, the LICENSEFILE command-line option is not included because the VMware Horizon Agent is already installed in the VM. (User Environment Manager is included with Horizon 7 Enterprise Edition.) If the Horizon Agent is not already installed in your VM, be sure to add the LICENSEFILE command-line option to specify the path to your license file. The syntax is:

LICENSFILE="\<file-server>\<share>\VMware UEM.lic"

In this example, `<\file-server>` `<\share>` is the file share where the license file is located. You can place this command-line option after the `/qn` option. You can copy the complete syntax of the command from Install User Environment Manager in NoAD Mode.

4. Verify Installation

1. Navigate to the Programs and Features control panel.
2. Verify the VMware User Environment Manager agent was successfully installed.
If you plan to use this VM as a master, or template, VM for creating a desktop pool or RDSH server farm, you can shut the VM down and take a VM snapshot.

5. Log in to the VM Where the Agent Is Installed

To verify that User Environment Manager is working correctly in NoAD mode, you must log in to the machine so that profile-specific files can be created on the file share.

If you are using a Horizon 7 virtual desktop, use Horizon Client to log in to the desktop pool that contains the VM with NoAD enabled.

If you are using an RDSH server, you must create an application or desktop pool and use Horizon Client to launch an application or session-based desktop.

6. Verify That User-Specific Profile Archives Are Created

1. Navigate to the profile archives share and verify that a user-specific folder has been created.
2. Verify that inside this folder, the Archives and Logs folders have been created.
7. Examine the Logs

1. After login is complete, open the `FlexEngine.log` file in the `Logs` folder, and verify that you see the line **Running from service (NoAD)**.

   For the example in this exercise, the path to this folder is `\file-share\UEM_Profiles\<username>\Archives\Logs`.

2. Also look for DEBUG lines, which verify that the agent is running using the Debug level of logging, which you set when running the installer.

The following **NoAD** video provides a detailed demonstration of the steps outlined in this exercise. If you need additional detail, you can find it here. If you already completed the NoAD Mode configuration, feel free to skip the video. This video is **4 minutes**.
Basic Features
Enable the Easy Start Feature

By default, User Environment Manager does not manage any applications or environment settings after you install it. You must specify which applications and settings to manage. Although this approach takes a little more work up front, this solution prevents excessive profile growth and profile corruption, enables user settings to roam across Windows versions, and gives you granular control to manage as much or as little of the user experience as needed.

To help with getting started, the Easy Start button instantly adds many common Windows applications, including several versions of Microsoft Office, to the whitelist of applications managed by User Environment Manager. Many Windows environment settings are also added by Easy Start. You can then easily select an application or Windows setting to review and change the default settings.

Prerequisites for Using Easy Start

To perform this exercise, you need the following:

- Credentials for the virtual or physical machine where you installed and performed the initial configuration of the User Environment Manager Management Console, as described in Configure the User Environment Manager Management Console.
- (Recommended but not required) Microsoft Office installed on the virtual desktop or RDSH server that you want to manage. You will be prompted to select the version of Microsoft Office that is installed.

1. Open the User Environment Manager Configuration File

The path to the file is `\<file-share-server>\UEM_Config\Immidio Flex Profiles Configuration.xml`. For the example in this exercise, the path is `\file\UEM_Config\Immidio Flex Profiles Configuration.xml`. Note that the file contains no application-specific settings yet.
2. Navigate to the General Folder

For the example in this exercise, the path is `\file\UEM_Config\General`. Note that the folder is empty. Application-specific files are created in this folder when you configure User Environment Manager to manage an application.

3. Start the User Environment Manager Management Console

1. On the physical or virtual machine where the Management Console is installed, from the Start screen, select the Management Console shortcut in the VMware UEM folder.
2. On the Personalization tab, note that in the left pane, no applications are listed under General. At this point, User Environment Manager is not managing any applications or Windows settings.
4. Click the Easy Start Toolbar Button

Clicking this button allows User Environment Manager to manage many common Windows applications.

5. Select the Versions of Microsoft Office

1. Select the version or versions that are installed on the virtual desktop or RDSH server that you want to manage.
2. Select OK in the confirmation dialog box that appears.
6. Examine the List of Common Applications Installed with Easy Start

In the left pane, under **General**, you see a list of commonly installed Windows applications. These applications will now be managed with User Environment Manager.

By default, when users log in and change application settings for these applications, their personalizations will be saved when they close the application. For example, if the user logs in to an instant-clone desktop and changes application settings, when the user logs out of the instant-clone desktop, the VM is destroyed. When the user logs in to a new instant-clone desktop and starts the application, the user will see that the settings were saved. The user has the experience of persistence even though the user logs in to a different instant-clone VM.
7. Examine the List of Office Applications and Windows Settings

These applications and Windows settings are now managed by User Environment Manager. You can examine the default settings and make any desired changes.

8. Open the Applications Folder in the General Folder

Navigate to the Applications folder on the configuration share. For this exercise, the path is `\file\UEM_Config\General\Applications`. Note that this folder did not exist before you clicked the Easy Start toolbar button. Scroll through the list of application files in this folder. Common types of files include:

- Application icon files – Files with the .ico extension.
• Application configuration files – Files with the .ini extension.
• Flag files – Files with the .INI.flag extension, which are for configuring the application to use the DirectFlex feature. With DirectFlex enabled, the User Environment Manager profile archives settings are imported and read when the user starts the application, rather than when the user logs in to the machine. Application settings are saved (exported) when the user quits the application, rather than when the user logs out of the machine.

The **Applications** folder contains settings for the common applications included with Easy Start. If you also selected to enable personalization for a Microsoft Office version, a folder for that version of Office also appears in the **General** folder.

A **Windows Settings** folder is also created in the **General** folder. Flag files are almost never used for these settings because the DirectFlex feature applies only to application settings. Except for things like integrated IE or Edge browser cache settings, Windows settings are usually imported and exported at OS login and OS logout, respectively.

![Windows Settings Folder](image)

The following **Easy Start** video provides a detailed demonstration of the steps outlined in this exercise. If you need additional detail, you can find it here. If you already completed the Easy Start configuration, feel free to skip the video. This video is 2 minutes.
**Test Application Personalization**

With the application personalization feature, end users can roam between disparate devices while preserving custom application settings and Windows personalization settings. When a user logs in to a virtual desktop or application, User Environment Manager reads the profile archive file for that user's profile and can, for example, display the desktop background or application settings that the user saved during the last session.

In this exercise, you will log in to a physical or virtual machine as an end user, open an application, change some application settings, log out, and then log in again and verify that the settings have been persisted across sessions. You can even log in from different devices if you like.

The following section, **Personalization of Application and Windows Settings**, provides more background information on the settings. (Approximate read time: 1 minute)

**Prerequisites**

In the example for this exercise, we use a virtual desktop VM that is part of a Horizon 7 setup, though this is not required. You can use whatever physical or virtual machine you used to install the agent, as described in Install the User Environment Manager Agent (FlexEngine) on the Desktop or RDSH Server or Install the User Environment Manager Agent in NoAD Mode.

If you are using a Horizon 7 environment, you will need to have access to the virtual desktop pool that has the User Environment Manager agent installed, and you will need Horizon Client or the web-based HTML Access client for logging in to the VM.

Before you begin this exercise, you also must complete the Enable the Easy Start Feature exercise, which includes enabling one or more of the Microsoft Office application templates.
1. Navigate to the Profile Archives Share

For the example in this exercise, the path is \\file\UEM_Profiles. Note that the folder is empty. User-specific folders are created in this folder after the end user logs in to the machine for the first time.

**Important:** Keep this window open, and size the window so that you can see it alongside the window you will use in the next step to open the virtual desktop.
2. Log In to a Virtual Desktop as an End User

For the example in this exercise, we are using a Horizon 7 instant-clone desktop, and we access it through the VMware Workspace™ ONE™ catalog.

3. Watch the Profile Archive Folder Get Created
As soon as the login process begins, a new folder is created on the profile archive share. The folder is named according to the user name of the user logging in.

At this point, the agent on the virtual desktop is importing the User Environment Manager settings from the configuration files in the General folder on the configuration share.

4. Verify Settings Have Been Imported

After login is complete and the desktop appears, note that several desktop shortcuts have been created by the Easy Start feature, including Calculator (Created by VMware UEM). Other examples include MS Paint, Notepad, and Wordpad.

For a list of application shortcuts created by the Easy Start feature, you can go to the User Environment tab in the Management Console and select Shortcuts in the left pane, as shown in the following figure.
5. Open PowerPoint

1. From the Start screen of the virtual desktop, click the Start button, select All Apps, and click to expand Microsoft Office 2016 (created by VMware UEM).

Note: If, when completing the Easy Start exercise, you selected a different Microsoft Office version, navigate to that version.
6. Open a Blank PowerPoint Presentation

1. If PowerPoint prompts you to accept the license agreement, for the update option, select **Ask me later**, and click **Accept** for the license agreement.
2. In the list of templates, select **Blank Presentation**.

**Note:** At this point, if you look in the profile archive **Archives** folder for the user, you see only an **Applications** folder and a **Logs** folder. No folders for Microsoft Office applications appear yet because this is the first time the user has started an Office application.

For the example in this exercise, the path to this folder is `\<file-share>\UEM_Profiles\<username>\Archives\`
In the Applications folder, the only application file you can see is for Notepad because Notepad is used to import settings.
7. Change Some Default View Settings

1. Select the **View** tab.
2. Select the **Ruler**, **Guidelines**, and **Guides** check boxes.
3. Close PowerPoint.
4. Log out of the virtual desktop OS.

After you log out of the VM, all the default settings for Microsoft Office applications, and the settings you changed for PowerPoint, are saved to the profile archives share.
8. Verify That Application Settings Are Saved to the Profile Archives

Navigate to the Archives folder for the user and verify that a folder for Microsoft Office has been created. For the example in this exercise, the path to the Archives folder is `\<file-share>\UEM_Profiles\<username>\Archives\`, and a Microsoft Office 2016 folder is created.

9. Examine the Archives for Microsoft Office

Open the Microsoft Office 2016 folder, and scroll through the list of files.

The PowerPoint.zip file contains settings used when you closed the application, including the settings you changed on the View tab. The other ZIP files in this folder contain default settings for the other Microsoft Office applications.
10. Log In Again to See Persistent Settings

1. Log in to the virtual desktop as the same end user.
2. Start PowerPoint, and select Blank Presentation again.
3. Note that the ruler, gridlines, and guides are shown rather than hidden.

If you are using a Horizon 7 instant-clone desktop, the VM that you first logged in to was destroyed, and this new desktop still displays the PowerPoint settings you chose using the previous VM.

If you are using a full-clone desktop, you might be able to replicate this experience by reverting the VM back to a snapshot taken before you ever logged in for the first time. When you log in after reverting, you will still see the personalized PowerPoint settings.

If you are using a physical PC, which would ordinarily persist the settings whether or not you are using User Environment Manager, you can test this feature by removing the user profile before you log in again. Alternatively, you can log in to a different physical PC.

This exercise demonstrates how User Environment Manager, when used in conjunction with stateless virtual desktops, can give the experience of persistent, stateful desktops.

The following App Personalization video provides a detailed demonstration of the steps outlined in this exercise. If you need additional detail, you can find it here. If you already completed the Application Personalization exercise, feel free to skip the video. This video is 2 minutes.
Create an Application Template with Application Profiler

For applications that do not have a corresponding application management template, you can use the Application Profiler, a standalone application that analyzes where an application stores its file and registry configuration. The analysis results in an optimized User Environment Manager Flex configuration file, which you can edit in the Application Profiler or use directly. You can also use Application Profiler to set the initial configuration state of applications.

In this exercise, you will install the Application Profiler tool, which is included in the User Environment Manager installation package. After Application Profiler is installed in a provisioning VM, you can run the tool to open the application you want to profile, change some settings, and then create a template you can use to manage the application for your end users.

The following section, Introduction to User Environment Manager Application Profiler, provides additional background. (Approximate read time: 1 minute)

Prerequisites for Using Application Profiler

To perform this exercise, you need the following:

- **Provisioning machine** – The machine that you use to profile the application must use the same Windows OS version and similar patch version as the machine that your end users will use. For supported Windows versions, see Application Profiler System Requirements. **Note:** The provisioning machine must not have the User Environment Manager agent installed on it. VMware recommends that the provisioning machine not have any additional applications installed aside from those included with the OS and VMware Tools, if you are using a VM.
- **User account** – When you log in to the provisioning machine to run the Application Profiler installer, the account you use must have administrative privileges.
- **Installer** – The Application Profiler installer is included in the User Environment Manager installation package, in the Optional Components folder. If necessary, you can download the package from the Product Evaluation Center or the VMware Downloads page. The installer is an architecture-specific (x86 or x64) MSI file.
- **Internet access** – The installation process includes a certificate revocation check to verify the digital signature of the MSI file. This check requires Internet access.
- **Application to profile** – For the example used in this exercise, you can download the Notepad++ application. The application that you profile must be the same version that is installed in the machine that your end users will use.

**Note:** Application Profiler can profile applications that are installed natively in virtual desktops or RDSH servers, as well as applications that are delivered by VMware App Volumes AppStacks.
1. Place the Installer in a Suitable Location

For this example, we downloaded the installer to a provisioning VM hosted on an ESXi server. To connect to this VM, called Provision, you would select the VM in the inventory list and select Launch Remote Console.

If you are performing this exercise in your own lab, you can download and extract the Application Profiler installer file, which is located in the Optional Components folder of the installation package, and copy the file to the system where it will run or to a location accessible to the system.

2. Run the Installer
1. Log in to the provisioning machine, and browse to the location of the Application Profiler installer.
2. Double-click the installer file to start the wizard, and follow the prompts. You can accept all the defaults.

**Tip:** (Optional) After installation is complete, shut down the machine and take a VM snapshot. With a VM snapshot of the machine, you can easily revert the machine to its pristine condition after you finish profiling an application. You can then use the machine to profile a different application, and so on.

### 3. Install the Application to Be Profiled

1. On the provisioning machine, browse to the location of the installer for the application you want to profile.
   - For the example in this exercise, we used the [Notepad++](https://notepad-plus-plus.org/) application, but you can use any application that your end users will use. Be sure to use the same version that your end users have.
2. Double-click the installer file to start the wizard, and follow the prompts. If you are installing Notepad++, configure the following options in the installation wizard:
   - De-select the **Auto-Updater** check box.
   - Select the **Localization** check box.
   - Select the **Create Shortcut on Desktop** check box.

**Important:** VMware recommends that, if possible, you install the application so that automatic updating is disabled, especially if you use instant clones. For the purposes of this exercise, enable localization packs, as shown in the following figure. In this exercise, we will test profile settings by changing the language used in the UI.
4. Start Application Profiler

From the All Programs list on the provisioning machine, **Application Profiler** is located in the **VMware UEM** folder.
5. Start the Profiling Session

1. Click **Start Session**.
2. Browse to and select the application.

After you click OK, Application Profiler opens the application to be profiled and begins monitoring the changes you make and where those changes are saved in the Windows registry and file system.

For example, the VLC Player application saves some changes to .ini files and some to the Windows registry. For more information, see [Profiling Applications with VMware User Environment Manager, Part 2: Applying and Troubleshooting Predefined Settings](#).
6. Make Some Changes to the Application

1. From the menu bar, select **Settings > Preferences**.
2. From the Toolbar list, select **Big icons**.
3. De-select the **Show status bar** check box.
4. Close the application.

Application Profiler saves the changes you made, and prompts you to confirm that profiling is finished, as shown in the following figure.
Application Profiler also displays the location in the file system where the Notepad++ configuration changes were made. In this case, settings were written to a Notepad++ subfolder of the AppData folder.

7. Verify the Location of Application Configuration Changes

![Image of Windows Explorer path to Notepad++ configuration folder]

Open Windows Explorer and type %AppData%\Notepad++ into the text box for navigating the path. The %AppData% variable resolves to the correct location on the machine, and the contents of the Notepad++ folder are displayed, which include a configuration file.

8. Save the Config File

1. Click the Save button, and select Save Config File.
2. When prompted, provide a file name, such as NPP, and save the Application Profiler configuration files to the desktop.

In this exercise, you are creating a configuration file to enable application personalization by the end user, so that when an end user changes a Notepad++ preference, the user’s preference will be saved across sessions and VMs.
Because you select *Save Config File*, rather than *Save Config File with Predefined Settings*, the preference settings you changed in this exercise will not be presented to end users. For more information, see [Saving a Flex Configuration File With Predefined Settings](#). You changed preference settings in Notepad++ only so that Application Profiler could monitor and determine the path to the application configuration file.

9. Copy the Notepad++ Configuration Files

For the example in this exercise, the files you copy from the desktop of the provisioning machine are:

- **NPP.ico** – The icon file.
- **NPP.ini** – The application configuration file.
- **NPP.ini.flag** – The flag file, which tells User Environment Manager to import settings when the application starts and export the user settings when the application closes.
10. Paste the Files in the Applications Folder on the Configuration Share

For the example in this exercise, the folder is located in `\<file-server>\UEM_Config\General\Applications`.

**Note:** After you paste the files in this location, if you close the User Environment Manager Management Console and start it again, you see Notepad++ added to the list of applications being managed, as shown in the following figure. Also note that the `NPP.ini.flag` file enables DirectFlex for this application, and the path to the executable is recorded.
11. Log In to a Virtual Desktop as an End User

For the example in this exercise, we are using a Horizon 7 instant-clone desktop, and we access it through the VMware Workspace ONE catalog.
12. Start Notepad++ and Change Some Settings

1. After login is complete, start the application, and select Settings > Preferences, and select Big icons.
2. From the Localization list, select Deutsch and save the settings.

In Notepad++ the toolbar icons are now large and the menu names are displayed in German, as shown in the following figure.
13. Verify That Application Settings Are Saved to the Profile Archives

Navigate to the profile archive Applications folder for the user, and note that a new NPP.zip file has been created.

The NPP.zip file was created as soon as you started the application. For the example in this exercise, the path to this folder on the profile archives share is \<file-share>\UEM_Profiles\<username>\Archives\.

14. Log Out and Log In Again to See Persistent Settings

After you log out of the virtual desktop and log in again as the same user, when you start Notepad++, you see that your settings have been preserved.

If you are using a Horizon 7 instant-clone desktop, the VM that you first logged in to was destroyed, and this new desktop still displays the Notepad++ settings you chose using the previous VM.

If you are using a full-clone desktop, you might be able to replicate this experience by reverting the VM back to a snapshot taken before you ever logged in for the first time. When you log in after reverting, you will still see the personalized Notepad++ settings.

This exercise demonstrated profiling a simple application. For the applications that you need to profile for your company, if an application profile is not already included with the Easy Start feature, use the following resources to create an application profile template:

• Go to the VMware User Environment Manager Community Forum, which contains many more templates created with Application Profiler.
• See the VMware User Environment Manager Application Profiler Administration Guide and the blog series that begins with Profiling Applications with VMware User Environment Manager, Part 1: Introduction to Application Profiler.

The following App Profiler video provides a detailed demonstration of the steps outlined in this exercise. If you need additional detail, you can find it here. If you already completed the Application Profiler exercise, feel free to skip the video. This video is 6 minutes.
Configure User Environment Settings

User environment settings include many different kinds of settings, some of which can be application-specific, and some can pertain to the user's whole virtual desktop environment. These are imported when the user logs in to the OS. For example, you can map a drive to a virtual desktop either when a user logs in to the OS or when a user starts a specific application. Besides configuring environment settings, you can specify the conditions under which the settings are applied, and you can specify which tasks might trigger a setting to be used.

To configure environment settings for a user's whole virtual desktop environment, you can click the User Environment tab at the top of the Management Console, as shown in the following figure.

As you can see, user environment settings include the following, among others:

- **Application Blocking** – An advanced feature that is discussed in the later exercise Configure Application Blocking.
- **Drive Mappings** – A feature that is explored in this exercise, but is applied to a specific application.
- **File Type Associations** – A feature that is explored in this exercise, wherein you configure which application is used to open files with a specific file extension.
- **Horizon Smart Policies** – A feature that integrates with Horizon 7, in which a number of key Horizon 7 features can be dynamically enabled or disabled based not only on who the user is, but on the many different variables available through Horizon 7: client device, IP address, pool name, and so on. For more information, see the chapter Horizon Smart Policies.
- **Privilege Elevation** – An advanced feature that is discussed in the later exercise Configure Privilege Elevation for Installing an Application.
- **Shortcuts** – A feature that lets you configure whether to use a desktop shortcut or a Program folders shortcut (or both), the shortcut name, the shortcut icon, and more. An introduction to this feature is provided in [Test Application Personalization](#).

Providing exercises for all the different types of user environment settings is beyond the scope of this quick-start tutorial, but you can easily get an introduction by selecting items in the list and reviewing the user friendly control labels for each one in the Management Console. Also see [Configuring User Environment Settings](#). For information about App Volumes settings, see [VMware User Environment Manager with VMware App Volumes](#).

In addition to configuring settings for the whole desktop environment, you can configure settings based on which applications a user launches. To configure environment settings for a specific application, you can select the application in the list, and click the corresponding User Environment tab, as shown in the following figure.

You will use both types of User Environment tabs in this exercise.

**Prerequisites**

To perform this exercise, you need the following:

- Notepad application listed as a managed application in the Management Console. This application is listed after you complete the exercise [Enable the Easy Start Feature](#).
- An Active Directory group containing an end-user account that you can use to log in to a virtual desktop. As part of this exercise, you will remove this user account from the AD group to test a conditional setting.
- End-user credentials for that end-user account.
- Credentials for the virtual or physical machine where you installed and performed the initial configuration of the User Environment Manager Management Console, as described in [Configure the User Environment Manager Management Console](#).
- One or more folders on a file-share server, to allow you to test drive mapping. For the example in this exercise, we created a Marketing file share, with the following path:

  `\<file-server>\Marketing\`
Inside the Marketing folder are the subfolders Docs, PPT Templates, and Reports.

**Note:** Throughout this exercise you will frequently change between your Windows end-point device where the User Environment Manager Agent is installed, and the physical or virtual machine where the Management Console is installed. It is recommended that you simply minimize the unused screen to streamline the testing process.

1. **Create an Environment Setting for the Notepad Application**

   1. In the User Environment Manager Management Console, select Notepad in the left pane.
   2. Select the DirectFlex tab, and select the Enable DirectFlex for this config file check box. Enabling DirectFlex is required for configuring application-specific user environment settings.
   3. Select the User Environment tab.

1.1. **Add a Drive-Mapping User Environment Setting**

   1. In the User Environment Manager Management Console, select Notepad in the left pane.
   2. Select the DirectFlex tab, and select the Enable DirectFlex for this config file check box. Enabling DirectFlex is required for configuring application-specific user environment settings.
   3. Select the User Environment tab.
1. Select the Add button.
2. Select Drive Mapping from the list.

1.2. Configure Drive Mapping for the Notepad Application

1. In the Name text box, enter Map Drive with Notepad. This is the name of the setting as it appears in the User Environment Manager Management Console.
2. For Drive letter, select a letter that is not already in use. For the example in this exercise, M is used.
3. For Remote path, enter the path to the share that you want to map to a drive letter. For the example in this exercise, \\file-server\Marketing is used.
4. For Friendly name, enter the name that you want end users to see in Windows Explorer next to the drive letter.
5. Select the Undo at application exit check box. This setting unmaps the drive when the user closes the application.

The Run asynchronously check box is selected by default. This setting helps the drive-mapping process to complete quickly.

After you save the settings in the Drive Mapping dialog box, the new configuration is listed on the User Environment tab for Notepad, using the name you specified in the Name text box.
1.3. Save the Configuration to the Configuration File

Select **Save Configuration** in the main toolbar.

2. Log In to a Virtual Desktop and Test the Feature

Log in to the virtual desktop as an end user. For the example in this exercise, we are using a Horizon 7 instant-clone desktop, and we access it through the VMware Workspace ONE catalog.
2.1. Verify That the Drive Has Not Yet Been Mapped

Open Windows Explorer to view the drives mapped to the virtual desktop. Note that the drive you configured is not mapped yet because, at this point, you have logged in but not started the Notepad application.
2.2. Start Notepad and Verify That the Drive Is Mapped

1. Start Notepad.
2. Open Windows Explorer to view the drives mapped to the virtual desktop. Note that the drive you configured is now mapped.
   
   **Note:** If you do not see the mapped drive immediately, wait a few seconds and refresh the window.
3. Close the Notepad application.
4. Open Windows Explorer again and note that the drive has been unmapped.
5. Log out of the virtual desktop.
2.3. Examine the Logs on the Profile Archives Share

Open the **FlexEngine.log** file in the Logs folder of the profile archives folder for the user, and verify that you see the line `Successfully unmapped drive 'M:' ('Notepad.INI.Map Drive with Notepad')`.

For the example in this exercise, the path to this folder is `\<file-share>\UEM_Profiles\<username>\Archives\Logs`. You can also search the file for all instances of the word "map" to find other entries for mapping events.

3. Create Conditions for the Drive-Mapping Setting
On the **Personalization** tab of the Management Console, select the **Map Drive with Notepad** setting, and select **Edit**.

### 3.1. Add a Condition for AD Group Membership

On the **Conditions** tab, select the **Add** button, and select **Group Membership**.
3.2. Select the AD Group

In the Group Membership dialog box, click **Browse** to search for and select the group.

This is the AD group mentioned in [Prerequisites](#) that contains an end-user account that you can use to log in to a virtual desktop. In this exercise, you will remove this user account from the AD group to test the conditional setting.
3.3. Add Another Condition for Windows Version

1. On the **Conditions** tab, select the **Add** button, and select **Windows Version**.
2. Select **Windows 10**, or whatever version of Windows is installed in the virtual desktop.

After you click **Save**, the condition is added to the **Conditions** tab, and is combined with the first condition, as shown in the following figure.
At this point in the exercise, the conditions for mapping a drive when the user starts the Notepad application are as follows: The user must be a member of a particular AD group (the Marketing group) and that the user must be logged in to a Windows 10 desktop.

**Note:** By default the AND operator is used when you add a condition, but you can select the condition and select **Edit** to change the default operator, as shown in the following figure. For this exercise, we use **AND**.
3.4. Save the Configuration to the Configuration File

Select *Save Configuration* in the main toolbar.

4. Test the Condition

In Active Directory Users and Groups, remove the end user from the AD group that you set up as part of the *Prerequisites*. For the example in this exercise, the group had only one member, which we removed.
4.1. Log In to the Virtual Desktop and Start Notepad

1. Log in to the virtual desktop using the end-user account that you just deleted from the AD group.
2. Start the Notepad application.
3. Open Windows Explorer and note that the drive is not mapped to the virtual desktop. The drive is not mapped because the user does not meet the condition of belonging to the AD group.
4.2. Examine the Logs on the Profile Archives Share

Open the **FlexEngine.log** file in the Logs folder of the profile archives folder for the user, and verify that you see the line `Conditions: Check for user membership of group '<group-name>' = false.`

**Note:** You must have the log level set to DEBUG to see this entry. The entry that follows, however, is visible at the INFO level: `Skipping drive mapping due to conditions.`

For the example in this exercise, the path to this folder is `\<file-share>\UEM_Profiles\<username>\Archives\Logs`.

At this point, you could add the user back to the AD group and then log in to the desktop again to verify that the drive will now be mapped when you start Notepad.
5. Test File Type Associations

1. In the Management Console, select the User Environment tab.
2. In the list, select File Type Associations.
3. In the right pane, double-click abc.
4. Review the Settings tab. With this setting, all files in the virtual desktop file system that use the file extension .abc are opened with the Notepad application.
5. Select Cancel. You do not need to save the settings because these are the default settings included with Easy Start.
6. Create and Open a File with the ABC Extension

1. Log in to the virtual desktop as an end user, and on the desktop, create a new text file with the .abc file extension.
2. Double-click the file, and note that the default application used to open the file is Notepad.

Refreshing Settings Without Logging Out of the Desktop

For the steps in this exercise, after you created a new setting or changed a setting, you had to log in to the virtual desktop again to verify that the new setting was properly applied. However, you can use FlexEngine command-line commands on the virtual desktop to refresh environment settings so that you do not need to log out and log back in.

For example, when you are logged in to a virtual desktop as an end user, you can try changing the file type association for files with the .abc extension so that Microsoft Word opens them rather than Notepad. Or you could change which application shortcuts are created for one of the default applications, such as Notepad or Calculator.

After you make the change in the Management Console and save the configuration, on the virtual desktop, you can run the command to refresh the shortcuts and file type associations. For the example in this exercise, use the following command.

```
"c:\Program Files\Immidio\Flex Profiles\flexengine.exe" -UemRefresh
```
Different command-line options are provided for refreshing different types of settings. For more information, see FlexEngine Command-Line Arguments and Additional FlexEngine Operations. Besides running these commands on the virtual desktop, you can use these commands in scripts and logon tasks.

The following User Environment Settings video provides a detailed demonstration of the steps outlined in this exercise. If you need additional detail, you can find it here. If you already completed the User Environment Settings exercise, feel free to skip the video. This video is 5 minutes.
Advanced Features
Configure Application Blocking

This feature, which is also called application authorization, enables administrators to build blacklists and whitelists of applications to control application and license sprawl. You can also create condition settings to control the circumstances under which an application can be used. For example, you can create a condition that allows a user access to company-specific applications only when the user is on the internal corporate network.

The following Configure Application Blocking section provides a brief overview of the application-blocking feature.
(Approximate read time: 2 minutes)

For the purposes of this Quick-Start Tutorial, we recommend that you limit this feature to endpoint devices used for testing purposes. After you are comfortable with the way the feature works, and have the appropriate application-blocking rules defined, you can expand to using devices in your production environment.

Prerequisites for Using Application Blocking

To perform this exercise, you need the following:

• Credentials for the virtual or physical machine where you installed and performed the initial configuration of the User Environment Manager Management Console, as described in Configure the User Environment Manager Management Console.

• End-user credentials for the virtual or physical endpoint machine where you installed the User Environment Manager Agent, as described in Install the User Environment Manager Agent (FlexEngine) on the Desktop or RDSH Server.

• One or more executable files with which to test application blocking. We recommend downloading the following executables for testing:
  • Putty
  • Notepad++

• To complete all exercises, we recommend creating the following file structure on a file-share server.
  • \<fileshare>\software
    Copy Putty.exe to the software folder.
  • \<fileshare>\software\installers
    Copy Notepad++ to the installers folder.

    The Domain Users group, or whichever group you selected in Profile Archives Share Prerequisites, must have read and execute permissions to this file share.

**Note:** Throughout this exercise you will frequently change between your Windows end-point device, where the User Environment Manager agent (FlexEngine) is installed, and the physical or virtual machine where the Management Console is installed. It is recommended that you simply minimize the unused screen to streamline the testing process.
1. Log In to the Desktop as an End User to Verify That Putty Can Run

Log in to your Windows end-point device where the User Environment Manager agent is installed.

For the example in this exercise, we used a Windows 10, instant-clone VM, accessed through the VMware Horizon Client.

1.1. Run Putty

From the Windows endpoint, browse to the file share and run Putty.exe.
1.2. Close Putty

Select **Cancel** to close Putty.

Remain logged in to the Windows endpoint device, but minimize the window before continuing to the next step.
2. Select Global Application Blocking in the Management Console

1. On the physical or virtual machine where the Management Console is installed, open the Management Console.
   From the Start screen, select the Management Console shortcut in the VMware UEM folder.
2. Select the User Environment tab.
3. Select Application Blocking.
4. Select Global Configuration.
3. Enable and Configure Application Blocking

1. Select Enable Application Blocking.
2. Select Add.

3.1. Specify the Path to the Windows Explorer Application

Browse to or enter the path to explorer.exe. Windows Explorer is considered a parent application, which means it is used to start other applications.
3.2. Complete the Configuration

Select OK to continue.

The **Message title**, **Message text**, and **Hide after** text boxes are automatically populated. These fields define the notification that the end-user receives when the user attempts to start an application that is blocked by User Environment Manager.

Although this notification is not required, we recommend that you leave this default configuration in place while testing the application-blocking feature.
3.3. Confirm Application Blocking

Review the disclaimer and select **OK** to continue. Application blocking is now enabled. If you use Windows Explorer to start an application whose executable file does not reside in `C:\Program Files` or `C:\Program Files (x86)`, you will see the notification you configured in the previous step, and the application will not start.

4. Refresh Settings and Verify That Application Blocking Is Enabled
1. Maximize the virtual desktop window or reconnect to your Windows endpoint device.
2. Open a command-prompt window and run the following command to force FlexEngine to check for updated application-blocking policies.

```
"C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe" -uemrefreshapplicationblocking
```

Application-blocking policy settings are read when a user logs in to Windows or when a triggered task occurs to refresh the policy settings. You can manually refresh the application-blocking policy settings on an endpoint device by running `FlexEngine.exe` at the command line with the appropriate argument.

There are a number of arguments that can be passed to `FlexEngine.exe`, as described in the following section. (Approximate read time: 2 minutes)

### 4.1. Verify That Running Putty from the File Share Is Blocked

From the Windows endpoint, browse to the file share and double-click the `Putty.exe` file.

This time, Putty is blocked by User Environment Manager. If the default settings were chosen when you enabled application blocking, a notification is displayed for ten seconds.
4.2. Verify That Running Putty from the Desktop Is Blocked

1. Copy `Putty.exe` from the file share to the virtual desktop.
2. Double-click `Putty.exe` and notice that again it is blocked from running.
4.3. Verify That Putty Runs from the Permitted Location

1. Copy Putty.exe to C:\Program Files.  
   **Note:** You may need to elevate permissions to copy the executable to this location.

2. Double-click Putty.exe and notice the executable runs normally. This is because C:\Program Files is one of the default whitelisted folders for application blocking.

   Remain logged in to the Windows endpoint, but minimize the window before continuing to the next step.
5. Create a Hash-Based Rule for Application Blocking

1. In the Management Console, select the User Environment tab.
2. Select Application Blocking.
3. Select Create to create a new Allow rule for application blocking.

User Environment Manager provides several types of application-blocking rules. After you select the rule type, you can create settings to allow or block applications. In this exercise, you will create a hash-based rule and a path-based rule.

The following section summarizes the rule types and the steps for creating application rules. (Approximate read time: 1 minute)
5.1. Specify the Name and Type for a Hash-Based Rule

1. In the Application Blocking dialog box that appeared after you completed the previous step, enter a name for this application-blocking rule.
2. Select Hash-based from the Type drop-down list.
3. In the Allow section, select Add to browse to an executable.

5.2. Select the Application Executable

Browse to the file share where Putty.exe is stored and select Putty.exe. Note that a hash of the executable is made.
5.3. Save the Hash-Based Rule

Select **Save** to commit the new application-blocking rule.
5.4. Refresh Application-Blocking Policies on the Virtual Desktop

1. Maximize the virtual desktop window or reconnect to your Windows endpoint device.
2. Open a command-prompt window and run the following command to force FlexEngine to check for updated application-blocking policies.

"C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe" -uemrefreshapplicationblocking
5.5. Verify That Putty Can Start from Any Location

1. Verify that `Putty.exe` runs from the Desktop.
2. Verify that `Putty.exe` runs from the file share.

With the application-blocking Allow rule in place, `Putty.exe` can now run from any location.
5.6. Verify That Putty Runs After You Rename the Executable

1. Rename `Putty.exe` to `myapp.exe`.
2. Double-click `myapp.exe` and notice the executable still runs.

One of the advantages of hash-based application-blocking rules is that they work even if the end user renames the executable.
6. Create an Approved Software Repository Using a Path-Based Rule for Application Blocking

1. In the Management Console, select the User Environment tab.
2. Select Application Blocking.
3. Select Create to create a new Allow rule for application blocking.

Enterprises often need to prevent end users from running executables located outside of an IT-approved repository. Because the contents of the repository might change over time, a path-based Allow rule is well-suited for this task.
6.1. Specify the Name and Type for a Path-Based Rule

1. Enter a name for this application-blocking rule.
2. Select Path-based from the Type drop-down list.
3. In the Allow section, select Add to browse to a folder.

6.2. Enter the Path to the Software Repository

Enter the path to the folder you want to use as a software repository.

This path should use the file structure you created as specified in Prerequisites for Using Application Blocking. For the example in this exercise, we use `\file\software\installers`.
6.3. Save the Path-Based Rule

Select Save to commit the new application-blocking rule.

Notice that an asterisk is automatically appended to the folder path. This wildcard character indicates that all executables in this folder will inherit the Allow rule.

6.4. Refresh Application-Blocking Policies on the Virtual Desktop

1. Maximize the virtual desktop window or reconnect to your Windows endpoint device.
2. Open a command-prompt window and run the following command to force FlexEngine to check for updated application-blocking policies.

```
"C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe" -UemRefreshApplicationBlocking
```
6.5. Verify That You Can Start an Application in the Software Repository

Navigate to `\<fileserver>\software\installers` and double-click the Notepad++ executable.

You can copy additional executables to this folder location and verify that application blocking allows them to run from this approved software repository.
7. Disable Application Blocking Before Proceeding to Other Exercises

1. In the Management Console, select the User Environment tab.
2. Select Application Blocking.
3. Select Global Configuration.

**Important:** Disabling application blocking is strongly recommended at this point to avoid having the feature interfere with other exercises.
8. De-select the Enable Application Blocking Check Box

1. Clear the Enable Application Blocking check box to disable the feature.
2. Select OK to commit the change.

The following [App Blocking](#) video provides a detailed demonstration of the steps for enabling application blocking. If you need additional detail, you can find it here. This video is 5 minutes.
Configure Privilege Elevation for Installing an Application

With privilege elevation, administrators can now allow end users to run certain applicators as administrators, as well as install their own applications if they meet the specified criteria. IT administrators can create rules that elevate privileges based on a file hash, a software publisher, or a path to a file or folder.

The following Configure Privilege Elevation section provides a brief overview of this feature. (Approximate read time: 2 minutes)

Prerequisites for Using Privilege Elevation

To perform this exercise, you need the following:

- Credentials for the virtual or physical machine where you installed and performed the initial configuration of the User Environment Manager Management Console, as described in Configure the User Environment Manager Management Console.
- End-user credentials for the virtual or physical endpoint machine where you installed the User Environment Manager Agent, as described in Install the User Environment Manager Agent (FlexEngine) on the Desktop or RDSH Server.

**Important**: The end-user credentials must have Local User privileges to the endpoint device, rather than Local Administrator privileges. The privilege elevation feature elevates privileges on specific executables, without requiring Local Administrator privileges.

- One or more executable files with which to test privilege elevation. We recommend downloading WireShark for testing. Starting this file requires Local Administrator privileges.
- To complete all exercises, we recommend creating the following file structure on a file-share server.

```\<fileshare>\software\installers```

Copy the WireShark file to the installers folder.

**Important**: The Domain Users group, or whichever group you selected in Profile Archives Share Prerequisites, must have read and execute permissions to this file share.

**Note**: Throughout this exercise, you will frequently change between your Windows end-point device, where the User Environment Manager agent (FlexEngine) is installed, and the physical or virtual machine where the Management Console is installed. It is recommended that you simply minimize the unused screen to streamline the testing process.
1. Verify Local User Privileges

Log in to your Windows end-point device, where the User Environment Manager agent is installed.

For the example in this exercise, we used a Windows 10, instant-clone VM, accessed through the VMware Horizon Client.

To properly demonstrate privilege elevation, you will verify that privileges for the end-user credentials are insufficient to run the Wireshark installer.

1.1. Attempt to Start Wireshark as an End User on the Virtual Desktop
1. Browse to the file share you created. For the example in this exercise, the path is `\\file\\software\installers`.
2. Double-click the Wireshark installer.

### 1.2. Verify That You Are Prompted for Administrator Credentials

![User Account Control](image)

Note that Windows User Account Control prompts you for administrator credentials because the end-user credentials lack the privileges required to run this installer.

Remain logged in to the Windows endpoint device, but minimize the window before continuing to the next step.
2. Select Global Privilege Elevation in the Management Console

1. On the physical or virtual machine where the Management Console is installed, open the Management Console.
   From the Start screen, select the Management Console shortcut in the VMware UEM folder. Select the User Environment tab.
2. Select Privilege Elevation.
3. Select Global Configuration.
2.1. Enable and Configure Privilege Elevation

1. Select Enable Privilege Elevation.
2. Select Also elevate all child processes. This is an optional, global setting that applies only to the case where you enable end users to install applications. This setting is not required to complete this exercise.
3. Select Ask user to elevate.
4. Enter text for Message title and Message text. This notification is displayed to the end user when the privilege elevation feature is invoked.

After you select OK a confirmation box appears.
2.2. Confirm Privilege Elevation

Review the disclaimer and select OK to continue. Privilege elevation is now enabled.

3. Create a Rule for Privilege Elevation

1. On the User Environment tab, select Privilege Elevation.
2. Select Create in the toolbar.

Privilege elevation operates as a whitelist. In addition to enabling the feature, you must create privilege elevation rules and specify files or folders to elevate.
3.1. Specify the Name and Type for the Privilege Election Rule

1. Enter a Name for this privilege elevation rule.
2. Select Path-based elevated application from the Type drop-down list.
3. Select Add to browse to a folder.

3.2. Select the Directory Path to Elevate

Browse to or type the path to the file share. For the example in this exercise, all executables in the file\software\installers folder will be elevated.
3.3. Save the Privilege Elevation Rule

1. Select **Also elevate child processes**.
2. Select **Save** to commit the new privilege elevation rule.
4. Refresh Privilege Elevation Rules on the Virtual Desktop

1. Maximize the virtual desktop window or reconnect to your Windows endpoint device.
2. Open a command-prompt window and run the following command to force FlexEngine to check for updated privilege elevation policies.

```
"C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe" -UemRefreshPrivilegeElevation
```

Privilege elevation policy settings are read when a user logs in to Windows or when a triggered task occurs to refresh the policy settings. You can manually refresh the privilege elevation policy settings by running **FlexEngine.exe** at the command line with the appropriate argument.

There are a number of arguments that can be passed to **FlexEngine.exe**, as described in the following section. (Approximate read time: **2 minutes**
5. Start the Wireshark Installer

1. Browse to the file share you created. In this case, the path is `\file\software\installers`.
2. Double-click the Wireshark installer.
   A notification is displayed with the text you entered when configuring the privilege elevation feature.
3. Select Yes to elevate the installer.
6. Verify That the Installer Runs Without Prompting for Administrator Credentials

![Wireshark Setup Wizard]

Notice that the setup wizard starts. This time, the Wireshark installer runs without the Windows User Account Control prompt for alternate credentials.

The following Privilege Elevation video provides a detailed demonstration of the steps outlined in this exercise. If you need additional detail, you can find it here. This video is 2 minutes.

Additional Information and Use Cases for Privilege Elevation

In this exercise, you created a single, path-based privilege elevation rule. User Environment Manager provides several types of privilege elevation rules, including the ability to elevate executables for applications that have already been installed but that require local administrator privileges to run.

The following User Environment Manager 9.2 - Privilege Elevation Demo video provides demos of several use cases, as well as a brief technical discussion of the way privilege elevation uses Access Tokens in Windows. This video is 8 minutes.
Horizon Smart Policies
Introduction to Horizon Smart Policies

This chapter introduces you to the Horizon Smart Policies feature of VMware User Environment Manager, which is included with VMware Horizon 7 Enterprise Edition. The exercises demonstrate the process of creating Horizon Smart Policies and applying them based on conditions such as user group, client device type, pool name, and more.

For an overview of Horizon 7, and information about key features, such as publishing applications, creating instant-clone desktops, and more, see the Reviewer’s Guide for View in Horizon 7: Overview.

What Are Horizon Smart Policies?

With Smart Policies, administrators have granular control of a user’s desktop experience. A number of key Horizon 7 features can be dynamically enabled, disabled, or controlled based not only on who the user is, but on the many different variables available through Horizon 7: client device, IP address, pool name, and so on.

You can use Smart Policies to enable or disable features including clipboard redirection, USB access, printing, and client drive redirection. For example, you can create a policy so that a desktop login from outside the corporate network results in disabling of security-sensitive features such as cut-and-paste or USB drive access. Additionally, bandwidth profile settings allow you to customize the user experience based on user context and location.

Smart Policies can be enforced based on role, and evaluated at login and logout, disconnect and reconnect, and at predetermined refresh intervals. With all these capabilities and fine-grained control, you can use one desktop pool to address many different use cases.

Note: In most cases, Smart Policy settings that you configure for remote desktop features in User Environment Manager override any equivalent registry key and group policy settings.

Features Controlled by Smart Policies

You can use Smart Policies to enable, restrict, or disable Horizon 7 features that include clipboard redirection, USB access, printing, and client drive redirection, and you can select a profile that manages bandwidth usage.

- **USB redirection** – Controls whether a user is allowed to use locally attached USB devices, such as thumb flash drives, cameras, and printers, from the remote desktop.
- **Printing** – Controls if a user is allowed to print documents from the remote desktop to a network printer or a USB printer that is attached to the client computer.
- **Clipboard** – Controls whether users are allowed to copy and paste text and graphics only from the client system to the remote desktop, only from the remote desktop or application to the client system, or both, or neither.
• **Client drive redirection** – Controls whether drives and folders on the client system are shared with the remote desktop and, if so, whether they are readable only or readable and writeable.

• **HTML Access file transfer** (available with User Environment Manager 9.1 and later) – Controls whether you can upload files from the client system to the remote desktop, download files from the remote desktop to the client system, or both, or neither, when you are using the web client to access the remote desktop. Note that this feature requires Connection Server and Horizon Agent 7.0.1 or later.

• **Bandwidth profile** – Prevents the agent (remote desktop) from attempting to transmit data at a higher rate than the link capacity.

**Note:** If you have User Environment Manager 9.1 or later and Horizon Agent 7.0.1 or later, this setting applies when users are using either the Blast Extreme display protocol or the PCoIP display protocol. If you have User Environment Manager 9.0, this setting is called PCoIP Profile and applies only when users are using PCoIP.

The actual bit rate for the profiles varies, depending on whether you use the PCoIP or the Blast Extreme display protocol. For this reason, the list of profiles in the menu does not display the bit rate next to the profile name in User Environment Manager 9.1 or later.

![Horizon Smart Policies](image)

**Figure 1:** Bandwidth Profile List

For details about the profiles, see the profile reference topic in the *Using Smart Policies* section of [Configuring Remote Desktop Features in Horizon 7](#).
How Smart Policies Are Applied

To create a Smart Policy, you select settings for the Horizon 7 features that you want to control and specify the conditions, if any, under which the policy will go into effect. If you do not specify any conditions, the policy is applied to all users in the user OU configured for User Environment Manager.

Settings are always applied when the user logs in. You can optionally configure triggers to also re-evaluate the settings at other times, such as when users reconnect to the desktop or application.

When Users Do Not Match the Conditions That Are Set

If you specify conditions, the policy is applied to users who match the conditions. For users who do not match the conditions, no functionality changes are made to the features. For example, by default, you can copy and paste text from your client system to a remote desktop or application. If you create a policy that says clipboard redirection is disabled for a certain group of users, then users outside of this group will still be able to copy and paste text from the client to the remote desktop or application, unless the administrator has used some other method to configure the feature.

When a Setting Within a Policy Is Not Specified

If you create a Smart Policy but do not select the check box for a feature, then no functionality changes are made to that feature. For example, by default, you can copy and paste text from your client system to a remote desktop or application. If you create a Smart Policy and do not select the Clipboard check box, the user will continue to be able to copy and paste from the client system to the remote desktop or application.

You might notice that the default Smart Policy setting for the Clipboard check box is Allow All, but unless you select the check box, the Allow All setting is not used. That is, the default settings shown for the check boxes do not reflect the default settings used by the features when no policies are applied.

When Users Match Conditions for Multiple Policies

User Environment Manager processes multiple policies in alphabetical order based on the policy name. Horizon Smart Policies appear in alphabetical order in the Horizon Smart Policies pane. If policies conflict, the last policy processed takes precedence.

In some environments, you might want to strictly control functionality even when no policies are being matched on their conditions and therefore any functionality would normally be left as is. For these environments, create a default policy that sets all features, except the bandwidth
profile, to **Disabled**. Use no conditions so that the policy is always matched, and give the policy a name that begins with “A,” such as **A Default Policy**. Because policies are evaluated in alphabetical order, this policy will be first in the list and because it has no conditions it will always be matched.

Then create your other policies with conditions to enable or set specific features when those conditions are matched (for example, client location or specific groups of users), as outlined in the exercises that follow. These other policies will be processed after the default policy, and the resultant feature settings will be applied only after all policies have been evaluated.

If no policies match, then the default policy will disable all controlled functionality. If another policy matches, then the settings in that policy will override the default policy you created.
Create a Basic Smart Policy for Internal Users

Now that you have installed and configured User Environment Manager, you can use policy settings that are readily available in the User Environment Manager Management Console. You will enable USB access and clipboard redirection and assign a bandwidth profile. The conditions that must be met for this policy to be applied are that the user must connect from inside the corporate network and must connect to a desktop from the Human Resources (HR) pool.

Prerequisites

If you want to apply these settings to an actual desktop or application pool in your environment, you must create the desktop or application pool and entitle it to a group of users included in the user OU configured for User Environment Manager. Having an existing pool is not required, however, if you just want to see how the management console works and try creating a policy.

1. Click the Create Button for Horizon Smart Policies

1. In the User Environment Manager Management Console, click the User Environment tab.
2. Select Horizon Smart Policies in the left pane.
3. Click Create in the toolbar.
2. Complete the Settings Tab for Internal Users

On the **Settings** tab, enter the following settings:

- Enter a name for the policy.

  The **Label** and **Tag** fields are optional. You can use them to describe or organize the settings. The **Group By Tag** ribbon button uses the **Tag** field for grouping the list items.

- Select the check boxes next to **USB redirection**, **Clipboard**, and **Bandwidth profile**.

- For **Bandwidth profile**, select **LAN**.
3. Add a Condition for a Horizon Client Property

1. On the Conditions tab, click Add.
2. Select Horizon Client Property.

4. Set the Client Location to Internal

1. For Property, select Client location.
2. Set the location to Internal.
3. Click OK.

This setting is compared with the `gatewayLocation` property set for the server.

- By default, if you connect directly to a Connection Server, the gateway location is `Internal`.
• If you connect to a VMware Unified Access Gateway appliance or Security Server, the gateway location is **External** by default.

If you want to override the default location reported from a server, you can change these defaults by setting the gatewayLocation property in the locked.properties file for the server. For instructions, see the Configure the Gateway Location for a View Connection Server or Security Server Host.

5. Add Another Horizon Client Condition

1. On the **Conditions** tab, click **Add**.
2. Select Horizon Client Property.

6. Set a Specific Pool Name

1. For **Property**, select **Pool name**.
2. Set **Starts with** to HR (or the first few letters of the name of an actual desktop pool you want to use).

3. Click **OK**.

By default, this new condition is added with an AND operator, meaning that the condition is applied if the user is connecting from inside the corporate network and if the user is trying to access a desktop pool that begins with the letters you specified.

**7. View the Operators Available for Combining Conditions**

![Horizon Smart Policies](image)

On the **Conditions** tab, click **Edit** to see which other operators are available to combine conditions.

The Smart Policy settings and conditions are now defined. These settings are always evaluated and applied whenever the user logs in. Next, you will specify an event that triggers the reevaluation of the Smart Policy whenever the user reconnects, rather than logs in. This is called a **triggered task**.
8. Create a Triggered Task

1. Select **Triggered Tasks** in the left pane.
2. Click **Create** in the toolbar.
9. Complete the Settings for the Triggered Task

1. On the **Settings** tab, enter a name for the task.

   The **Label** and **Tag** fields are optional. You can use them to describe or organize the settings. The **Group By Tag** ribbon button uses the **Tag** field for grouping the list items.

2. For **Trigger**, select **Session reconnected**. The Smart Policies will be reevaluated and applied every time the user connects to the remote desktop.

3. For **Action**, select **User Environment refresh**.
10. Specify That Smart Policies Are to Be Refreshed

In the list of check boxes that appear after you select **User Environment refresh**, select the **Horizon Smart Policies** check box and click **Save**.

Refreshing the user environment in this case means reevaluating the user’s connection characteristics, such as internal or external, and reapplying the Smart Policy appropriately. For example, if the user first connects at the office but then later connects from a café or other external network, the Smart Policy is reapplied to disable USB redirection and copying and pasting between the client and remote desktop.

In a production environment, you can select additional check boxes, depending on the other User Environment settings you configure.

**Note:** The **Privilege Elevation Settings** and **Triggered Task Settings** check boxes were added in User Environment Manager 9.2. Although these features are not part of Smart Policies, they can be used in conjunction with Smart Policies, such as when managing Just-in-Time Desktops and Apps as part of a JMP approach.

- The **Privilege Elevation Settings** option refreshes settings for the privilege-elevation feature. With this feature, administrators specify applications that end users are allowed to install or run without having elevated privileges. Standard user accounts can run these applications as if they were a member of the local administrators group.
- The **Triggered Task Settings** option allows triggered task settings to be refreshed when users disconnect, reconnect, or lock or unlock their workstation. Previously, these settings were refreshed only after users logged out of the virtual desktop or application.
The Smart Policy you created will now be applied whenever a user connects to a remote desktop with Horizon Client.
Create a Smart Policy Based on User Group

In this exercise, you explore some of the more advanced condition settings. Horizon Client properties give you many variables for evaluating conditions and applying Smart Policies. Some of these properties are provided in drop-down menus in the User Environment Manager Management Console, but many more are available when you enter the property name, which is derived from Windows Registry keys.

To view these properties, use Horizon Client to log in to a remote desktop, open the Windows Registry Editor (regedit.exe) on the remote desktop, and go to HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\SessionData\n, where n is the number of the session, as shown in the following figure. When creating Smart Policies, you enter the properties names without the ViewClient_prefix. The SessionData registry setting is created when you log in using Horizon Client or the HTML Access web client. If you log in with HTML Access, fewer properties are listed.

![Horizon Client Properties from the Windows Registry on the Remote Desktop](image)

Figure 2: Horizon Client Properties from the Windows Registry on the Remote Desktop

In this exercise, you create a Smart Policy that enables all features for a select Active Directory group of users who log in to a server with a specific launch tag and whose remote desktop belongs to a specific domain.
1. Click the Create Button for Horizon Smart Policies

1. In the User Environment Manager Management Console, click the User Environment tab.
2. Select Horizon Smart Policies in the left pane.
3. Click Create in the toolbar.
2. Complete the Settings Tab for the Group of External Users

On the **Settings** tab, enter the following settings:

- Enter a name for the policy.

  The **Label** and **Tag** fields are optional. You can use them to describe or organize the settings. The **Group By Tag** ribbon button uses the **Tag** field for grouping the list items.

- Select all the check boxes.
- For **Bandwidth profile**, select **LAN**.
3. Add a Condition for a Horizon Client Property

1. On the Conditions tab, click Add.
2. Select Horizon Client Property.

4. Set the Launch Tag

1. For Property, select Launch tag(s).
2. In the second list, select Is equal to.
3. In the text box, enter the tag name HR-Dept.

The tag name HR-Dept is a hypothetical name. To create a condition that will actually work in your environment, you must enter a tag name that you have actually assigned to a Connection Server and a desktop pool. For more information about assigning tags, see the topic Restricting Desktop or Application Access in Setting Up Virtual Desktops in Horizon 7.
4. Click OK.
5. Add Another Horizon Client Condition

1. On the Conditions tab, click Add.
2. Select Horizon Client Property.

6. Set a Specific Machine Domain

1. For Property, enter `Machine_Domain`.

   This property is derived from the Windows Registry key called `ViewClient_Machine_Domain`, which is pictured in Figure 2. You do not enter the `ViewClient_` portion of the name.
2. In the second list, select Is equal to.
3. In the text box on the right, enter `MyDomain` (or the name of an actual domain in your enterprise).
4. Click OK.

7. Add a Condition for Group Membership

1. On the Conditions tab, click Add.
2. Select Group Membership.

8. Complete the Group Membership Box

1. Select User.
2. Click Browse.
9. Select a User Group

1. Enter a user group name.
2. Click Check Names and select a name.
3. Click OK.

10. Click OK in the Group Membership Box

Accept the defaults and click OK.
11. Save the New Smart Policy

Click **Save**. The default operator AND is used to combine the conditions, which is correct for this exercise.

This Smart Policy is set to enable all features and use the LAN bandwidth profile for all users from the Domain Admins user group who connect to a server and desktop assigned the HR-Dept tag and whose remote desktop VM belongs to the specified domain.

For more information about conditions and client properties, see *Adding Conditions to Horizon Policy Definitions* in *Configuring Remote Desktop Features in Horizon 7*.

You do not need to create a triggered task because you created a triggered task during the first exercise.
Verify That a Smart Policy Is Being Applied

In this exercise, you look at the User Environment Manager log to see that a Smart Policy is being evaluated and applied to a particular user.

Prerequisites

The first four steps of this procedure guide you through setting the logging level using the Group Policy Management Console. Before you can perform these steps, you must have created a FlexEngine GPO, as described in Initial Configuration Using an Active Directory Group Policy Object.

If instead you configured User Environment Manager using NoAD mode, you have already set the logging level to Debug, as described in Create the User Environment Manager NoAD Configuration File. In this case, you can skip to Step 5 of this exercise.

1. Log In to Active Directory and Launch the Group Policy Management Console

1. Type `group policy management` into the search box on the taskbar.
2. Select Group Policy Management in the results.
2. Edit the Group Policy Object

1. Expand your domain.
2. Expand Group Policy Objects.
3. Select the GPO that you created for the User Environment Manager group policy settings.
4. From the Action menu, select Edit.

3. Open the FlexEngine Logging Policy

1. Navigate to User Configuration > Policies > Administrative Templates > VMware UEM > FlexEngine.
2. In the right pane, double-click FlexEngine logging.
4. Set the Logging Level to Debug

1. Verify that logging is set to **Enabled**.
2. Select **Debug** as the log level.
3. Click **OK**.

VMware recommends that you set the log level to **Debug** only temporarily because the amount of logging can affect performance.

**Note:** This dialog box also shows the location of the log file. You specified the log file location when you installed and set up User Environment Manager.
5. Log In to the Virtual Desktop

Log in as a user to a virtual desktop that matches the Smart Policy.
Logging in will create a User Environment Manager log file for the user.

6. Search the User’s FlexEngine Log File for "Applied Horizon Smart Policies Settings"

On the file share machine, open the user’s FlexEngine log file, and search from the bottom up for Applied Horizon Smart Policies settings. For the example in this exercise, the path to this folder is `\\<file-share>\UEM_Profiles\<username>\Archives\Logs`.

In this example, the user does not meet the conditions for the policy called Internal, so those settings are skipped. Because the `Broker_GatewayLocation` property is set to External, the Smart Policy called External is applied for all the feature settings.
**Note:** In this example, the user logged in from an external location. You might be performing this exercise from your corporate office, using a desktop or some other test machine, which would be an **internal** device.
Summary and Next Steps
Introduction

This Quick-Start Tutorial introduced you to User Environment Manager and enabled you to set up a proof-of-concept environment through practical exercises.

After you have deployed your proof-of-concept implementation, you can explore the product further or plan your production environment by examining Additional Resources.
## Terminology Used in This Tutorial

The following terms are used in this tutorial.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant clone</td>
<td>A copy of an existing VM that shares virtual disks with the parent VM, but that, at creation time, shares the memory of the running parent VM from which it is created.</td>
</tr>
<tr>
<td>Instant-clone desktop</td>
<td>A virtual desktop run from a snapshot of a parent VM. An instant-clone desktop is always deleted and re-created when the user logs off.</td>
</tr>
<tr>
<td>Master image</td>
<td>A VM that has been created and configured for desktop deployment and which will serve as the core image for clones. For full clones, the master image is a VM template. For instant clones, the master image is the parent VM plus a selected VM snapshot. The master image can also be referred to as a desktop image, a golden image, or an instant-clone desktop image.</td>
</tr>
<tr>
<td>Virtual desktop</td>
<td>The user interface of a virtual machine that has been made available to an end user.</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>A software computer running an operating system or application environment that is backed by the physical resources of a host.</td>
</tr>
</tbody>
</table>

For more information about terms, see the [VMware Glossary](https://www.vmware.com/vmware-glossary.html).

To comment on this paper, contact VMware End-User-Computing Technical Marketing at [euc_tech_content_feedback@vmware.com](mailto:euc_tech_content_feedback@vmware.com).
Additional Resources

For more information about User Environment Manager, you can explore the following resources:

- Benefits of VMware Horizon Cloud on Microsoft Azure & VMware User Environment Manager
- Evaluate VMware Products
- Horizon Support Center
- Profiling Applications with VMware User Environment Manager, Part 1: Introduction to Application Profiler
- Profiling Applications with VMware User Environment Manager, Part 2: Applying and Troubleshooting Predefined Settings
- User Environment Manager Documentation
- VMware Knowledge Base:
  - Enabling debug logging for a single user in VMware User Environment Manager (2113514)
- VMware Product Guide
- VMware Product Interoperability Matrices
- VMware Professional Services
- VMware User Environment Manager with VMware App Volumes
- VMware vSphere documentation
- VMware Workspace ONE and VMware Horizon Packaging and Licensing guide
About the Authors

Josh Spencer is an End-User-Computing Architect in the Technical Marketing group at VMware.

Caroline Arakelian is a Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware.

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.