VMWARE USER ENVIRONMENT MANAGER DEPLOYMENT CONSIDERATIONS
VMware User Environment Manager 9.1
Table of Contents

Introduction ......................................................................................................................... 4
  Audience .......................................................................................................................... 4
  What Is VMware User Environment Manager? .............................................................. 4
  How User Environment Manager Works .................................................................... 5
  User Environment Manager Terminology ................................................................... 5

User Environment Manager Overview ............................................................................. 6
  Application Configuration Management ................................................................ 6
  Personalization .................................................................................................................. 7
  User Environment Settings ........................................................................................... 7
  Dynamic Configuration ................................................................................................. 7

Planning the Deployment ................................................................................................. 8
  User Environment Manager Configuration Share .................................................... 9
    Centralized IT Infrastructure .................................................................................... 10
    Decentralized IT Infrastructure with Multiple Locations ....................................... 10
    Multiple Environments ............................................................................................ 11
    Centrally Managed User Environment Manager Environments ......................... 11
    Tiered User Environment Manager Environments .................................................. 12
  User Environment Manager Profile Archives Share .................................................. 13
  FlexEngine Group Policy Configuration ................................................................ 14
    Mandatory GPO Settings ......................................................................................... 15
    Optional GPO Settings ............................................................................................. 15
  FlexEngine NoAD Mode ............................................................................................... 16
  FlexEngine .................................................................................................................... 17
    DirectFlex .................................................................................................................. 17
    Triggers ....................................................................................................................... 18
    SyncTool for Offline Scenarios ................................................................................. 18

Infrastructure Design ...................................................................................................... 20
  Scalability ....................................................................................................................... 20
  High Availability .......................................................................................................... 21
  Disaster Recovery ......................................................................................................... 21

Upgrading ........................................................................................................................... 22
# VMWARE USER ENVIRONMENT MANAGER DEPLOYMENT CONSIDERATIONS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDSH and VDI Integration</td>
<td>22</td>
</tr>
<tr>
<td>Application Virtualization Integration</td>
<td>23</td>
</tr>
<tr>
<td>Access Control</td>
<td>24</td>
</tr>
<tr>
<td>- Configure Management Console Through GPO</td>
<td>24</td>
</tr>
<tr>
<td>- Export Settings Between Environments</td>
<td>24</td>
</tr>
<tr>
<td>- Application Profiler</td>
<td>25</td>
</tr>
<tr>
<td>Best Practices</td>
<td>25</td>
</tr>
<tr>
<td>- Initial Setup and Installation Best Practices</td>
<td>25</td>
</tr>
<tr>
<td>- Management Best Practices</td>
<td>26</td>
</tr>
<tr>
<td>- Troubleshooting Best Practices</td>
<td>27</td>
</tr>
<tr>
<td>- Folder Redirection Best Practices</td>
<td>27</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>29</td>
</tr>
<tr>
<td>About the Authors and Contributors</td>
<td>30</td>
</tr>
</tbody>
</table>
Introduction
The VMware User Environment Manager Deployment Considerations guide helps administrators plan and design phases of a VMware User Environment Manager™ deployment. It includes examples of common deployment scenarios, including guidance for scalability, high-availability, and disaster recovery. For more information, see Installing and Configuring VMware User Environment Manager and the VMware User Environment Manager Administration Guide.

Audience
This guide is for architects, consultants, IT professionals, or anyone involved in creating high-level, functional, and technical designs.

What Is VMware User Environment Manager?
User Environment Manager provides end users with a personalized and dynamic Windows desktop based on their role, device, and location. User Environment Manager is a cost-effective solution that requires minimal infrastructure.

Many organizations suffer from productivity loss because of ad hoc activities for end users, such as manually mapping network drives and printers, creating policy settings, or providing application shortcuts.

User Environment Manager provides several benefits:

• Increases productivity by delivering consistent and personalized desktops across devices
• Reduces help desk workload with the provided Helpdesk Support Tool and the Self-Support tool
• Improves login and logout times by using DirectFlex, which imports only the settings needed when an application is started, folder redirection, and profile segmentation
• Scales seamlessly by leveraging the existing Windows infrastructure
• Requires minimal infrastructure

User Environment Manager is a component of the Just-in-Time Management Platform (JMP). JMP (pronounced jump) represents capabilities in VMware Horizon® 7 Enterprise Edition that deliver Just-in-Time Desktops and Apps in a flexible, fast, and personalized manner. JMP is composed of the following VMware technologies:

• VMware Instant Clone Technology for fast desktop and Remote Desktop Session Host (RDSH) provisioning
• VMware App Volumes™ for real-time application delivery
• User Environment Manager for contextual policy management

JMP allows components of a desktop or RDSH server to be decoupled and managed independently in a centralized manner, yet reconstituted on demand to deliver a personalized user workspace when needed. JMP is supported with both on-premises and cloud-based Horizon 7 deployments, providing a unified and consistent management platform regardless of your deployment topology. The JMP approach provides several key benefits, including simplified desktop and RDSH image management, faster delivery and maintenance of applications, and elimination of the need to manage “full persistent” desktops.
How User Environment Manager Works
FlexEngine clients are installed on virtual desktops or Microsoft RDSH servers and physical devices, such as desktop computers and laptops. Using the provided administrative templates, IT creates an Active Directory Group Policy Object (GPO) and uses the GPO to enable and configure FlexEngine. IT creates Flex configuration files using the User Environment Manager Management Console. The configuration files contain application, Windows, and user environment settings.

User Environment Manager is context aware and applies settings using conditions. When a user logs in to a laptop or virtual desktop, FlexEngine imports the user environment and personalization settings based on these conditions. Network and printer mappings, application blocking rules, shortcuts, and many more settings are configured according to the policy.

The DirectFlex feature allows FlexEngine to import application settings only when a user starts an application. The application settings can be predefined and preconfigured for quick application access. Settings can be applied to published applications and virtual desktops, such as Horizon 7, RDSH desktops and applications, or Citrix XenApp and XenDesktop.

User Environment Manager Terminology
The following table describes the terminology used in reference to installing and configuring User Environment Manager.

<table>
<thead>
<tr>
<th>TERM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Configuration share   | The UNC path to the share where the Flex configuration files are stored.  
| Flex configuration file| A Flex configuration file contains application, Windows, and user environment settings. The User Environment Manager Management Console creates and manages the Flex configuration file.  
| DirectFlex            | DirectFlex imports application settings when an application is started, instead of importing the settings at login. DirectFlex is an optional setting.  
| FlexEngine            | The client component that is installed on each managed physical or virtual Windows device.  
| General folder        | The User Environment Manager Management Console creates the General folder in the User Environment Manager configuration share. The General folder is where Flex configuration files are created, managed, and accessed by FlexEngine.  
| Management Console    | The main user interface used to manage user profiles, Flex configuration files, and user environment settings.  
| Profile archive       | The profile archive is a ZIP file where FlexEngine stores the users’ personalized settings based on the content of the Flex configuration files. A profile archive is created for each user.  

Table 1: User Environment Manager Terminology
User Environment Manager Overview

User Environment Manager offers a complete user environment management solution without requiring additional back-end infrastructure servers. It can manage user and Windows settings and dynamically configure the desktop. For example, User Environment Manager can create drive and printer mappings, file type associations, and shortcuts. User Environment Manager can even manage virtual applications for users.

Figure 1 highlights the Windows components that JMP can centrally manage. The next sections describe these User Environment Manager functionalities.

![Figure 1: Windows Components Managed Through JMP](image)

Application Configuration Management

User Environment Manager application configuration management enables you to configure the initial settings of an application without forcing users to use application defaults. You can use predefined settings as one-time defaults or have them set each time the application starts to ensure that application settings are always in the same state. A hybrid approach is also possible: Define which application settings can be personalized and which always remain at their initial values.

Using User Environment Manager Application Profiler, you can capture predefined settings for an application. Run the application on a reference system (monitored by Application Profiler) and configure it as required. See Application Profiler.

User Environment Manager also provides the capability to manage certain user environment settings when an application is started, such as mapping drives and printers, applying custom files, folders, and registry settings, and running custom tasks.

With application configuration management, IT administrators can easily manage end users. IT can define settings and configurations for all users and ensure compliance with company policy. For example, IT might require a certain message to be shown whenever the end user starts an enterprise application.
Personalization
User Environment Manager personalization decouples and segments user-specific desktop and application settings from the Windows operating system (OS), making them available across multiple devices, Windows versions, and application instances. Because application settings are managed with User Environment Manager, you can start using application virtualization technologies, such as VMware ThinApp®, Microsoft App-V, and Citrix XenApp, and retain existing user settings. Users can instantly migrate to a newer Windows version or application virtualization technology without losing their personal settings.

User Environment Manager personalization integrates seamlessly with natively installed and virtualized applications, providing users with one user profile and a consistent user experience across any Windows platform: physical, virtual, or cloud-based desktops. Additionally, personalization simplifies Windows upgrades, such as migrating from Windows 7 to Windows 10. Users can roam between client and server OS versions, like Windows Server 2008 R2 or Windows Server 2012.

Personalization is a key feature of User Environment Manager. With personalization, IT can provide default settings while allowing end users to personalize additional settings. For example, developers can customize and preserve Eclipse settings across multiple development environments while quality engineers can set their bug-tracking website as the home page of all browsers.

User Environment Settings
User Environment Manager enables you to centrally manage a variety of settings that users need to perform daily tasks. The user environment settings that you configure are applied when users log in.

The following user settings are supported:
• ADMX-based settings (user policies)
• Application blocking
• Drive and printer mappings
• Environment variables
• Folder redirection
• Horizon Smart Policies
• Application shortcuts and file type associations
• Custom files, folders, and registry settings
• Custom tasks during login, logout, lock, unlock, disconnect, and reconnect

For example, a multinational corporation with end users from different countries can centrally manage the various display languages, wallpaper, and keyboard configurations.

Dynamic Configuration
User Environment Manager condition sets allow you to combine conditions based on user, location, and device characteristics, enabling dynamic adaptation of content and the appearance of the end-user desktop. For example, you can provide access to a network printer based on the user’s current location or create an application shortcut on the desktop based on the user’s identity. You can also define separate application configurations for various departments, such as Finance and IT.

Condition sets are managed centrally from the User Environment Manager Management Console and can be applied to all configurable items within User Environment Manager, such as the settings for personalization, user environment, and application configuration. You can also apply different configurations based on specific conditions. In this way, you decouple the configuration from the environment and applications.
Planning the Deployment

User Environment Manager does not need additional infrastructure components, such as SQL databases. Instead, it leverages the existing infrastructure.

User Environment Manager uses the following components in the IT infrastructure:

- **User Environment Manager Configuration Share** – The configuration share can be replicated for multisite scenarios. You can use multiple GPOs to configure the path to the share for all client devices.
- **User Environment Manager Profile Archives Share** – For best performance, place the profile archives on a share close to the computer where FlexEngine runs.
- **(Optional) Active Directory GPO for configuration of FlexEngine** – ADMX template files are provided with User Environment Manager.
- **FlexEngine** – Client component, installed on managed Windows computers.

Figure 2 shows how these components work together and the protocols used to communicate. User Environment Manager does not use custom ports, but it leverages existing Windows protocols, mainly Server Message Block (SMB).

![Diagram of User Environment Manager Technical Infrastructure](image)

**Figure 2:** Overview of the User Environment Manager Technical Infrastructure

For the ports that SMB uses, see [Server Message Block](#). For the ports required by GPOs, see the Microsoft article, [Configure Firewall Port Requirements for Group Policy](#).
User Environment Manager Configuration Share

The User Environment Manager configuration share has a predefined folder structure. The General folder contains the Flex configuration files. IT can optionally create subfolders under the General folder to better organize applications. The Flex configuration files are used for personalization and application configuration management (predefined settings).

The General folder also contains the mandatory FlexRepository folder. This folder, created automatically, contains all the configuration files for the user environment settings and dynamic configuration features of User Environment Manager, including shortcuts, file type associations, and condition sets.

Figure 3 shows the folder structure in the Management Console. The FlexRepository folder is hidden from the Management Console.

![Figure 3: Management Console Personalization Tree View](image)

The User Environment Manager configuration share is accessed during login and logout and during starting and closing of DirectFlex-enabled applications. To provide the best performance and fastest login times, store the configuration share in the same data center or network location as the user desktop. Because User Environment Manager accesses data only when needed in real time, for example, when an application is started, the bandwidth used to access this folder is low. The bandwidth used mainly depends on the number of configuration files and the size of the predefined settings.

Total storage space needed for this share is low. In a typical environment, 1 GB is sufficient for deployments up to 5,000 users.
An example share name is `\server\UEMconfigshare$`.

The minimum share permissions are **change** for administrators and **read** for users. Set the following NTFS security permissions on this share:

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERMISSION</th>
<th>APPLY TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>Full control</td>
<td>This folder, subfolders, and files</td>
</tr>
<tr>
<td>Users</td>
<td>Read &amp; execute</td>
<td>This folder only</td>
</tr>
</tbody>
</table>

Table 2: NTFS Security Permissions for the Configuration Share

The layout of the IT infrastructure determines where to create this share. See [Centralized IT Infrastructure](#) and [Decentralized IT Infrastructure with Multiple Locations](#).

**Centralized IT Infrastructure**

In a centralized infrastructure with products such as Horizon 7, Microsoft RDSH, or Citrix XenApp, FlexEngine runs on the virtual desktops or RDSH servers in the data center. In this scenario, using the same data center for the User Environment Manager configuration share provides the best performance. This scenario is also the easiest because the configuration share needs to be available only in one central location.

For a configuration share in the same data center as desktops, do one of the following:

- Use an existing file server (cluster) to create the User Environment Manager configuration SMB share.
- Create a file server for the User Environment Manager configuration SMB share.

Which option to choose depends on the current load of the file server and the number of users. To determine the best solution, create a test environment to measure the performance. Some best practices are covered in [Best Practices](#).

**Decentralized IT Infrastructure with Multiple Locations**

In a decentralized infrastructure with fat clients dispersed across different locations connected through WAN links, the User Environment Manager configuration share can be replicated to file servers at multiple locations.

If the locations are connected with a LAN, you can also use a central User Environment Manager configuration share. As with all infrastructure changes and products, the solution depends on your specific scenario. The only way to determine the best solution with the best performance is to test thoroughly.

In general, it is best to use your existing replication methods. If you have a SAN or NAS that provides a replication solution for high availability and disaster recovery, use that. The replication method can be either file-based or block-based replication. If you already use Microsoft Failover Clustering or DFS, use that. You can also use scripts to create an infrastructure that supports User Environment Manager.

You can configure the different clients to connect to the right User Environment Manager environment by using multiple Active Directory GPOs, as described in [Multiple Environments](#).
Multiple Environments
Creating and managing multiple User Environment Manager environments is easy. Having multiple separated environments can also be a requirement in a multitenant infrastructure or to separate departments.

You create multiple environments by creating multiple User Environment Manager configuration shares and manage them from a central installation of the Management Console. With the Management Console, you can switch between environments and export and import settings between different environments. You can configure the Management Console manually or through GPO.

See Managing Multiple Environments in the VMware User Environment Manager Administration Guide. For information on importing and exporting settings between different User Environment Manager environments, see Configuring Application and Windows Settings in the VMware User Environment Manager Administration Guide.

Centrally Managed User Environment Manager Environments
Figure 4 shows an example of two users with separate User Environment Manager environments, managed centrally with the User Environment Manager management tools.

A central IT department can manage multiple User Environment Manager environments. This example assumes that the User Environment Manager clients for the two users are in different Active Directory domains, and IT uses two GPOs (one in each domain) to configure the clients. Each domain has its own User Environment Manager configuration and profile shares. IT manages each environment centrally and can create new printer mappings, reset profiles, and so on.
Tiered User Environment Manager Environments

User Environment Manager supports a tiered model with development, test, acceptance, and production environments. Figure 5 illustrates tiered User Environment Manager environments. Changes are made in the central development environment and then copied to the departments’ acceptance environments. Environment-specific administrators can use their own installed User Environment Manager management tools to test and accept changes and move them to production.

This example requires both environment A and B to install their own User Environment Manager, so each environment can be managed separately. The tiered approach with development, acceptance, and production allows users to test the configuration in different environments before moving those changes to production. This setup does not require multiple Active Directory domains.

The setup of FlexEngine and file shares is the same as a regular setup but additional GPOs are used to link computers to the correct environment. For example, create a GPO called Acceptance and link a set of computers to this GPO. Use these computers to test changes before copying them to the production environment. Using multiple GPOs allows you to separate computers and link them to the correct User Environment Management environment.

Functionality is not limited to the use cases depicted in Figure 4 and Figure 5. For instance, you could also combine the two use cases or design your own approach.
User Environment Manager Profile Archives Share
This share stores personal settings for all users. A unique subfolder is created for each user. The personal user settings are read from this share at login or application start, and are written back at logout or application exit. To ensure the best performance, place this folder in the same data center or network location as the users. Configuring FlexEngine to the correct folder can be achieved by using multiple GPOs, for instance, a GPO per Active Directory site or per organizational unit (OU). Users need change permissions to store their personal settings in this share.

This share primarily contains User Environment Manager profile archives, stored as ZIP files. Most administrators configure User Environment Manager to store all user profile archives, profile archive backups, and log files in the same share. Best practice is to use a dedicated share and not the home drive.

If limited bandwidth is available between the end-user computer and the profile archives file share, consider using the User Environment Manager SyncTool. SyncTool lets users access their User Environment Manager files when they are working offline and synchronizes the changes when the user is back on the corporate network. See User Environment Manager SyncTool.

Figure 6 shows the profile archive share for user1 and the folder structure of how the profile archives are stored. The naming and folder structure of the configuration files have a one-to-one relation in the Management Console shown in Figure 3.

Figure 6: Example of Profile Archive Share
The size of the profile archive folder per user depends on the following:

- Number of applications used
- Number of backups configured
- Types of applications

The measurement for application types varies because different applications store different settings. Some applications store only small registry settings, while others create many files in the user profile.

For sizing the file share, on average, estimate 100 MB storage per user.

Setting the following NTFS security permissions on a share creates a folder for each user on first login and limits the permissions to only the user’s folder. This functionality prevents users from accessing other users’ folders.

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERMISSION</th>
<th>APPLY TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators and Helpdesk</td>
<td>Full control</td>
<td>This folder, subfolders, and files</td>
</tr>
<tr>
<td>Users</td>
<td>Create folders, append data</td>
<td>This folder only</td>
</tr>
<tr>
<td>Creator Owner</td>
<td>Full control</td>
<td>Subfolders and files only</td>
</tr>
</tbody>
</table>

Table 3: NTFS Security Permissions for Profile Archive Share

An example share name is `\server\UEMprofileshare$`.

The minimum file share permission required is `change` permission for all users.

**FlexEngine Group Policy Configuration**

To configure FlexEngine, you create a GPO in Active Directory. To configure the GPO, use the administrative templates that are provided with User Environment Manager.

You can use multiple GPOs if you need to provide different FlexEngine configurations, for example, if you manage multiple environments for multiple users. An example of different GPOs is shown in Figure 7.

![Figure 7: Example of User Environment Manager GPOs](image)
Important: Command-line arguments can override all FlexEngine settings configured through a GPO. FlexEngine command-line arguments have a higher priority than GPO settings. See FlexEngine Command-Line Arguments in Installing and Configuring VMware User Environment Manager.

Mandatory GPO Settings
After you deploy FlexEngine to the client devices, you must configure three mandatory settings:
• FlexEngine to run during the Windows login process
• FlexEngine to run during the Windows logout process
• Location of the configuration and archives path

FlexEngine needs to run during the Windows login process so that User Environment Manager can get all the settings for the client device and apply some of them as soon as the user logs in. You can enable FlexEngine to run during the Windows login process in two ways:
• Set Group Policy to Run FlexEngine as Group Policy Extension.
• Configure a Windows logon script in Group Policy.

The first method is recommended if you are deploying User Environment Manager 8.x or later, because it is easy to configure and works on all supported operating systems. If you use an earlier release of User Environment Manager, such as Immidio FlexProfiles 6.x, or if you prefer to write a Windows logon script, use the second method.

To have FlexEngine run during the Windows logout process, configure a Windows logoff script in Group Policy. The Windows logoff script is required to save user settings to the network user profile share.

You must configure these two paths:
• Flex configuration files
• Profile archives

See Configuring User Environment Manager in Installing and Configuring VMware User Environment Manager.

Optional GPO Settings
User Environment Manager has several optional GPO settings. If you are deploying User Environment Manager in a test or production environment, consider the following settings.

Use the Profile Archive Backups Group Policy setting to configure the location and number of backups to create. Users can restore a profile archive using either the Self-Support tool or the Helpdesk Support Tool.

For more information, see:
• Using User Environment Manager Self-Support in the VMware User Environment Manager Administration Guide
• VMware User Environment Manager Helpdesk Support Tool Administration Guide
Use the FlexEngine Logging Group Policy setting to configure the location and filename of the FlexEngine log file, the level of log detail, and the maximum size of the log file.

The following two settings can be configured for individual users without using the GPO:

- To enable debug logging for only one user, see the VMware knowledge base article, Enabling debug logging for a single user in VMware User Environment Manager (2113514). Debug logging can be enabled for all users with a GPO setting.
- To disable FlexEngine for a single user, see the VMware knowledge base article, Skipping the path-based import/export, Offline import, DirectFlex refresh, and UEM refresh for single user in VMware User Environment Manager (2138928).

**FlexEngine NoAD Mode**

The NoAD mode, introduced in User Environment Manager 9.1, 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. 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 or wait for Active Directory replication.

With NoAD mode, you do not need to create a GPO, Windows logon and logoff scripts, or configure Windows Group Policy settings. All User Environment Manager GPO settings are ignored. If settings from a previous GPO-based deployment are encountered, no actions are performed, and a message is logged to the FlexEngine log file.

**Note:** SyncTool 9.1 does not support NoAD mode. You must continue using a Group Policy configuration for User Environment Manager if you use SyncTool.

To install FlexEngine in NoAD mode, specify the path to the User Environment Manager configuration share through the `NOADCONFIGFILEPATH` MSI property. An example installation command:

```
msiexec.exe /i "VMware User Environment Manager 9.1 x64.msi" /qn LICENSEFILE="\filesrv1\share\VMware UEM.lic" /l* InstallUEM.log NOADCONFIGFILEPATH=\Filesrv\UemConfig$\General
```

This command inserts the basic NoAD configuration in the HKLM registry hive and enables NoAD mode.

**Note:** To disable NoAD mode, uninstall FlexEngine, and reinstall it without the `NOADCONFIGFILEPATH` MSI property.

You can provide the rest of the settings for configuring FlexEngine with NoAD mode through an XML file on the central User Environment Manager configuration share. When a user logs in, FlexEngine reads the settings from the XML file and applies them to the registry.

The XML file is called `NoAD.xml` and must reside in the `\General\FlexRepository\NoAD` subfolder.

See Installing and Configuring User Environment Manager in NoAD Mode in Installing and Configuring VMware User Environment Manager.
FlexEngine
You need to install the FlexEngine component for each Windows client device, either physical or virtual, that you want to manage with User Environment Manager.

If you are deploying a small environment for a demo (such as a proof of concept) or test, you can install FlexEngine manually on the client device. See Install User Environment Manager Manually in Installing and Configuring VMware User Environment Manager.

If you are deploying User Environment Manager in a production or large-scale environment, you can download FlexEngine as an MSI that can be installed automatically and unattended.

If you are deploying User Environment Manager in a virtual desktop infrastructure (VDI) or RDSH environment, for example, Horizon 7, you can manually install FlexEngine in the template or parent virtual machines and then deploy pools and farms of virtual desktops and RDSH servers based on these templates. If you are deploying to physical machines, you can use any software deployment tool to perform batch deployment or use Active Directory Group Policy Software Installation.

DirectFlex
FlexEngine starts when a user logs in to a client device, and it runs until the user logs out. When a user logs in, the Active Directory GPO configures FlexEngine. FlexEngine starts at login and imports settings, including application and user environment settings from the configuration share, and loads the personalization from the user profile archives share.

When the user starts an application while being logged in, FlexEngine (through DirectFlex) loads and applies the related settings to the application. When the user closes the application, FlexEngine stores the changes back to the user profile archives share. When the user logs out, FlexEngine writes the remaining Windows personalization back to the user profile archives share. Figure 8 illustrates this process.
If an IT administrator makes changes while a user is logged in, the changes are applied the next time the user logs in to a session. Changes made by the user are applied to the current session and the following sessions.

Without DirectFlex, all settings are read during the login process and written back during the logout process. For example, a user could have 10 applications on the desktop but use only 2 applications in one session. If DirectFlex is not enabled, settings for all 10 applications are loaded, which can slow down the login and logout process if there are many settings.

DirectFlex improves usage efficiency. By configuring an application for DirectFlex, the application’s settings are read when the user starts it rather than at login. Changes to settings are written back when the user exits the application instead of when the user logs out.

Take the following into consideration when enabling DirectFlex:

• To enable DirectFlex, FlexEngine must be configured to run at login. See GPO Mandatory Settings.
• Do not enable DirectFlex for configuration files containing Windows settings, such as the wallpaper, keyboard, and regional settings. These settings must always be processed during login and logout.
• Best practice is to not enable DirectFlex for applications that act as middleware and use many plug-ins, such as Microsoft Office and Internet browsers.

Triggers
In addition to the login and logout and application start and exit (DirectFlex) triggers, User Environment Manager also has triggers that can perform actions on Windows lock and unlock and session disconnect and reconnect events. Any action can be linked to one of these triggers, for example, a refresh of the User Environment settings at reconnect.

Some User Environment Manager settings can be refreshed during the session: ADMX-based settings, application blocking settings, drive mappings, environment variables, file type associations, Horizon Smart Policies, printer mappings, and shortcuts.

As an example, User Environment Manager supports location-aware printing. The session always has the correct printers for the user, because the printer mappings are created based on the location of the user and are refreshed when the user reconnects. See Configuring User Environment Settings in the VMware User Environment Manager Administration Guide.

SyncTool for Offline Scenarios
SyncTool lets you use User Environment Manager when Windows computers are working offline or have unreliable or slow WAN connections. SyncTool is not suitable for VDI and RDSH users.

SyncTool synchronizes the User Environment Manager configuration share and the personal archives to a local cache folder, so the user can always log in, even when the WAN connection is unreliable or unavailable. SyncTool is completely configurable and can generate detailed log files that provide troubleshooting assistance for IT.

You can limit network traffic by configuring SyncTool to replicate data only at specified intervals.
Figure 9 shows the SyncTool architecture and how the components work together. See the VMware User Environment Manager SyncTool Administration Guide.

Figure 9: SyncTool Architecture
Infrastructure Design

You can design your infrastructure to support User Environment Manager high availability, scalability, disaster recovery, and the steps needed to upgrade User Environment Manager to the latest version.

Scalability and high availability are required for the User Environment Manager file shares in various scenarios, such as when you have multiple data centers with VDI clients or when a decentralized infrastructure with fat clients is dispersed across different locations. In such cases, the User Environment Manager file shares can be replicated to file servers at multiple locations.

If the locations are connected with enough bandwidth and low latency, it is possible to use a central User Environment Manager configuration share. As with all infrastructure changes and products, it depends on the scenario. The only way to determine the best solution with the best performance is to test thoroughly.

A single Windows file server can scale up to 10,000 users for User Environment Manager if enough CPU and RAM are assigned to the file server. For a dedicated file server, at least four CPUs and 16 GB RAM are needed to scale to 10,000 users.

The different clients can be configured to connect to the right User Environment Manager environment by using multiple Active Directory GPOs (see Figure 2 in Planning the Deployment). If multiple file shares are used for User Environment Manager because you have multiple sites and locations, create multiple GPOs for User Environment Manager and link those GPOs to the users or computers in the correct site.

Scalability

Scalability has never been an issue with User Environment Manager because the only back-end components required are SMB file shares. User Environment Manager has been implemented for years in production environments with over 100,000 devices without scalability issues.

As one of the steps in the internal Quality Engineering process, we have performed tests with 2,000 concurrent VDI sessions on Horizon 6 and User Environment Manager. These tests have been performed with a single Windows file server, Windows 7, and Windows 10 clients and completed without any problems for User Environment Manager. All logins were successful and within an acceptable time limit.

The tests were performed with Microsoft Office 2010 and 2013. The User Environment Manager configuration was based on the Easy Start configuration that contains configuration files for many default Windows settings, Microsoft Office, and a dozen other applications. Easy Start installs a default set of Flex configuration files quickly and helps you get familiar with the various User Environment Manager settings.

Some smaller tests were also performed with User Environment Manager in combination with Citrix XenDesktop, RDSH, and App Volumes. These tests were performed with hundreds of users and passed successfully. All logins were successful and within an acceptable time limit.

The most critical component in a User Environment Manager infrastructure is the SMB file share. The tests have all been performed using a single file server virtual machine with Windows Server 2008 R2, four vCPUs, and 10 GB RAM stored on a central VMFS storage. This configuration was sufficient to manage 2,000 users.

A general recommendation is to use Windows file servers for the SMB shares because they have proven to be faster and more reliable than SMB implementations from SAN and NAS devices. Use the latest Windows version for the best SMB performance, at least Windows Server 2012, which introduced SMB 3.0.
High Availability
Because User Environment Manager leverages the existing infrastructure, you do not need to take many measures to make a highly available solution.

For an example User Environment Manager configuration with Microsoft DFS, see User Environment Manager in the VMware Horizon 7 Enterprise Edition Multi-Site Reference Architecture. If your current infrastructure does not support high availability, the multi-site reference architecture guide offers guidance on how to create a highly available infrastructure by leveraging Microsoft DFS.

You can also use Windows failover clustering for high availability of the User Environment Manager file shares. A failover cluster is a group of independent computers that provide continuous availability for applications and services. If one computer fails, another computer continues to provide the service, and users experience minimum downtime. For more information, see the Microsoft article, Failover Cluster Step-by-Step Guide: Configuring a Two-Node File Server Failover Cluster.

![Image of High Availability Wizard](image.png)

Figure 10: Select an Option for a Clustered File Server

**Important:** When Using Windows Server 2012, select **File Server for general use**. Do not select the **Scale-Out File Server for application data** option, because it is incompatible with User Environment Manager data, user profiles, redirected folders, and home drives.

You can combine DFS and clustering for better scalability and high availability. For more information, see the Microsoft blog post, Deploying DFS Replication on a Windows Failover Cluster – Part III.

Disaster Recovery
Because User Environment Manager uses the existing file servers and domain controllers, ensure that those servers are highly available (see High-Availability for options) and that a disaster recovery plan is in place.

It is recommended to integrate the Management Console into an already existing disaster recovery plan. You can install the Management Console on as many computers as required. If the Management Console is not available after a system failure, you can install it on a new management server or administrator workstation.
Upgrading
Upgrading User Environment Manager from an earlier version or from Immidio Flex+ 8.x involves these high-level steps.

1. Upgrade FlexEngine on all Windows desktops and RDSH servers.
2. Upgrade the User Environment Manager Management Console.
3. Select each Flex configuration file containing Application Templates or Windows Common Settings to automatically update to the new definitions.
   **Note:** After an upgrade, if you select a Flex configuration file and an update is available, you are prompted to upgrade the binary settings.
4. Install the ADMX templates from the User Environment Manager download package, and remove the old Immidio Flex+ ADMX templates (if any).

See Upgrade User Environment Manager in Installing and Configuring VMware User Environment Manager.

RDSH and VDI Integration
User Environment Manager works in every infrastructure on any device, both physical and virtual. User Environment Manager is supported on Citrix XenApp, Citrix XenDesktop, Horizon 7, Microsoft RDSH, and any other VDI or RDSH solution.

User Environment Manager supports multiple sessions, for example, a laptop managed by User Environment Manager and some RDSH published applications. When multiple sessions are active, the last session that logs out writes the changes to the user profile.

Consider these best practices and recommendations for any RDSH or VDI environment.

• User Environment Manager adds the most value to a nonpersistent environment because it can quickly provision the user environment at login.
• Use DirectFlex when possible to ensure that the user environment is provisioned as quickly as possible at login.
• The GPO that configures FlexEngine contains user settings. If you want to apply this policy to an OU that contains only computer objects, enable GPO loopback processing. In most cases, select Loopback Processing in merge mode. For more information, see the Microsoft article, Loopback processing of Group Policy.
• If you use silos in your RDSH environment, use conditions in User Environment Manager to support the silos. User Environment Manager also has a silos feature, but using conditions provides more flexibility.
• When a user starts both a published desktop and one or more published applications, the user could have multiple sessions on the same RDSH server. In this case, the default Windows behavior is for all sessions to share the same user profile and registry, causing issues such as drive mappings not appearing. User Environment Manager has a workaround: Add the parameter -HorizonMultiSession (for VMware) or -MultiSession (for Microsoft RDS and Citrix) to the User Environment Manager login and logout script.
• Four conditions in User Environment Manager are created for remote sessions. All the conditions work with RDP, ICA, PCoIP, and Blast Extreme remote display protocols, unless otherwise noted.

  **Endpoint IP Address** – Checks the IP address of the client from which the user is connecting to determine the user’s physical location.

  **Endpoint Name** – Checks the computer name of the client from which the user is connecting to determine the physical location of the device.
Endpoint Platform – Checks the operating system of the client from which the user is connecting. It can detect an Android, iOS, macOS, or Windows device. This condition works only with PCoIP, Blast Extreme, and ICA.

Remote Display Protocol – Checks which remote display protocol is used to deliver the remote session. It supports ICA, RDP, PCoIP, and Blast Extreme.
• You can use the User Environment Manager ADMX-based settings and registry settings to replace traditional GPOs, Citrix policies, or other policies. This option provides easier central management from a single management console.

Application Virtualization Integration
Managing the profile information for virtualized applications with User Environment Manager provides the same benefits as with natively installed applications. These settings are managed at application startup and shutdown, because the sandbox in which a virtual application is running does not exist at login and logout. Therefore, the DirectFlex feature is required for integration with application virtualization products.

User Environment Manager supports the following application virtualization products:
• VMware ThinApp 5.2
• Microsoft App-V 4.x
• Microsoft App-V 5.x
  – See Integrating User Environment Manager with Microsoft App-V in the VMware User Environment Manager Administration Guide.
• Symantec Workspace Virtualization 7.5
• VMware App Volumes
  – If you want to combine App Volumes with User Environment Manager and know which AppStacks or writable volumes template to use, see the VMware blog post, VMware User Environment Manager with VMware App Volumes.
  – There is a known timing issue when combining App Volumes and User Environment Manager. User Environment Manager has a built-in condition to check for files and folders. Because User Environment Manager runs before App Volumes, the file or folder is not yet present because the AppStacks are not yet attached. This condition is mostly used for creating shortcuts to applications. The timing issue occurs only with user-assigned AppStacks because they are attached at login. Computer-assigned AppStacks, as used in RDSH, are attached at computer startup and are not affected.
    A workaround has been implemented in App Volumes 2.12. The last AppStack attached runs a script that refreshes all shortcuts and adds them if conditions apply.
Access Control
It is possible to manage multiple User Environment Manager environments from within one management console. You can separate the test environment from the production environment or create multiple environments for different departments within an organization. In this way, User Environment Manager supports multitenant environments. See Managing Multiple Environments in the VMware User Environment Manager Administration Guide.

Configure Management Console Through GPO
User Environment Manager provides ADMX templates to configure the User Environment Manager Management Console. You can configure one or more environments (configuration shares) in the GPO and link the GPO to the right users.

When the GPO is used, a user cannot change the management console environment settings manually. The settings are mandatory to prevent users from adding other environments.

See Configuring Environments through Group Policy in the VMware User Environment Manager Administration Guide.

If environments are configured using policy, you can also lock down access to the management console using the policy setting Lock down access to VMware User Environment Manager Management Console (defined in the Management Console ADMX template). You can lock down the management console entirely or choose which management console features users can access.

See Lock Down Access to the Management Console in the VMware User Environment Manager Administration Guide.

Export Settings Between Environments
It is easy to transfer changes from one environment to another. The export feature prevents users from manual copy errors in the production environment and prevents copy errors when transferring changes from test to production. With this feature, User Environment Manager supports a tiered change model, which is often seen in organizations that use ITIL-based processes.

To export a setting from one environment to another, right-click the Flex configuration file or setting in the User Environment Manager Management Console and select Export. You can also select multiple User Environment Manager settings and export them at the same time.

Administrators can configure User Environment Manager settings and then send them to another department by using the management console export function. When only one configuration share is configured, the export function sends settings to a file, allowing the administrator to send exported files using any transport mechanism, such as USB removable media or FTP. If more than one configuration share is configured, you can export Flex configuration files to another share, for example, to a test environment.

If the administrator has access to the Application Profiler, the output of the Application Profiler can also be saved in this configuration share.
Application Profiler

You can create Flex configuration files for applications using:

• The User Environment Manager Management Console default templates
• Additional templates on the User Environment Manager community forum
• User Environment Manager Application Profiler to manually create templates

Application Profiler is a standalone application that simplifies creating Flex configuration files and predefined settings for use with User Environment Manager. It analyzes where an application stores its file and registry configuration. The output is saved in a Flex configuration file, which you can edit in Application Profiler or use directly in User Environment Manager.

You can also create application-specific predefined settings and set the initial configuration for applications. After you have specified the settings, you can export them by saving the Flex configuration file.

The Application Profiler output can be saved in any location. The administrator can save the settings directly inside a User Environment Manager environment (configuration share) or on the reference computer. The output for an application can be three or four files, depending on whether predefined settings were created for the application.

For more information, see the VMware blog posts, Profiling Applications with VMware User Environment Manager, Part 1: Introduction to Application Profiler and Part 2: Applying and Troubleshooting Predefined Settings.

Best Practices

This section contains best practices based on experience with enterprise users for deploying, managing, and troubleshooting User Environment Manager.

Initial Setup and Installation Best Practices

Consider the following best practices when installing User Environment Manager.

• To optimize login speed and the user experience, use DirectFlex as much as possible. Application Profiler enables DirectFlex by default for all created User Environment Manager configuration files. Do not enable DirectFlex for applications that act as middleware and use many plug-ins, such as Microsoft Office and Internet browsers.

• To optimize login time, enable the Run FlexEngine as Group Policy client-side extension GPO setting to start FlexEngine at login. FlexEngine can also be started with a Windows logon script, but it starts later in the login process, which means that some Windows settings, such as language and themes, cannot be managed.

• SyncTool is an optional User Environment Manager component. It provides synchronization capabilities for laptop users that work offline and users connected to a network with limited bandwidth. See the VMware User Environment Manager SyncTool Administration Guide.

• Application Profiler is a standalone application that simplifies creating configuration files and predefined settings for User Environment Manager. See the VMware User Environment Manager Application Profiler Administration Guide.

  Note: You must install Application Profiler on a machine where FlexEngine is not installed.

• If possible, do not use roaming profiles. Instead, use local profiles for desktops and laptops. Use mandatory profiles for RDSH servers and VDI desktops. Use User Environment Manager for Windows and applications settings, and use folder redirection for your personal data, documents, pictures, and so on.
• Redirect profile folders that contain user data, such as My Documents and My Pictures, to the user’s home directory. However, the administrator must make a decision about the Desktop folder location, because this folder stores personal data as well as documents, settings, and shortcuts.

• For profile folders that contain application and Windows configurations, such as Application Data, use the User Environment Manager import and export functionality instead of folder redirection to strictly manage which personalization settings to store.

• Use a dedicated share to store user profile archives instead of the existing home drive. Doing so prevents users from browsing the share or accidently deleting the profile archives. It also simplifies configuring SyncTool and makes it easier to set the correct permissions for the Helpdesk Support Tool.

• To ensure that the Group Policy client-side extension runs during each login, enable the Always wait for the network at computer startup and logon computer Group Policy setting. Apply this Group Policy to an OU in Active Directory where all the Windows clients are located.

• When a computer is offline and a user logs in with cached credentials, Group Policy client-side extensions do not execute. To ensure that FlexEngine is still running at login, use the -offlineImport parameter. See Additional FlexEngine Operations in Installing and Configuring VMware User Environment Manager.

• Because the Group Policy client-side extension runs only during login, make sure that the FlexEngine logout command is configured through a Group Policy logout script. See Configure FlexEngine to Run From a Logoff Script in Installing and Configuring VMware User Environment Manager.

Management Best Practices
Consider the following best practices when managing your User Environment Manager deployment.

• When creating drive and printer mappings, make sure that the Run asynchronously option is enabled (this setting is enabled by default). This setting optimizes the login speed because the user login process is not waiting for the mappings to be created. The user can start working while the drives and printers are mapped in the background.

• Use the User Environment Manager Management Console Comments tab to keep track of configuration changes. Administrators can use the tab to note and review changes and comments.

• Use condition sets where possible. Instead of using the same condition multiple times (for actions such as a drive mapping, printer mapping, or shortcut), it is faster to create one condition set and link it to all related items. Login time is quicker because the condition set is processed only once, and the result is cached.

• Use triggered tasks to further optimize the login speed and refresh the user environment during a session. The available triggers are lock and unlock, disconnect and reconnect. For example, printer mappings are refreshed when a remote session is reconnected only if the client IP has been changed. Printers are added and removed based on the physical location of the user.
Troubleshooting Best Practices

Consider the following best practices when troubleshooting User Environment Manager.

- User Environment Manager can generate an XML file that contains information about all configuration files and user environment settings that have been processed. See *Generating Reports About Flex Configuration Files and User Environment Settings* in the *VMware User Environment Manager Administration Guide*.

- The Helpdesk Support Tool is an optional User Environment Manager component. It provides support capabilities for User Environment Manager profile archives and profile archive backups through an intuitive graphical user interface. The Helpdesk Support Tool also displays total profile archive sizes for a user and an integrated log file viewer. See the *VMware User Environment Manager Helpdesk Support Tool Administration Guide*.

- User Environment Manager provides a Self-Support tool as part of the FlexEngine installation. See *Using User Environment Manager Self-Support* in the *VMware User Environment Manager Administration Guide*.

- To troubleshoot issues when running Windows logon scripts on Windows 7 and Windows Server 2008 R2 synchronously, see the Microsoft article, *Group Policy logon scripts do not run in Windows 7 or in Windows Server 2008 R2*.

- In some cases when using User Environment Manager to manage user-mapped printers, you might experience intermittent high CPU usage and increased disk I/O with `spoolsv.exe`. See the Microsoft article, *Intermittent High CPU and Increased Disk I/O with SPOOLSV.EXE When Mapping TS User Session Printers on Windows Server 2008 R2*.

- For details on the differences between Windows user profiles version 1 (as used in Windows XP and Windows Server 2003) and version 2 (as used in Windows 7, Windows Vista, and Windows Server 2008), see the *Microsoft Managing Roaming User Data Deployment Guide*. Other topics of interest in this deployment guide include mandatory profiles and super mandatory profiles, as introduced with Windows Vista.

The most frequently used VMware knowledge base articles are:

- Enabling debug logging for a single user in VMware User Environment Manager (2113514)
- Imports and exports in VMware User Environment Manager are slow (2113665)
- How to migrate VMware Persona Management to VMware User Environment Manager (2118056)
- VMware UEM FlexEngine Advanced Settings (ADMX template) (2145286)
- User Environment Management and ThinPrint conflicts when managing printers (2145750)

Folder Redirection Best Practices

User Environment Manager is good at managing user profile settings, including registry and personal application settings. However the user data, such as documents and pictures, need to be managed.

Best practice is to redirect profile folders that contain user data to the user’s home directory so that the documents are always available and easy to back up. The administrator must make a decision about the location of the Desktop folder because it stores personal data as well as documents, settings, and shortcuts.

When folder redirection is applied, the folders are typically redirected to the user’s home drive. Folders that are redirected are not copied back and forth at each login and logout, which can dramatically improve login and logout times.
You can configure folder redirection in the User Environment Management Console, as shown in Figure 11. Combined with the conditions that User Environment Manager provides, folder redirection is a flexible way of managing user data.

![Folder Redirection Configuration](image)

You can also configure folder redirection through standard group policies available in Active Directory. The difference is that a GPO offers the option to move the user data to the redirected folder, something User Environment Manager cannot do. A GPO can also enable offline files, which makes the redirected folders available offline. This option is mainly used for laptops.
When users roam across physical or virtual desktops or RDSH servers, it is recommended to redirect only profile folders that contain user data, such as *My Documents* and *My Pictures*, to the user's home directory.

For performance reasons, it is not recommended to redirect folders like *AppData* and the *Programs Menu*, as shown in Figure 11.

Instead, for profile folders that contain application and Windows configurations, such as *Application Data*, it is recommended to create Flex configuration files and use the User Environment Manager import and export functionality to manage which personalization settings to store. Figure 12 shows the Import/Export configuration for Adobe Acrobat Reader.

![Figure 12: Adobe Acrobat Reader Config File Import/Export Section](image)

Additional benefits of managing profile settings with User Environment Manager include:
- Reduced network storage because the folders and files have stricter management and compression
- Cross-platform usage for settings
- Fewer open file handles to the file servers

**Additional Resources**
For more information, see the following resources:
- VMware User Environment Manager product webpage
- VMware User Environment Manager product documentation
- VMware User Environment Manager Community
- VMware Horizon 7 Enterprise Edition Multi-Site Reference Architecture
- VMware Horizon 7 Enterprise Edition Reference Architecture
- VMware End-User Computing YouTube Channel: User Environment Manager
- Horizon 7 Suite: Extend Your Value (HOL-1751-MBL-3) (VMware Hands-On Lab)
- VMware End-User-Computing blog
- Microsoft article, Customize the default local user profile user when preparing an image of Windows
About the Authors and Contributors

The following authors co-wrote this paper:

- Pim van de Vis, Product Engineer, End-User Computing, VMware
- Gina Daly, Technical Marketing Manager, End-User-Computing Technical Marketing, VMware

Pim van de Vis works in the End-User-Computing Research and Development department and is the link between customers and developers. He has experience with various enterprise IT infrastructures and focuses mainly on end-user-computer virtualization solutions such as VDI, application virtualization, and User Environment Manager.

Contributors to this document include:

- Stephane Asselin, Lead Architect, App Volumes, VMware
- Jason Bassford, VMware alumnus
- Arnout Grootveld, Staff Engineer, User Environment Manager Research and Development, VMware
- Jason Marshall, Senior Manager, Product Engineering, End-User Computing, VMware
- Barak Nissim, Senior Systems Engineer, End-User-Computing Practice, VMware
- Josh Spencer, Architect, End-User-Computing Technical Marketing, VMware
- Jim Yanik, Senior Manager, End-User-Computing Technical Marketing, VMware
- Raymond Wiesemann, Product Experience Manager, Research and Development, End-User Computing, VMware
- Judy Wu, Senior Solution Engineer, End-User Computing, VMware

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